



**UNIVERSIDAD ESTATAL
PENINSULA DE SANTA ELENA**

**FACULTAD DE SISTEMAS Y
TELECOMUNICACIONES**

CARRERA DE INFORMÁTICA

TRABAJO DE TITULACIÓN

Propuesta Tecnológica, previa a la obtención del título de:

INGENIERO EN SISTEMAS

“ESTUDIO DE ASEGURAMIENTO DE LA INFRAESTRUCTURA DE
COMUNICACIONES IMPLEMENTANDO UNA DMZ Y FIREWALL
PERIMETRAL EN LA COOPERATIVA DE AHORRO Y CRÉDITO VISIÓN
INTEGRAL, SANTA ELENA”

AUTOR

DIMAS MENDOZA GONZALEZ

PROFESOR TUTOR

ING. IVÁN CORONEL SUÁREZ, MSIA

LA LIBERTAD – ECUADOR

2016

AGRADECIMIENTO

Primero a Dios por darme salud, vida y permitirme llegar a culminar esta etapa de mi carrera profesional.

A mi padre Dimas por la confianza, el apoyo, por inculcarme la perseverancia de culminar algo que inicie, por estar siempre ahí cuando necesite su ayuda, por ayudarme en mis proyectos universitarios, por ser el soporte para poder conseguir este objetivo, estoy seguro que está orgulloso de todo lo que estoy logrando.

A mi madre Ivonne por esas veces que le toco levantarse de madrugada a darme el desayuno para ir a tutorías, por todas las atenciones que me dio a lo largo de toda mi carrera universitaria, por sacarme siempre una sonrisa cuando ya no sabía qué hacer, ella así como mi padre son mi orgullo y por ustedes va este trabajo.

A mis tíos en especial a mi tía Josefina, mi segunda madre gracias por los consejos, su ayuda y su apoyo para seguir estudiando y por estar siempre ahí para tener una charla, esto también va por usted “Mama”.

A mis hermanos, sé que soy su ejemplo a seguir profesionalmente solo espero no desmayen y continúen.

A mis abuelitos maternos y paternos, sé que no los tengo físicamente a algunos ya pero siempre los tengo presentes y les agradezco por todo.

A Jenny, gracias por siempre estar ahí cuando te he necesitado, tu apoyo incondicional, tus consejos y por no dejarme desmayar cuando a veces me rendía.

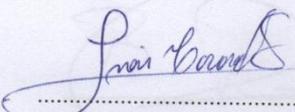
Y finalmente agradecer al Ing. Iván Coronel, por saber guiarme a lo largo de todo este proyecto, sin sus conocimientos no hubiera culminado este proyecto gracias por el apoyo y el tiempo que supo darme.

Dimas Fernando Mendoza González

APROBACIÓN DEL TUTOR

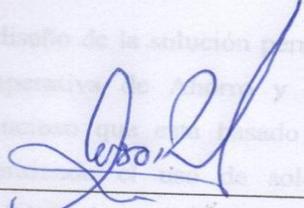
En mi calidad de tutor del trabajo de titulación denominado: **“ESTUDIO DE ASEGURAMIENTO DE LA INFRAESTRUCTURA DE COMUNICACIONES IMPLEMENTANDO UNA DMZ Y FIREWALL PERIMETRAL EN LA COOPERATIVA DE AHORRO Y CRÉDITO VISIÓN INTEGRAL, SANTA ELENA”**, elaborado por el estudiante Mendoza González Dimas Fernando de la carrera de Informática de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo al estudiante para que inicia los trámites legales correspondientes.

La Libertad, septiembre del 2016

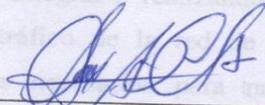
A rectangular box containing a handwritten signature in blue ink. The signature is cursive and appears to read 'Iván Coronel Suárez'. Below the signature is a horizontal dotted line.

Ing. Iván Coronel Suárez, MSIA

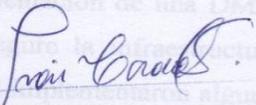
TRIBUNAL DE GRADO



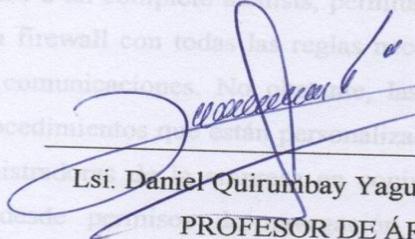
Ing. Walter Orozco Iguasnia, MSc.
DECANO DE FACULTAD



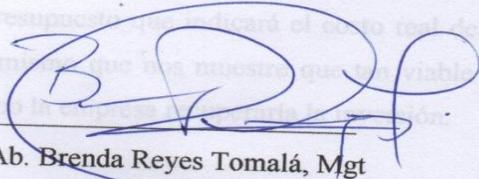
Ing. Mariuxi De la Cruz De la Cruz, MSig.
DIRECTORA DE CARRERA



Ing. Iván Coronel Suárez, MSia
PROFESOR TUTOR



Lsi. Daniel Quirumbay Yagual, MSia
PROFESOR DE ÁREA



Ab. Brenda Reyes Tomalá, Mgt
SECRETARIA GENERAL

RESUMEN

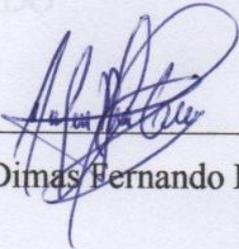
El diseño de la solución permite resolver los problemas que actualmente tiene la Cooperativa de Ahorro y Crédito “Visión Integral”, realizando un estudio minucioso que está basado en asegurar el tráfico de la red de la empresa, permitiendo el uso de solo de los puertos necesarios para navegación y administración de servidores, de esta manera la institución no será un blanco fácil de algún ataque y proteger la información que existe dentro de la misma. Este documento tiene como objetivo determinar las opciones más viables tanto en hardware como software que en base a un completo análisis, permita elaborar la implementación de una DMZ y un firewall con todas las reglas necesarias para que asegure la infraestructura de comunicaciones. No obstante, las reglas del firewall implementaron algunos procedimientos que están personalizados en base a los requerimientos de los administradores de la empresa en conjunto con el administrador de red, que van desde permisos de navegación web hasta administración remota de los servidores. Adicionalmente concluido el estudio se elaborará el respectivo presupuesto que indicará el costo real del proyecto y por supuesto un análisis del mismo que nos muestre que tan viable sería tenerlo en producción y en qué tiempo la empresa recuperaría la inversión.

ABSTRACT

The design of the solution allows you to resolve the problems that currently has the Savings and Credit Cooperative "Integral Vision", conducting a thorough study that is based on ensuring the network traffic of the company, allowing the use of only the ports required for navigation and administration of servers, in this way the institution will not be an easy target of attack and protect the information that exists within the same. This document has as objective to determine the most viable options in both hardware and software that is based on a comprehensive analysis, will permit the development of the implementation of a DMZ and a firewall with all the rules necessary to ensure the communications infrastructure. However, the firewall rules implemented some procedures that are customized based on the requirements of the administrators of the company in conjunction with the network administrator, ranging from web browsing permissions until remote administration of servers. Additionally concluded the study will be prepared the respective budget that will indicate the actual cost of the project and of course an analysis of the same to show us that as viable serious take in production and in what time the company would recover the investment.

DECLARACIÓN

El contenido del presente Trabajo de Graduación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



Dimas Fernando Mendoza González

TABLA DE CONTENIDO

ITEM	PAG.
APROBACIÓN DEL TUTOR	III
TRIBUNAL DE GRADO	IV
RESUMEN	V
ABSTRACT	VI
DECLARACIÓN	VII
TABLA DE CONTENIDO	VIII
ÍNDICE DE FIGURAS	X
ÍNDICE DE TABLAS	XIII
LISTA DE ANEXOS	XIV
INTRODUCCIÓN	1
CAPÍTULO I	2
FUNDAMENTACIÓN	2
1.1. Antecedentes	2
1.2. Descripción del Proyecto	3
1.3. Objetivos del Proyecto	4
1.3.1. Objetivo General	4
1.3.2. Objetivos Específicos	4
1.4. Justificación	5
1.5. Metodología	6
1.5.1. Metodología de Investigación	6
CAPÍTULO II	8
LA PROPUESTA	8
2.1. Marco contextual	8
2.1.1. Cooperativa de Ahorro y Crédito “Visión Integral”	8
2.1.2. Visión	9
2.1.3. Misión	9
2.1.4. Objetivos	9
2.1.5. Organigrama de la Cooperativa de Ahorro y Crédito Visión Integral	10
2.2. MARCO CONCEPTUAL	11
2.2.1. Redes de Computadoras	11
2.2.2. Modelo OSI	11

2.2.3	TCP/IP	12
2.2.4	ISO 27001	12
2.2.5	Direccionamiento IP	13
2.2.6	Seguridad Informática	14
2.2.7	Políticas de Seguridad	15
2.2.8	Tipos de Ataques	16
2.2.9	Zona Desmilitarizada	18
2.2.10	Firewall	18
2.2.11	Virtualización	19
2.3	DISEÑO DE LA PROPUESTA	22
2.3.1	Análisis de la Situación actual	22
2.3.2	Diseño de la solución	23
2.3.3	Servidor Web	31
2.3.4	Servidor Aplicaciones	31
2.3.5	Servidor Base de Datos	32
2.3.6	Servidor Proxy	32
2.3.7	Instalación y configuración del firewall perimetral	33
2.3.8	Configuración y reglas del firewall	39
2.3.9	Proxy Administrativo	43
2.3.9.1	Instalación de Squid proxy Administrativo y proxy Usuarios	45
2.3.9.2	Instalación de SquidGuard proxy Administrativo y proxy Usuarios	50
2.3.10	Proxy Usuarios	54
2.4	ESTUDIO DE FACTIBILIDAD	59
2.4.1	Factibilidad Técnica	59
2.4.2	Factibilidad Económica	60
2.4.3	VAN y TIR	64
2.4.4	Pentesting	67
2.5	RESULTADOS	76
	CONCLUSIONES	77
	RECOMENDACIONES	78
	GLOSARIO	79
	BIBLIOGRAFÍA	81
	ANEXOS	

ÍNDICE DE FIGURAS

ITEM	DESCRIPCIÓN	PAG.
Figura 1	Ubicación actual de la empresa, (Google Maps, 2016)	8
Figura 2	Organigrama de la empresa	10
Figura 3	Direccionamiento Ip, (Cisco, 2016)	14
Figura 4	Diagrama de la Cooperativa de Ahorro y Crédito "Visión Integral"	23
Figura 5	Diagrama de red propuesto	24
Figura 6	WAN	27
Figura 7	RED SERVIDORES	28
Figura 8	RED INTERNA	29
Figura 9	Pantalla principal de pfSense	33
Figura 10	Inicio instalación de pfSense	35
Figura 11	Instalación pfSense paso 1	35
Figura 12	Instalación pfSense paso 2	35
Figura 13	Instalación pfSense paso 3	36
Figura 14	Instalación pfSense paso 4	36
Figura 15	Instalación pfSense paso 5	36
Figura 16	Instalación pfSense paso 6	36
Figura 17	Culminación de la instalación de pfSense	36
Figura 18	Reiniciando la máquina virtual	37
Figura 19	Interfaces del firewall perimetral	37
Figura 20	Asignar tarjeta de red a interfaz WAN	37
Figura 21	Configuraciones IP firewall perimetral	38
Figura 22	Firewall perimetral con sus interfaces configuradas	38
Figura 23	Reglas de la interfaz WAN firewall perimetral, pfSense	39
Figura 24	Página web de la cooperativa	40
Figura 25	Aplicación web de la cooperativa, formulario de ejemplo	41
Figura 26	Reglas de interface RED_SERVIDORES, pfsense	41
Figura 27	Reglas de la interface RED_INTERNA, pfSense	42
Figura 28	Esquema proxy administrativo	43
Figura 29	Proxy Administrativo	44

Figura 30	Reglas interface WAN proxy Administrativo, pfSense	44
Figura 31	Reglas interface LAN proxy Administrativo, pfSense	45
Figura 32	Instalación Squid paso 1, (“Squid en pfsense,” 2012)	45
Figura 33	Instalación Squid paso2, (“Squid en pfsense,” 2012)	46
Figura 34	Instalación de Squid paso 3, (“Squid en pfsense,” 2012)	46
Figura 35	Configuración de Squid ajustes generales	47
Figura 36	Configuración Squid administración de cache	48
Figura 37	Configuración de Squid control de acceso red Administrativo	49
Figura 38	Configuración de Squid control de acceso red Usuarios	49
Figura 39	Configuración SquidGuard ajustes generales	50
Figura 40	Configuración SquidGuard ajustes generales	51
Figura 41	Descarga del paquete Shallalist para bloquear contenido web	51
Figura 42	Bloqueo de sitios por su contenido en SquidGuard	52
Figura 43	Bloqueo de sitios por su contenido en SquidGuard	53
Figura 44	Esquema proxy usuarios	54
Figura 45	Proxy usuarios	55
Figura 46	Reglas interface WAN proxy usuarios	55
Figura 47	Reglas interface LAN proxy usuarios	56
Figura 48	Configuración de Windows para trabajar con el proxy usuarios	57
Figura 49	Bloqueo de configuración de las opciones de internet	58
Figura 50	Opciones de internet bloqueadas	58
Figura 51	Ingresos anuales	66
Figura 52	Ataques a redes. Fuente: "Seguridad Informática, UNAM"	68
Figura 53	Mapeo Externo	69
Figura 54	Escaneo de puertos de la interface WAN	69
Figura 55	Putty hacia la interface WAN	70
Figura 56	Conexión fallida a la interface WAN	70
Figura 57	Identificación sistema operativo	71
Figura 58	Identificación de servicios	71
Figura 59	Mapeo Interno	72
Figura 60	Nmap interno	73
Figura 61	Traceroute hacia los servidores	73

Figura 62	Buscando el sistema operativo del servidor	74
Figura 63	Búsqueda de firewalls activos	74
Figura 64	Búsqueda de puertos UDP	75
Figura 65	Conexión al servidor web con Putty	75
Figura 66	Conexión al servidor web con FileZilla	75

ÍNDICE DE TABLAS

ITEM	DESCRIPCIÓN	PAG.
Tabla 1	Direccionamiento IP	22
Tabla 2	Direccionamiento IPV4 de la nueva infraestructura de red	25
Tabla 3	Direccionamiento IPV6 de la nueva infraestructura de red	25
Tabla 4	Puertos TCP y UDP definidos en el estudio	26
Tabla 5	Porcentaje de crecimiento de las redes	27
Tabla 6	Sitios restringidos red administrativa	30
Tabla 7	Sitios restringidos red trabajadores	30
Tabla 8	Costo de hardware	61
Tabla 9	Costos de software	61
Tabla 10	Costo del personal	62
Tabla 11	Costo de materiales de oficina	62
Tabla 12	Costos servicios básicos	62
Tabla 13	Costos movilización y alimentación	62
Tabla 14	Costos de implementación	62
Tabla 15	Costo del proyecto	63
Tabla 16	Ingresos primer año	64
Tabla 17	Ingresos segundo año	65
Tabla 18	Ingresos tercer año	65
Tabla 19	Ingresos cuarto año	65
Tabla 20	Ingresos quinto año	66
Tabla 21	Proyecciones proyecto DMZ	67
Tabla 22	Resultados proyecciones del proyecto al 10%	67

LISTA DE ANEXOS

N.-	DESCRIPCIÓN
1	Formato de la entrevista
2	Formato de la encuesta
3	Carta Aval de la Cooperativa de Ahorro y Crédito “Visión Integral”
4	Instalación y configuración del servidor web
5	Configuración del servidor de aplicaciones
6	Instalación de SQL 2012

INTRODUCCIÓN

En la actualidad en todas las empresas el uso de las tecnologías de comunicación es indispensable, la mayoría de instituciones poseen una infraestructura de red compleja, y por lo general estas son implementadas de manera empírica, actualmente se encuentran trabajando y soportando grandes cantidades de usuarios, el problema es que dichas redes son blanco fácil de ataques de terceras personas por el hecho que no se siguen normas, protocolos y estándares al momento de implementar la misma.

La Cooperativa de Ahorro y Crédito “Visión Integral” tiene una infraestructura de red que no está acorde con lo que en realidad una institución como la que se menciona debe tener, por este motivo surge la necesidad de hacer un estudio técnico, que determinará que equipos de red usar, sean estos (antenas, switches, medios, etc.), que sistemas operativos (Windows, Linux, FreeBSD, etc.) y que tipo de servidores se deben utilizar para de esta manera obtener un presupuesto que se ajuste a lo que la empresa necesite.

En el primer capítulo se plantea la problemática, justificaciones, los objetivos a cumplir, situación de la empresa, etc. los cuales contienen la teoría de todo lo planteado anteriormente con más detalle.

En el segundo capítulo contiene todas las bases teóricas de los temas que se abarcarán al hacer el estudio de la implementación, los detalles de los equipos a utilizar, el diseño de la propuesta, su estudio de factibilidad y finalmente los resultados de la misma los cuales vendrían a ser el reporte final.

CAPÍTULO I

FUNDAMENTACIÓN

1.1. Antecedentes

La cooperativa de ahorro y crédito Visión Integral “COAC”, inició sus funciones desde septiembre del 2009, ha tenido participación en la mayoría de las comunidades de manera activa con las que han impulsado proyectos integrales de desarrollo en la Península de Santa Elena.

Cuenta aproximadamente con 300 beneficiarios en su cartera de crédito, además tiene en su sede los departamentos de gerencia, oficina de crédito, contabilidad y atención al cliente.

La COAC es una cooperativa pequeña, sus bienes tecnológicos son limitados a 16 computadoras entre portátiles y de escritorio, 1 router y 2 switches.

La COAC cuenta con acceso a Internet para el envío de todos los informes mensuales, trimestrales, semestrales y anuales que le exigen los órganos reguladores.

En el acceso a internet tanto el ancho de banda del proveedor, como el router son limitados, ambos por no tener la capacidad de soportar más de cuatro usuarios en línea a la vez teniendo en cuenta que ambas conexiones están habilitadas, mientras que la intranet tiene recursos compartidos en este caso impresoras y carpetas, adicional a esto no se tiene implementado ningún firewall por lo que sería sencillo el ingreso a intrusos a través de la web.

Cabe recalcar que en auditorias previas ya se llamó la atención al gerente de la cooperativa sobre la infraestructura de red que maneja la empresa porque no tiene implementado un firewall, no hay segmentación de la red, no hay servidor de

dominio, etc.; en conclusión, no existe una adecuada implementación de seguridad en la red en la empresa.

La seguridad en redes de computadoras actualmente es un tema muy común, debido a la suma importancia que ésta representa en el mundo de la informática, y por ende de todos los sistemas de información que se encuentran en ella; de esta manera, desde las grandes hasta las pequeñas empresas y los millones de usuarios que dependen de esta, son vulnerables ya sea de manera directa o indirecta a las diferentes amenazas que atentan contra su seguridad.

Por tal motivo se sugiere hacer un estudio de toda la infraestructura de comunicaciones y de esta manera plantear a futuro como se implementaría una Zona Desmilitarizada, con el fin de parametrizar los servidores y servicios de estos para acceder a internet que se tienen proyectados instalar, teniendo en cuenta que la información que se tiene y se gestiona es de suma importancia para la Cooperativa, mejorar el ancho de banda en base a los terminales que se tiene proyectado instalar y los componentes de red que se utilizarían.

1.2. Descripción del Proyecto

El siguiente proyecto propone a futuro implementar una DMZ como medio de protección interna de la Cooperativa de Ahorro y Crédito Visión Integral, con la finalidad de mejorar la seguridad de la infraestructura tecnológica de la institución.

Una red Perimetral, se ubica entre la red pública (WAN) y la red privada de la institución (LAN), esta se encarga de asegurar el tráfico de información entre la red interna y externa sin comprometer la seguridad de la Cooperativa de Ahorro y Crédito Visión Integral.

Uno de los sistemas más utilizados para la implementación de una DMZ por preferencia es LINUX, puesto que este ofrece programas OPEN SOURCE, lo que

es un gran beneficio para la economía de las PYMES por el costo/beneficio de la empresa.

El presente proyecto se centra en realizar el análisis y determinar el diseño de red, el hardware y software que podría ser utilizado cuando se implemente la red, teniendo en cuenta el mejor coste/beneficio de la Cooperativa de Ahorro y Crédito Visión Integral.

Además de la configuración de los servicios que se van a restringir y permitir para los usuarios de la empresa (YouTube, Facebook, Correos, SRI, etc.).

La implementación de CentOS7, Windows Server y el firewall pfSense ofrecen múltiples beneficios y varios tipos de configuraciones, pero en este proyecto nos enfocaremos en implementar un Proxy, Servidor Web, Servidor de Aplicaciones, Servidor de Base de Datos y el Firewall con todas las reglas que son necesarias para tener asegurada de manera óptima la red.

1.3. Objetivos del Proyecto

1.3.1. Objetivo General

Elaborar un estudio para la implementación de un DMZ y firewall perimetral aplicando CENTOS7 y pfSense para la Cooperativa de Ahorro y Crédito Visión Integral.

1.3.2. Objetivos Específicos

- ✓ Diagramar la DMZ y el aseguramiento de la red, teniendo en cuenta el direccionamiento IPv4 e IPv6 en un nuevo esquema y las políticas de seguridad basado en un estándar.
- ✓ Iniciar un proceso de virtualización de un Servidor en Centos7 y configurarlo de acuerdo a los requerimientos del esquema de la nueva red.

- ✓ Realizar la virtualización y configuración del Firewall pfSense, además de establecer todas las políticas para la nueva infraestructura de red.

1.4. Justificación

La seguridad de la información y de los equipos ha adquirido tal grado de importancia en una empresa, que cada vez se necesita una red más protegida para asegurar estos bienes.

Con el estudio de implementación de una DMZ y un Firewall de Borde la COAC Visión Integral se beneficiará al asegurar la red de personal no autorizado que desee dañarla además de tener una protección adicional para esta institución. El personal o la persona competente al analizar los riesgos que conlleva no tener protegida la información confidencial que se maneja en la empresa, los conduce a la necesidad de operar de una manera más eficiente y de segmentar la red para tener un nivel de seguridad más alto, por lo que nace el interés de contar con una DMZ como la propuesta de obtener una estructura de red que pueda ser utilizada en la empresa.

Existen varias razones que motivan a la COAC Visión Integral en integrar los servicios de una DMZ:

- ✓ Aumentar la imagen institucional, dadas las expectativas que esta infraestructura de seguridad provee.
- ✓ Estar a la par con la tecnología: DMZ es una infraestructura de moda, y existe la creencia de que las empresas que no la utilizan quedan rezagados en cuanto a seguridad de la información.
- ✓ Tanto el sistema operativo como las herramientas a utilizar son OPEN SOURCE por lo que el costo de licenciamiento es 0 en la mayoría de los casos.

Actualmente la COAC está en categoría 5 dentro del rango nacional que establece la Superintendencia de Economía Popular y Solidaria (SEPS), en este caso la Gerencia desea empezar los trámites para subir de categoría y uno de los requisitos indispensables es contar con una buena infraestructura tecnológica (seguridad de red, internet, pagina web, etc.) por lo que el estudio que se va a realizar y la solución a implementar tendría un impacto muy positivo que ayudaría a alcanzar los logros que espera la gerencia.

1.5. Metodología

1.5.1. Metodología de Investigación

Para este proyecto se utilizará el método de investigación de campo, esta clase de investigación se apoya en informaciones que provienen entre otras, de entrevistas, cuestionarios, encuestas y observaciones.

También el método de observación directa es uno de los más utilizados, en este caso por su eficacia. Su aplicación resulta mucho más exacta cuando se consideran estudios de micro-movimientos, de tiempos y métodos. Es más recomendable para aplicarlo a los trabajos que comprenden operaciones manuales o que sean sencillos o repetitivos.

Y complementando ambos se usa la investigación bibliográfica amplia (investigación bibliográfica propiamente dicha), de carácter general o especializado con fines de investigación general (tesis, disertaciones, etc.).

La información bibliográfica pretende obtener los conocimientos necesarios para llevar a cabo un proceso de investigación más amplio sobre cualquier tema determinado.

Estas metodologías se pueden utilizar en distintos momentos de la investigación, desde su etapa inicial para diagnosticar el problema a investigar, hacer las respectivas preguntas y ser concisas a la hora de plantear la solución

La recopilación de la información se respaldará mediante la técnica de entrevistas que se la realizaran a los trabajadores de la COAC Visión Integral para comparar que los resultados de la observación concuerden con los resultados de la entrevista.

1.5.2. Metodología de desarrollo.

Se aplicará una metodología de desarrollo Top-Down que implica:

- ✓ Recopilar los requisitos mediante la observación y las entrevistas.

- ✓ En la fase de observación se llevaron a cabo las siguientes actividades
 - Visitar la empresa para proceder con la entrevista y levantamiento de la información necesaria

 - Observación directa en la Cooperativa de Ahorro y Crédito “Visión Integral” para comprobar los datos obtenidos.

- ✓ Analizar la información recopilada y diseñar un modelo de solución de la red.

- ✓ Fase de desarrollo e implementación en la cual se realiza el diseño de la red y las reglas del firewall.

- ✓ Fase de prueba en el que se corrige posibles errores.

- ✓ Fase de implementación final, en esta fase la DMZ queda de manera funcional y libre de errores.

CAPÍTULO II

LA PROPUESTA

2.1. Marco contextual

2.1.1. Cooperativa de Ahorro y Crédito “Visión Integral”

La Cooperativa de Ahorro y Crédito “VISION INTEGRAL”, es una organización campesina de apoyo al desarrollo fundada en el año 2009, cuyos principios institucionales han impulsado la práctica solidaria de desarrollo, donde los actores protagonistas de las acciones institucionales son los propios campesinos comuneros de las diferentes comunidades campesinas en las provincias de Santa Elena (Colonche - Manglaralto y Chanduy); y Manabí (Salango).

Después de haber pasado por un proceso de transformación institucional, que dio la oportunidad de ser Comité Avícola “VISION INTEGRAL”, luego a Asociación de Pequeños Productores Agropecuarios “VISION INTEGRAL”, la Cooperativa de Ahorro y Crédito “VISION INTEGRAL”, adquiere vida jurídica en septiembre del 2009.

Y desde esa fecha hasta la actualidad se brindan servicios que tienen como fin promover el desarrollo agropecuario.

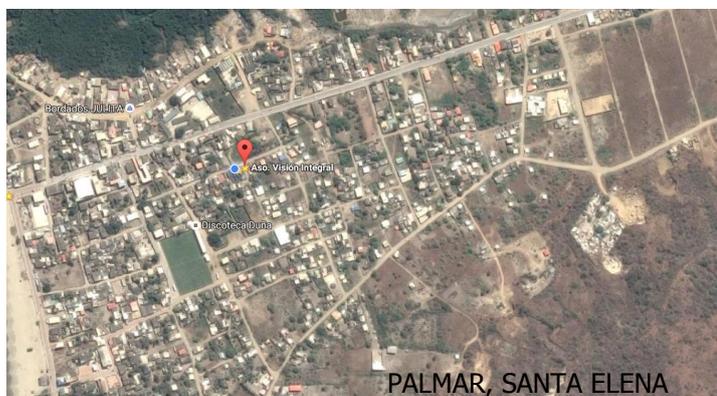


Figura 1 Ubicación actual de la empresa, (Google Maps, 2016)

2.1.2. Visión

La Cooperativa de Ahorro y Crédito "VISION INTEGRAL" es una entidad financiera que presta servicios de operaciones crediticias a campesinos comuneros de las parroquias y recintos del cantón Santa Elena, brindándole a sus socios confianza, seguridad y trato personalizado

2.1.3. Misión

En el 2017 ser una institución financiera sólida que trabaje con lineamientos estratégicos propios construidos participativamente con los comuneros socios de la cooperativa, con lo cual se busca satisfacer las necesidades de socios y clientes, para de esta manera obtener el reconocimiento de los habitantes y autoridades de la región.

2.1.4. Objetivos

1. Incrementar gradualmente el número de socios y facilitar el ingreso de los mismos
2. Disponer de recursos suficientes para satisfacer las necesidades de todos los socios de la cooperativa.
3. Buscar nuevas fuentes de financiamiento que nos permitan crecer.
4. Promover el desarrollo económico de sus socios mediante una adecuada gestión financiera.
5. Incrementar la rentabilidad de la institución por medio de actividades que se definan dentro del marco legal permitido para las cooperativas de ahorro y crédito
6. Establecer la mejora continua en todos los niveles de la institución.

7. Disponer del recurso humano, físico y tecnológico idóneo para la institución.

2.1.5. Organigrama de la Cooperativa de Ahorro y Crédito Visión Integral

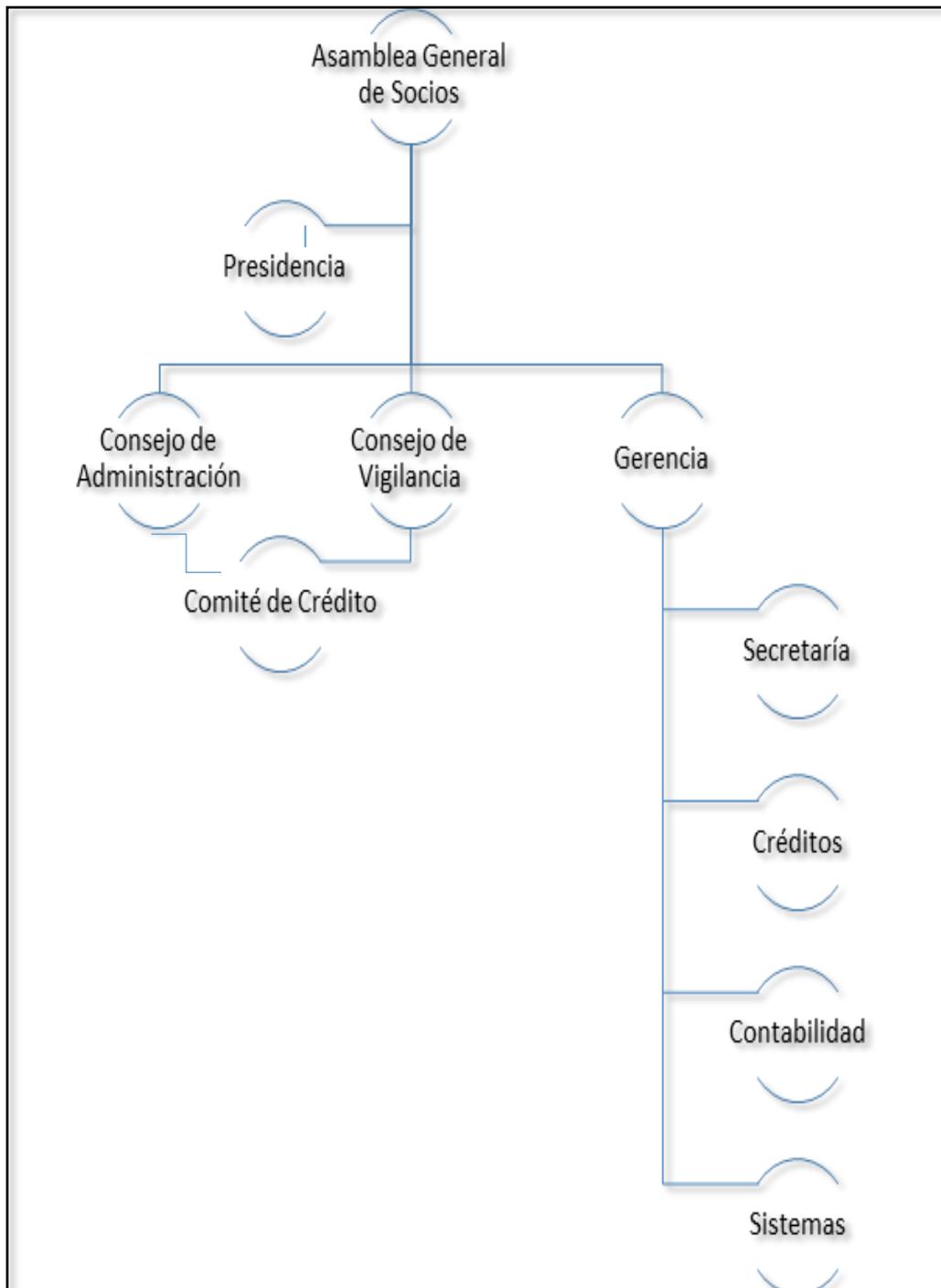


Figura 2 Organigrama de la empresa

2.2. MARCO CONCEPTUAL

2.2.1 Redes de Computadoras

Se tiene muchos conceptos generales sobre redes de computadoras pero el mejor concepto que define a este conglomerado de equipos sería el siguiente:

“Las redes de ordenadores actuales son una amalgama de dispositivos, técnicas y sistemas de comunicación que han ido apareciendo desde finales del siglo XIX o, lo que es lo mismo, desde la invención del teléfono.” (David et al., 2004)

Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos.

2.2.2 Modelo OSI

A la hora de describir la estructura y función de los protocolos de comunicaciones se recurre a un modelo de arquitectura desarrollado por la ISO.

“La torre OSI pretendía ser un modelo básico de referencia, un marco para el desarrollo de estándares que permitieran la interoperabilidad completa.”(David et al., 2004)

“El modelo OSI está constituido por 7 capas que definen las funciones de los protocolos de comunicaciones. Cada capa del modelo representa una función realizada cuando los datos son transferidos entre aplicaciones cooperativas a través de una red intermedia.” (“TCP/IP y el modelo OSI | Textos Científicos,” 2015)

Este modelo tiene la característica de ser de carácter teórico puesto que explica cada capa y sus servicios de forma detallada sin obviar ningún detalle.

2.2.3 TCP/IP

TCP/IP es el conjunto de todas las reglas de comunicación que existen en el internet, un concepto acertado sería el siguiente:

Los protocolos que distinguen la red Internet como una unidad son el IP (Internet protocol) y el TCP (Transmission control protocol). Estos protocolos no son los únicos, pero sí los más importantes de entre los que se necesitan para hacer funcionar la red Internet. Por este motivo, a todos en conjunto se les llama normalmente pila TCP/IP (TCP/ IP stack).(David et al., 2004)

Se describe al protocolo IP como un mecanismo de acceso a Internet que está disponible a través de una red de área local LAN.

2.2.4 ISO 27001

Es uno de los estándares de seguridad más usados por el hecho que estas contienen la metodología que usan los mejores especialistas del mundo sobre la seguridad de la información.

“Las normas publicadas bajo esta serie 27001 son estándares alineados con el conjunto de normas de la International Organization for Standardization (ISO) y International Electrotechnical Commission (IEC), que son desarrolladas mediante comités técnicos específicos”. (“ISO27000.es Gestión de Seguridad de la Información,” 2012)

ISO 27001 es una norma que se basa principalmente en la definición, implantación y certificación de los Sistemas de Seguridad de Gestión de la Información cuyo objetivo es velar por la protección de la información puesto que definimos el control y la clasificación de los activos de la organización según su criticidad y de esta manera evaluar los riesgos de manera coherente con el modelo

de negocio, tienen 5 aspectos importantes que debemos tener en cuenta, si la empresa desea tener:

- ✓ Compromiso y sensibilización.
- ✓ Organización.
- ✓ Análisis de procesos y servicios.
- ✓ Gestión de riesgos.
- ✓ Mejora continua.

2.2.5 Direccionamiento IP

Se coincide que el direccionamiento IP es un identificador único de red para cada ordenador, existen muchos conceptos sobre este tema pero el más acertado sería el siguiente:

Las direcciones IP son únicas para cada máquina. Para ser precisos, cada dirección es única para cada una de las interfaces de red IP de cada máquina. Si una máquina dispone de más de una interfaz de red, necesitará una dirección IP para cada una. (David et al., 2004)

Las direcciones IP (IP es un acrónimo para Internet Protocol) son un identificador único e irrepetible con el cual se identifica un ordenador conectado a una red que corre el protocolo IP. (userservers, 2016)

Una IP es un conjunto de cuatro números del 0 al 255 separados por puntos. Por ejemplo, www.google.com.ec tiene la IP: 216.58.192.99, en conclusión una IP es una forma más sencilla de comprender números muy grandes.

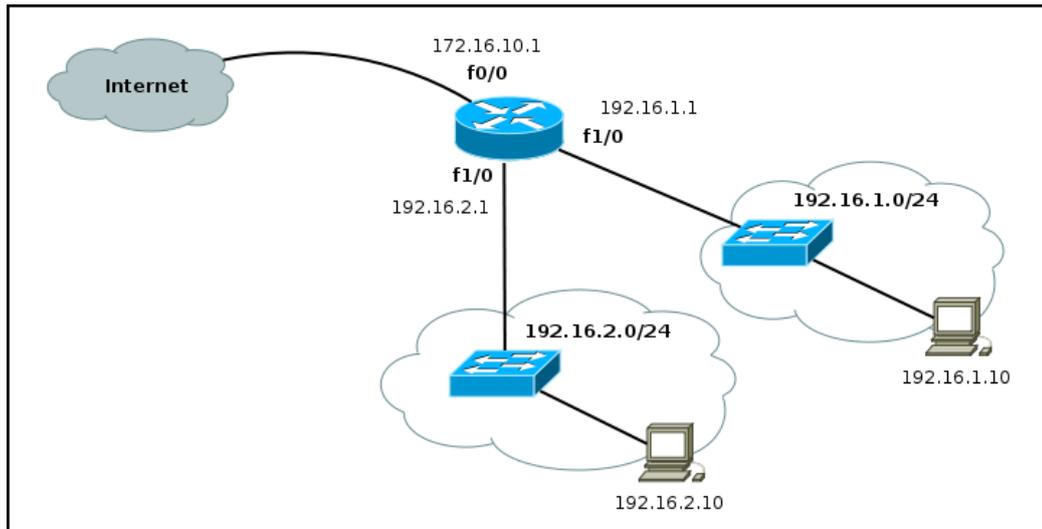


Figura 3 Direccionamiento Ip, (Cisco, 2016)

“Todos los computadores también cuentan con una dirección física exclusiva, conocida como dirección MAC. Estas son asignadas por el fabricante de la tarjeta de interfaz de la red. Las direcciones MAC operan en la Capa 2 del modelo OSI.” (Urueña León, 2006)

2.2.6 Seguridad Informática

La Seguridad Informática en términos generales es una rama de la informática que se dedica a la protección de la información, un concepto general sobre el tema sería el siguiente:

La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada. (Fernandez, 2013)

Solamente cuando estamos conscientes de las potenciales amenazas, agresores y sus intenciones dañinas (directas o indirectas) en contra de nosotros, podemos tomar medidas de protección adecuadas, para que no se pierda o dañe nuestros recursos valiosos, en este sentido, la Seguridad Informática sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella. (Erb, Markus; Flores, Carolina; Chub, Arturo; Kurzen, Adrian; Sarantes, 2010)

2.2.7 Políticas de Seguridad

Las políticas son un conjunto directrices documentadas que nos dan una guía de cómo llevar a cabo determinados procesos dentro de una organización, está dirigido exclusivamente al personal interno de una organización aunque existen casos que hay intervenciones de personal externo, describen cómo comportarse ante un determinado problema o situación.

“Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro y en algunos casos fuera de la organización.” (Dussan Clavijo, 2006)

Para continuar, se deben definir algunos ámbitos conceptuales que se usan en la definición de las Políticas de Seguridad Informática:

- ✓ Seguridad de la red corporativa: configuración de los sistemas operativos, acceso lógico y remoto, autenticación, Internet, disciplina operativa, gestión de cambios, desarrollo de aplicaciones.
- ✓ Seguridad de usuarios: composición de claves, seguridad en estaciones de trabajo, formación y creación de conciencia.
- ✓ Seguridad de datos: criptografía, clasificación, privilegios, copias de seguridad y recuperación, antivirus, plan de contingencia.

- ✓ Auditoria de seguridad: análisis de riesgo, revisiones periódicas, visitas técnicas, monitoreo y auditoria.
- ✓ Aspectos legales: prácticas personales, contratos y acuerdos comerciales, leyes y reglamentación

2.2.8 Tipos de Ataques

Durante el paso del tiempo en especial en las últimas décadas, el avance y desarrollo tecnológico ha crecido de una manera exponencial. Conjuntamente, también ha crecido el conocimiento sobre cómo aprovechar las vulnerabilidades de los sistemas para hacerlos caer, o cambiarles el propósito para el cual están creados.

“Cada día son miles los virus informáticos que nacen y circulan a través de la red. Estos han sido creados con base en las debilidades de los sistemas, para atacar sus puntos vulnerables y aunque no todos los ataque informáticos se basan en ellos, es bueno conocer cuáles son los más utilizados, para actuar contra ellos”. (Urrego, 2013)

Ataque destinados a páginas y portales web

Las páginas web son el blanco ideal para atacantes por el hecho que son de dominio público y siempre se encuentran disponibles, basados en varios aspectos técnicos de los sitios que se encuentran en línea, se determinará de qué forma se pueden obtener el control parcial o total de este.

A continuación se detallan algunos de los principales tipos de ataques que pueden utilizarse para tal fin:

- ✓ **Cross Site Scripting (XSS):** “Los ataques de “Cross-Site Scripting” consisten básicamente en la ejecución de código “Script” (como Visual

Basic Script o Java Script) arbitrario en un navegador, en el contexto de seguridad de la conexión a un determinado servidor Web”. (Gómez Vieites, 2009)

- ✓ **Fuerza bruta:** “Tratan de explorar todo el espacio posible de claves para romper un sistema criptográfico.”(Gómez Vieites, 2009)
- ✓ **Inyección de código:** “Se produce cuando no se filtra de forma adecuada la información enviada por el usuario. Este tipo de ataque es independiente del sistema de bases de datos ya que depende únicamente de una inadecuada validación de los datos de entrada.”(Gómez Vieites, 2009)
- ✓ **Denegación del servicio (DOS):** “Consisten en distintas actuaciones que persiguen colapsar determinados equipos o redes informáticos, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios.”(Gómez Vieites, 2009)
- ✓ **Fuga de información:** “Consiste en dejar público el registro de errores, lo que facilita al atacante ver las fallas exactas del sistema.”(Urrego, 2013)
- ✓ **Ataques destinados a personas y usuarios de Internet:** Al igual que una persona del común que anda por la calle, entre el tráfico y la gente, cualquier usuario conectado a Internet está expuesto a riesgos de seguridad, y de él depende estar protegido y atento para no ser víctima de un ataque virtual. (Urrego, 2013)
- ✓ **Ingeniería social:** “El usuario podría ser engañado por una persona ajena a la organización para que le facilite sus contraseñas y claves de acceso.” (Gómez Vieites, 2009)
- ✓ **Análisis de tráfico:** “Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los “sniffers.” (Gómez Vieites, 2009)

Estos son algunos de los muchos tipos de ataques cibernéticos que existen, todos con los mismos objetivos: hacer caer los sistemas o usurpar la información buscando aquella que tenga valor y represente una ganancia para el atacante.

2.2.9 Zona Desmilitarizada

Es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red o como dice el autor:

La DMZ es la parte de la red de la empresa que se encuentra fuera del perímetro de seguridad. Cualquier cosa puede pasar aquí. Al colocar una máquina tal como un servidor web en la DMZ, las computadoras en Internet se pueden comunicar con ella para navegar por el sitio web de la empresa. (Tanenbaum & Wetherall, 2012)

La intención de una DMZ es la de asegurar que los servidores que son de acceso público no puedan comunicarse con otros segmentos de la red interna, en el caso de que un servidor se encuentre comprometido.

Debido a la naturaleza no-trivial de la implementación de DMZ, no se recomienda utilizar un DMZ salvo que tenga una gran familiaridad con las redes. Una DMZ no suele ser un requisito, pero en general es recomendada por los administradores conscientes de seguridad de la red. (TP-LINK, 2016)

2.2.10 Firewall

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos.

Los firewalls (servidores de seguridad) son simplemente una adaptación moderna de la vieja estrategia medieval de seguridad: excavar un foso defensivo profundo alrededor de su castillo. Este diseño obligaba a que todos

los que entraran o salieran del castillo pasaran a través de un único puente levadizo, en donde los encargados de la E/S los pudieran inspeccionar. En las redes es posible el mismo truco: una compañía puede tener muchas redes LAN conectadas de forma arbitraria, pero todo el tráfico que entra y sale de la compañía debe pasar a través de un puente levadizo electrónico (firewall). (Tanenbaum & Wetherall, 2012)

Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad. De hecho, los Firewalls no tienen nada que hacer contra técnicas como la Ingeniería Social y el ataque de Insiders. Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet). (Hernandez, 2000)

2.2.11 Virtualización

El mejor concepto para definir virtualización sería el siguiente:

La virtualización nos permite usar toda la capacidad de nuestros servidores durante el mayor tiempo posible. Así, podemos exprimir nuestros recursos de hardware sin gastar de más. Nos da la posibilidad de tener varios servidores en uno solo y, de este modo, compartir todos los recursos. (Marchionni, 2011)

La virtualización se puede aplicar a todo lo que tenga que ver con servidores, aplicaciones, almacenamiento y redes, es la manera más eficaz de reducir los costos y aumentar la eficiencia negocios de cualquier tamaño.

“La mayoría de los servidores funcionan a menos del 15 % de su capacidad. Gracias a la virtualización de servidor, se abordan estas ineficiencias mediante la

ejecución de varios sistemas operativos como máquinas virtuales en un único servidor físico.” (VmWare, 2016)

Como adicional las propiedades claves de las máquinas virtuales son:

- ✓ Puedes ejecutar varios sistemas operativos en una sola máquina.(VmWare, 2016)
- ✓ Los recursos se pueden dividir de acuerdo a cada máquina virtual.(VmWare, 2016)
- ✓ Aprovechamiento óptimo de los recursos de la máquina física.(VmWare, 2016)
- ✓ Aislamiento por fallas y seguridad a nivel hardware. (VmWare, 2016)
- ✓ Almacenamiento del estado completo de la máquina virtual en archivos. (VmWare, 2016)
- ✓ Se puede mover o copiar máquinas virtuales de una manera sencilla. (VmWare, 2016)
- ✓ Se puede migrar cualquier máquina virtual a cualquier servidor físico. (VmWare, 2016)

Virtualización de redes

La virtualización de redes es la reproducción completa de una red física en software. La virtualización de redes brinda dispositivos y servicios de red lógicos (es decir, puertos lógicos, switches, enrutadores, firewalls, balanceadores de carga, redes privadas virtuales [VPN, Virtual Private

Network] y mucho más) a las cargas de trabajo conectadas. Las redes virtuales ofrecen las mismas funciones y garantías que una red física, junto con las ventajas operacionales y la independencia de hardware propias de la virtualización. (VmWare, 2016)

Ventajas de la virtualización

- ✓ Reducción de los costos de capital y operacionales. (VmWare, 2016)
- ✓ Minimización o eliminación del tiempo fuera de servicio.(VmWare, 2016)
- ✓ Aumento de la capacidad de respuesta, la agilidad, la eficiencia y la productividad de TI. (VmWare, 2016)
- ✓ Aprovisionamiento de aplicaciones y recursos con mayor rapidez. (VmWare, 2016)
- ✓ Continuidad del negocio y recuperación ante desastres. (VmWare, 2016)
- ✓ Simplificación de la administración del centro de datos. (VmWare, 2016)
- ✓ Desarrollo de un verdadero centro de datos definido por software (VmWare, 2016)
- ✓ Entre otras cosas, la virtualización permite a las empresas pequeñas y medianas tener recursos adicionales en espera, y asignarlos según sea necesario.
- ✓ La utilización de tecnologías de virtualización facilita mucho las soluciones.
- ✓ Reduzca los tiempos y las tareas del aprovisionamiento.

2.3 DISEÑO DE LA PROPUESTA

2.3.1 Análisis de la Situación actual

Actualmente la Cooperativa de Ahorro y Crédito Visión Integral cuenta con una infraestructura de red básica, el direccionamiento IP no tiene ninguna segmentación, no existen bloqueos de puertos en los firewalls, no cuenta con servidor proxy por ende se tiene acceso libre a todo tipo de páginas en línea.

No cuenta con ningún tipo de servidor, los dispositivos de red son de capa 1 y 2, el cableado de la red es de UTP categoría 6a, los routers inalámbricos segmentan de cierta forma la red interna, pero siguen brindando acceso a la totalidad de la red.

Tomando en cuenta estos detalles, se considera que la red que maneja la empresa no brinda ningún tipo de seguridad porque está expuesta a una cantidad considerable de ataques cibernéticos.

Cabe recalcar que el direccionamiento IP es la básica 192.168.1.0 con máscara de red 255.255.255.0 y en ciertos tramos de la red se trabaja con 192.168.0.0 que es la dirección que por defecto usan los routers inalámbricos y que trabaja con DHCP.

Dirección IP	Máscara de Red	Puerta de Enlace
192.168.1.0	255.255.255.0	192.168.1.1

Tabla 1 Direccionamiento IP

De hecho, en una auditoría previa hecha por la Superintendencia de Economía Popular y Solidaria (SEPS), hizo un llamado de atención a la cooperativa por lo problemas antes mencionados.

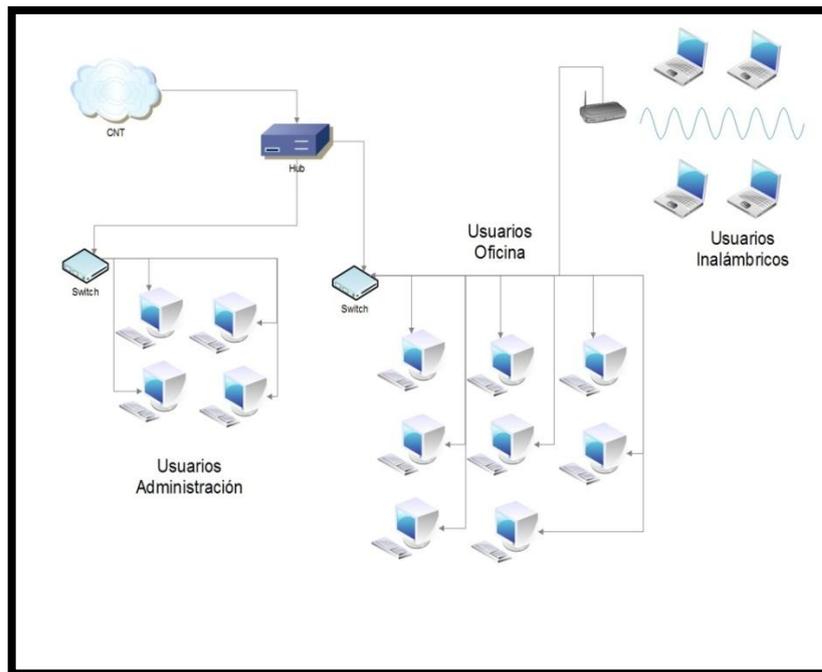


Figura 4 Diagrama de la Cooperativa de Ahorro y Crédito "Visión Integral"

2.3.2 Diseño de la solución

Como primer punto se iniciará una reestructuración completa de toda la infraestructura de comunicaciones, se reutilizarán algunos implementos de la red anterior como el cable utp 6a y los switches de capa 2 que se tienen disponibles, para asegurarla se diseñó un esquema que permite a esta expandirse tanto en servidores como en usuarios.

Se usará el direccionamiento IPV4 inicialmente pero también está contemplado el IPV6 por si se necesitara en algún momento migrar a esa tecnología.

Los servidores que darán servicios externos por el momento son 3 como propuesta inicial:

- Servidor WEB
- Servidor de Aplicaciones
- Servidor de Base de Datos

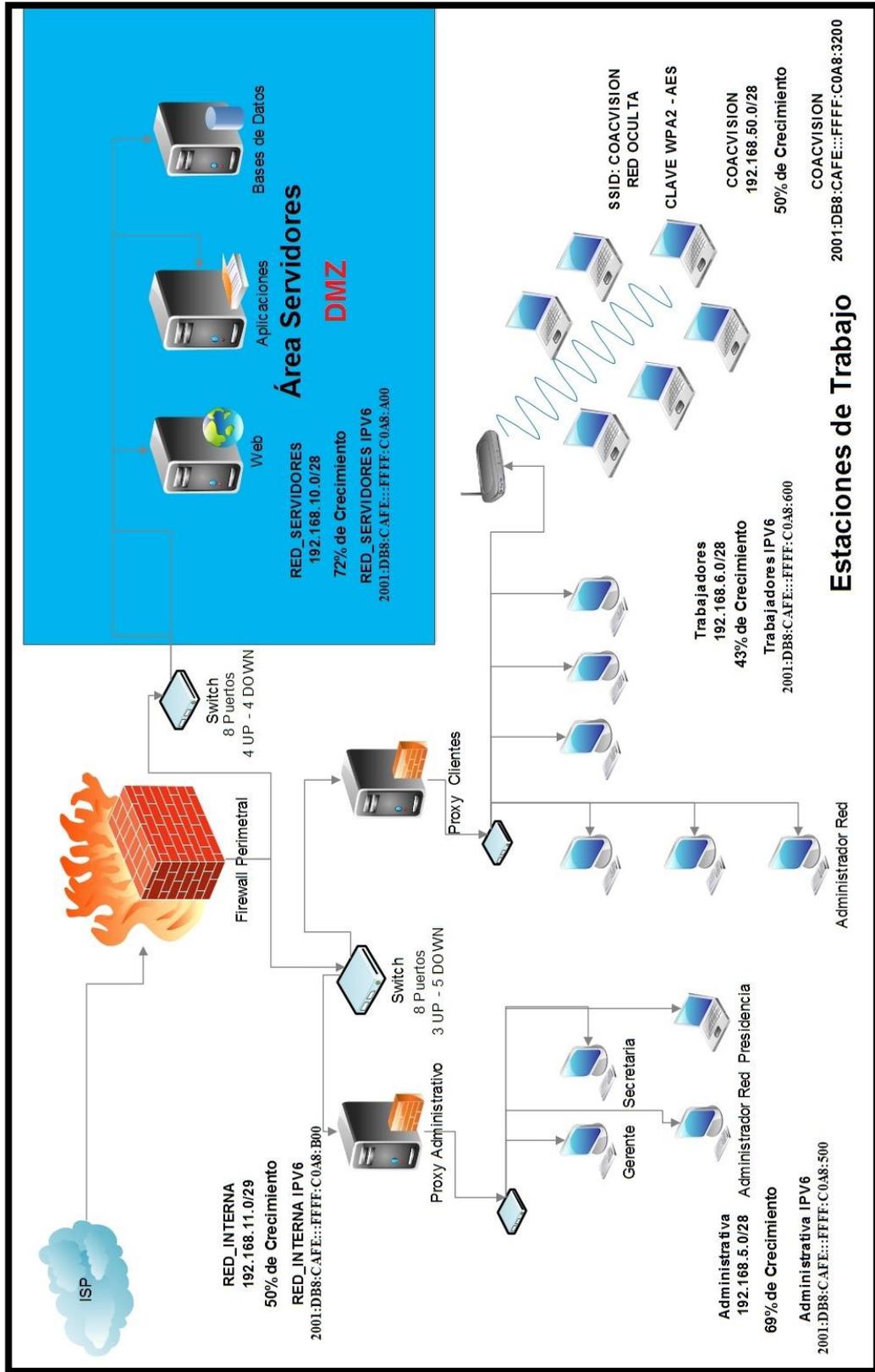


Figura 5 Diagrama de red propuesto

Direccionamiento IPV4

	Segmento Red	Máscara de Red	Puerta de Enlace
Red WAN	192.168.0.0	255.255.255.0	192.168.1.1
Red Servidores	192.168.10.0	255.255.255.240	192.168.10.1
Red Interna	192.168.11.0	255.255.255.248	192.168.11.1
Red Administrativa	192.168.5.0	255.255.255.240	192.168.5.14
Red Trabajadores	192.168.6.0	255.255.255.240	192.168.6.14
Wireless COACVISION	192.168.50.0	255.255.255.240	192.168.6.14

Tabla 2 Direccionamiento IPV4 de la nueva infraestructura de red

Direccionamiento IPV6

	Dirección Ipv6	Gateway IPV6
Red WAN	2001:DB8:CAFE:::FFFF:C0A8:0	2001:DB8:CAFE:::FFFF:C0A8:101
Red Servidores	2001:DB8:CAFE:::FFFF:C0A8:A00	2001:DB8:CAFE:::FFFF:C0A8:A01
Red Interna	2001:DB8:CAFE:::FFFF:C0A8:B00	2001:DB8:CAFE:::FFFF:C0A8:B01
Red Administrativa	2001:DB8:CAFE:::FFFF:C0A8:500	2001:DB8:CAFE::: FFFF:C0A8:050E
Red Trabajadores	2001:DB8:CAFE:::FFFF:C0A8:600	2001:DB8:CAFE::: FFFF:C0A8:060E
Wireless COACVISION	2001:DB8:CAFE:::FFFF:C0A8:3200	2001:DB8:CAFE::: FFFF:C0A8:060E

Tabla 3 Direccionamiento IPV6 de la nueva infraestructura de red

El firewall perimetral contiene 3 tarjetas de red las cuales gestionarán las conexiones tanto al área de servidores como a la red interna.

Este trabajará bajo el sistema operativo pfSense que ofrece grandes prestaciones para la gestión tanto de puertos como de conexiones.

Los puertos que estarán abiertos y que darán los servicios a la red son:

Puerto	Protocolo	Descripción	Estado
80	TCP	HTTPS Protocolo de Transferencia de HiperTexto	Abierto
8080	TCP	Tomcat lo usa como puerto por defecto.	Abierto
443	TCP	HTTPS/SSL usado para la transferencia segura de páginas web	Abierto
53	UDP	DNS Sistema de Nombres de Dominio	Abierto
1433	TCP	Microsoft SQL	Abierto
22	TCP	SSH, SFTP	Filtrado
3128	TCP	HTTP usado por web caches y por defecto en Squid cache	Abierto
21	TCP	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - control	Filtrado
ICMP	TCP	Ping, solo usado para pruebas de conexión	Filtrado

Tabla 4 Puertos TCP y UDP definidos en el estudio

Los demás puertos por motivos de seguridad estarán deshabilitados y se abrirán solo por motivos de pruebas como es el caso del puerto ICMP.

Cada segmento de red tiene un porcentaje de crecimiento de acuerdo a la cantidad de usuarios que soporta y que a futuro podría albergar.

	Host Actuales	% de Crecimiento	Host de crecimiento
Red Servidores	4	72 %	10
Red Interna	3	50 %	3
Red Administrativa	5	69 %	9
Red Trabajadores	8	43 %	6
Wireless COACVISION	7	50 %	7

Tabla 5 Porcentaje de crecimiento de las redes

Cada tarjeta de red hace una tarea distinta:

Red WAN:

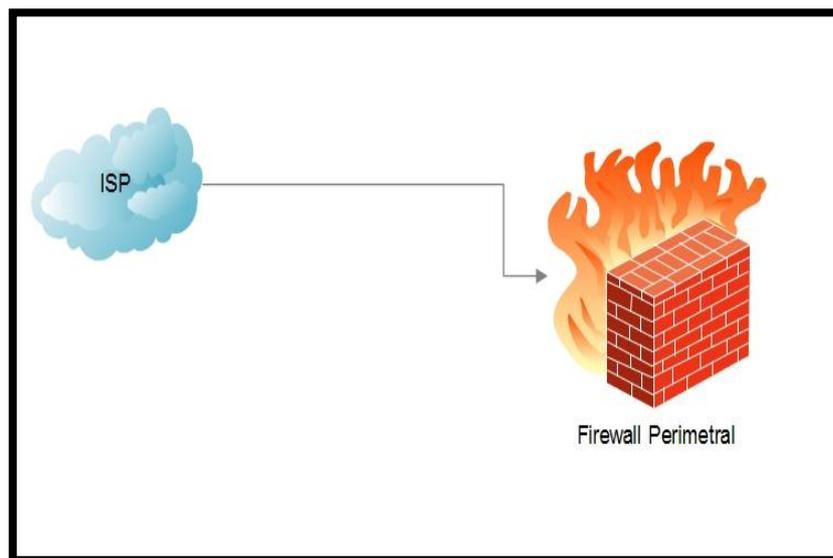


Figura 6 WAN

Esta interface es la encargada de proveer del servicio de internet a toda la red de la empresa, así mismo tiene la tarea de recibir las peticiones de usuarios externos a la página web y las aplicaciones de la misma.

Por ser la primera barrera de defensa de la red contra ataques y previo a un estudio minucioso se configura de tal manera que gestione únicamente peticiones

de ingreso al puerto 80 HTTP y 8080 de esta manera solo tendrá acceso a la navegación web y aplicaciones web bloqueando las conexiones vía FTP (21), ICMP (ping), SSH (22), entre otras.

Red SERVIDORES:

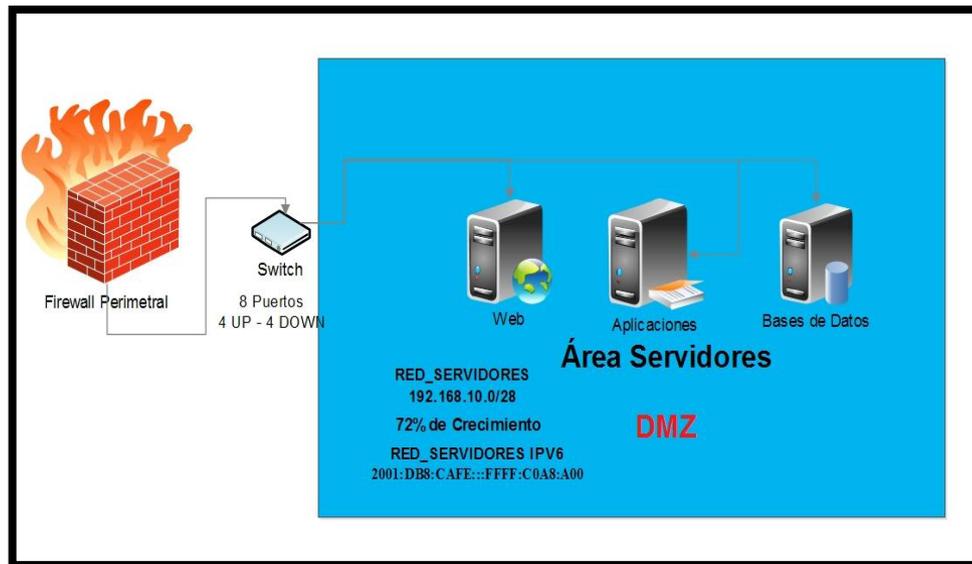


Figura 7 RED SERVIDORES

Esta interface es la encargada de proveer una conexión al área de servidores y recibir únicamente peticiones de conexión del puerto 80 y el 8080 desde la Red WAN a través de un NAT que se basa en la redirección de acuerdo al puerto que se utilice al momento de conectarse, por mantenimiento o configuraciones solo permite conexiones tipo FTP y SSH únicamente desde una IP fija ya establecida desde la Red INTERNA.

En conclusión desde el exterior se puede acceder exclusivamente a la página y a la aplicación web que tiene la empresa y desde las redes internas solo el administrador de red está en capacidad de gestionar los servidores por vía FTP o SSH debido a los permisos que se establecieron al momento de diseñar la nueva estructura de la red.

Esta red tiene la ventaja de que por su diseño se puede aumentar hasta un 72 % en la capacidad de servidores por si la empresa lo amerita en algún momento.

Red INTERNA:

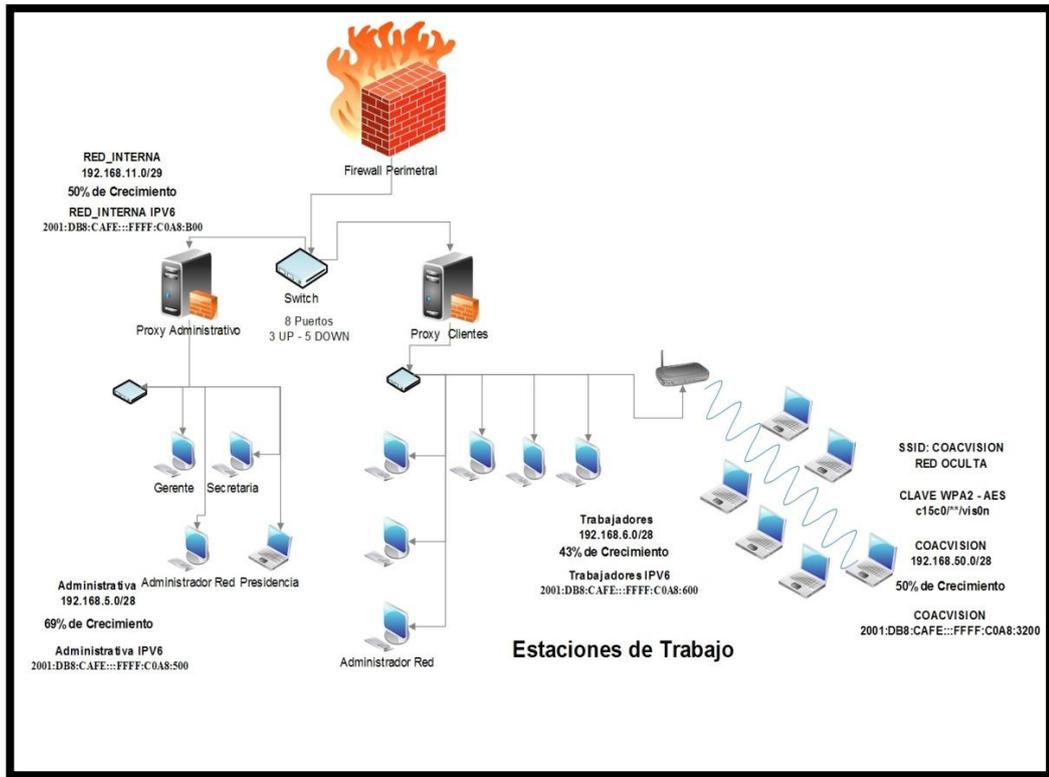


Figura 8 RED INTERNA

Esta interface es la encargada de dar el servicio de internet a la red corporativa permite las conexiones hacia la Red WAN al puerto 80 en salida y viceversa como configuración inicial.

Se toma en cuenta ciertos factores las peticiones de acceso a puertos irán aumentando dependiendo de los servicios que requiera la empresa.

La conexión hacia la Red SERVIDORES está permitida para navegar dentro de la página web es decir el puerto 80 y 8080, como se menciona anteriormente sólo se permitirá el acceso a los servidores para administrador de red, a través de una IP fija que se determina al momento de diseñar el nuevo esquema de la red.

Dentro la red interna se tendrá además dos proxys que tienen una función específica cada uno: el proxy administrativo y proxy usuarios:

El proxy administrativo tiene la función de bloquear conexiones remotas desde la red interna a la red de servidores y viceversa, y también realiza esta tarea desde la interface WAN a la red interna, se permite únicamente la navegación web pero con restricciones de acceso a ciertos sitios entre los cuales se destacan.

Sitios Restringidos
Pornografía
Descargas

Tabla 6 Sitios restringidos red administrativa

El proxy usuarios cumple con funciones similares que el proxy administrativo, la gran diferencia es que la navegación interna es más restringida los usuarios solo tienen acceso a una cantidad limitada de páginas que están destinadas solo a cuestiones netamente del trabajo.

Sitios Restringidos
Pornografía
Paginas Filtradas: Taringa, Laneros, etc.
Descargas (archivos .exe y flash)
Redes Sociales
Acceso a la administración web del proxy
Multimedia
Streaming Radio y Tv
Servidores de Descarga: Mega, 4Shared, etc.

Tabla 7 Sitios restringidos red trabajadores

2.3.3 Servidor Web

Se virtualizará el sistema operativo para implementar este servidor que es CentOS7 con el software Virtual Box por motivos de pruebas, su interfaz de red será red interna (intnet), la memoria a utilizar serán 2Gb y el disco duro a usar será de 20 Gb aproximadamente.

Ya en ambiente de producción utilizaremos una herramienta más robusta como es Proxmox, esta es la herramienta Open Source más utilizada en grandes empresas e instituciones públicas que tienen virtualizado sus servidores, no es solo una máquina virtual más, con una interfaz gráfica muy sencilla esta herramienta permite la migración en vivo de máquinas virtuales, clustering de servidores y backups automáticos.

Este servidor por estar basado en Red Hat brinda un excelente rendimiento, seguridad, escalabilidad y disponibilidad; y de hecho sus configuraciones son similares.

Este servidor se configuró para trabajar modo comando por la ventaja que es más seguro y consume menos recursos, posteriormente se instalaron algunos paquetes para que el servidor pueda soportar el alojamiento de Joomla el cual es un gestor de páginas web.

Se instalaron los siguientes paquetes PHP, Apache y MySQL.

Los pasos de la instalación y configuración del servidor web se encuentran en anexos 3.

2.3.4 Servidor Aplicaciones

Este servidor esta implementado en CentOS7 y se configuró para trabajar en modo comando por la ventaja que es más seguro y consume menos recursos,

posteriormente se instalaron algunos paquetes para que el servidor pueda soportar el alojamiento de aplicaciones.

Se usaron los siguientes paquetes Java en su versión 1.7.0 y Tomcat 8.

Este servidor y el servidor de base de datos están listos para soportar aplicaciones y bases de datos, pero por motivos de certificaciones de la SEPS, aún no se puede implementar, por lo que se va a mostrar es una aplicación de ejemplo hasta que se tenga el visto bueno y los servidores entren en producción.

Los pasos de la instalación y configuración del servidor de aplicaciones se encuentran en anexos 4.

2.3.5 Servidor Base de Datos

Este servidor esta implementado en Windows Server 2012 se configuró para trabajar en modo gráfico, se instaló SQL 2012 que el servidor pueda soportar base de datos.

Los pasos de la instalación y configuración del servidor de aplicaciones se encuentran en anexos 5.

2.3.6 Servidor Proxy

Existe una gran variedad de software en el mercado y en la web, que cumplen las funciones de ser firewall, router, proxy, etc. La elección del software a utilizar es una de las partes más complejas por algunas variables entre las cuales se destacan:

- Versatilidad
- Interfaz Intuitiva
- Uso de recursos del equipo

- Curva de aprendizaje
- Paquetes adicionales de instalación

Luego del análisis se determinó usar el proxy-firewall pfSense por las múltiples ventajas que ofrece.

Se destaca entre muchas cosas la capacidad de operar en máquinas con pocos recursos de hardware, la robustez y su fácil configuración que se ha ganado merecidamente una muy buena reputación dentro de los usuarios informáticos.

2.3.7 Instalación y configuración del firewall perimetral

La instalación de pfSense es sencilla, su punto más alto es el hecho de que puede ser utilizada en la mayoría de computadores con recursos mínimos de hardware, el manejo es intuitivo en muchas de sus funciones, es una poderosa herramienta en cuanto a seguridad se refiere, un pfSense bien administrado y con las reglas adecuadas puede brindar seguridad de calidad a organizaciones grandes.

```
FreeBSD/i386 (prince.development) (ttyv0)
*** Welcome to pfSense 2.1.5-RELEASE-pfSense (i386) on prince ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.56/24
RED_INTERNA (lan) -> em1      -> v4: 192.168.11.1/29
RED_SERVIDORES (opt1) -> em2      -> v4: 192.168.10.1/28

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults    12) pfSense Developer Shell
5) Reboot system              13) Upgrade from console
6) Halt system                14) Enable Secure Shell (sshd)
7) Ping host                  15) Restore recent configuration

Enter an option: █
```

Figura 9 Pantalla principal de pfSense

En esta instalación se trabajará con 3 tarjetas de red o interfaces que luego se

denominarán: WAN, RED_INTERNA, RED_SERVIDORES.

Cada una de estas interfaces tiene su respectiva IP y sus reglas definidas para cada uno de ellos.

Se virtualizará todos los servidores usando el software Virtual Box por motivo de pruebas y como regla básica de este proyecto hay que definir qué adaptador se usará para cada interfaz, en el caso del firewall perimetral se lo hará de la siguiente manera:

- ✓ WAN: Adaptador Puente

- ✓ RED_INTERNA: Red Interna (intnet)

- ✓ RED_SERVIDORES: Red Interna (intnet)

WAN usa el adaptador puente, usa el hardware físico de la máquina anfitriona para conectarse directamente a la red física, usando una IP diferente al host anfitrión pero que está dentro del mismo rango de red e identifica a la máquina virtual como una máquina física dentro de la red.

RED_INTERNA y RED_SERVIDORES usan el adaptador red interna (intnet), esta configuración lo que hace es crear una red interna virtual que permite conexión entre máquinas virtuales.

La memoria RAM a utilizar en esta implementación será de 512 Mb y el disco duro de 20 Gb.

Cada interfaz ya tiene definida la dirección IPV4 y la IPV6, estas se pueden apreciar en las tablas 2 y 3.

También se aprecia en la tabla 5 el crecimiento de cada una de las redes

propuestas de acuerdo a la segmentación de la misma, esto indica el límite de máquinas que se podrían tener dentro de cada una.

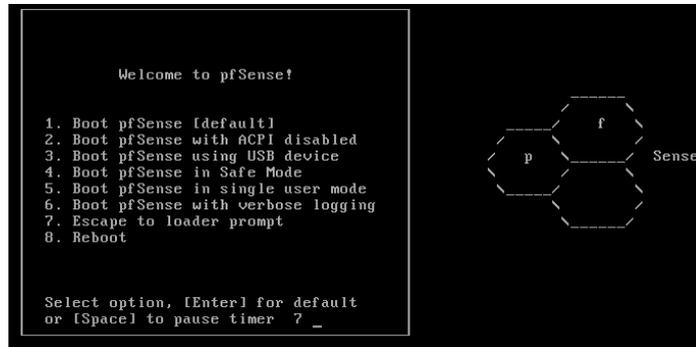


Figura 10 Inicio instalación de pfSense

Luego se digita 1 que permite hacer la instalación por defecto y posterior a eso la letra I, que muestra la siguiente pantalla.

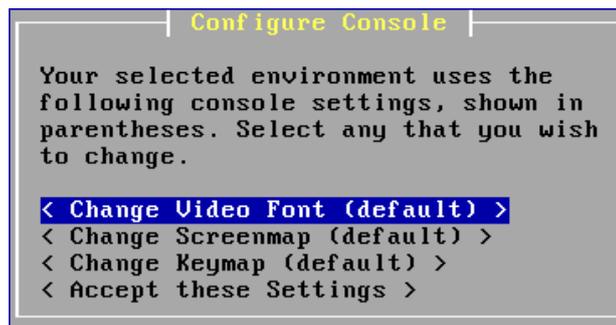


Figura 11 Instalación pfSense paso 1

Se da enter donde dice *Accept these Settings* y aparece lo siguiente.

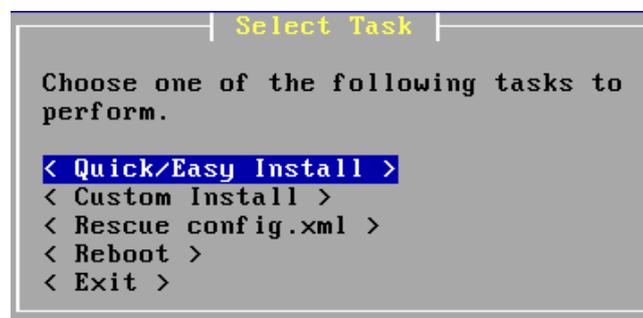


Figura 12 Instalación pfSense paso 2

Se selecciona OK y se continúa con la instalación.



Figura 13 Instalación pfSense paso 3

Se puede apreciar que inicia la instalación del sistema operativo.

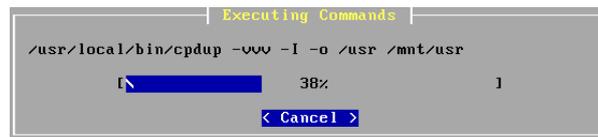


Figura 14 Instalación pfSense paso 4

Se escoge la opción *Standart Kernel*.

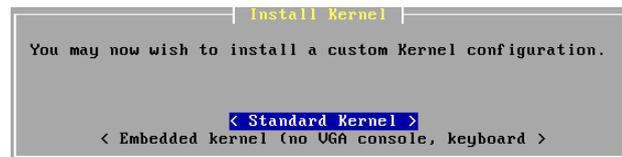


Figura 15 Instalación pfSense paso 5

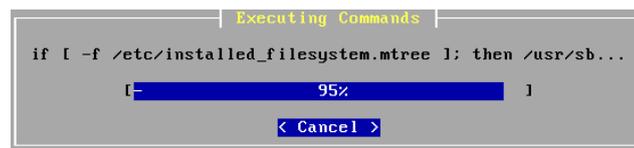


Figura 16 Instalación pfSense paso 6

Una vez concluido todo el proceso de instalación si no ha ocurrido ninguna novedad aparecerá la siguiente ventana y se selecciona *Reboot*.

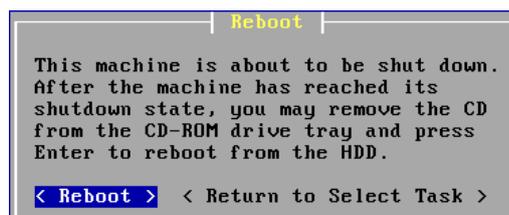


Figura 17 Culminación de la instalación de pfSense

```

pfSense is now rebooting

After the reboot is complete, open a web browser and
enter https://192.168.1.1 (or the LAN IP Address) in the
location bar.

You might need to acknowledge the HTTPS certificate if
your browser reports it as untrusted. This is normal
as a self-signed certificate is used by default.

*DEFAULT Username*: admin
*DEFAULT Password*: pfsense

Rebooting in 5 seconds. CTRL-C to abort.
Rebooting in 4 seconds. CTRL-C to abort.
Rebooting in 3 seconds. CTRL-C to abort.

```

Figura 18 Reiniciando la máquina virtual

Luego de culminar el proceso de instalación y haber reiniciado la máquina virtual aparece el siguiente mensaje.

```

Default interfaces not found -- Running interface assignment option.
Valid interfaces are:
em0  08:00:27:87:f0:2e  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6
em1  08:00:27:8a:be:c1  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6
em2  08:00:27:3d:94:ab  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.
Do you want to set up VLANs now [y/n]?

```

Figura 19 Interfaces del firewall perimetral

Aparecen 3 interfaces de red, las mismas que fueron definidas al inicio, y ahora tienen los nombres de em0, em1 y em2; las que luego tendrán los nombres de WAN, RED_INTERNA, RED_SERVIDORES en ese orden.

```

em1  08:00:27:8a:be:c1  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6
em2  08:00:27:3d:94:ab  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.
Do you want to set up VLANs now [y/n]? n

*NOTE*  pfSense requires *AT LEAST* 1 assigned interface(s) to function.
        If you do not have *AT LEAST* 1 interfaces you CANNOT continue.

        If you do not have at least 1 *REAL* network interface card(s)
        or one interface with multiple VLANs then pfSense
        *WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.
Enter the WAN interface name or 'a' for auto-detection:

```

Figura 20 Asignar tarjeta de red a interfaz WAN

Las interfaces em0 a WAN, em1 a RED_INTERNA y em2 a RED_SERVIDORES, se agregan las direcciones IP a cada una de las interfaces usando la opción 2.

```
0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults  12) pfSense Developer Shell
5) Reboot system             13) Upgrade from console
6) Halt system               14) Enable Secure Shell (sshd)
7) Ping host                  15) Restore recent configuration

Enter an option: 2

Available interfaces:
1 - WAN (em0 - dhcp)
2 - RED_INTERNA (em1 - static)
3 - RED_SERVIDORES (em2 - static)

Enter the number of the interface you wish to configure: █
```

Figura 21 Configuraciones IP firewall perimetral

Se selecciona la tarjeta de red a configurar, se sugieren algunas cosas tales como si se desea usar redes virtuales, ser configurado por un servidor DHCP externo o ser una interfaz de red estática, en este caso WAN permitirá que el servidor externo de DHCP le otorgue una IP; RED_INTERNA y RED_SERVIDORES tendrán una IP fija con una máscara de red definida ya anteriormente, habiendo hecho todas las configuraciones, el firewall perimetral quedaría de esta manera.

```
Message from syslogd@prince at Oct 17 22:07:38 ...
prince php: /index.php: Successful login for user 'admin' from: 192.168.11.2

FreeBSD/i386 (prince.development) (ttyv0)

*** Welcome to pfSense 2.1.5-RELEASE-pfSense (i386) on prince ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.56/24
RED_INTERNA (lan) -> em1      -> v4: 192.168.11.1/29
RED_SERVIDORES (opt1) -> em2      -> v4: 192.168.10.1/28

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults  12) pfSense Developer Shell
5) Reboot system             13) Upgrade from console
6) Halt system               14) Enable Secure Shell (sshd)
7) Ping host                  15) Restore recent configuration

Enter an option: █
```

Figura 22 Firewall perimetral con sus interfaces configuradas

Como se aprecia en la imagen la WAN tiene una IP que puede variar, mientras que RED_INTERNA y RED_SERVIDORES tienen direcciones fijas, a este punto ya tenemos el firewall perimetral debidamente instalado.

2.3.8 Configuración y reglas del firewall

Existen dos formas de trabajar con un firewall:

- ✓ La primera es tener todos los puertos abiertos y se van cerrando los que no se va a usar.
- ✓ La segunda es empezar con todos los puertos cerrados y solo se abren los que se necesitan.

PfSense puede trabajar de ambas formas, pero la segunda forma es la mejor y la más recomendada para trabajar como un firewall, se tiene en cuenta que solo se usarán los puertos que se necesitan y el resto estarán cerrados.

En el caso de esta solución en el área de servidores se tiene un servidor web que administra la página web de la COACVI y un servidor de aplicaciones basado en Tomcat los que serán los únicos que terceras personas pueden ver de la organización, entonces lo primero que se va a hacer es permitir que desde la interfaz WAN recibir peticiones únicamente del puerto 80 y 8080 que son los puertos con los que se va a trabajar, la configuración de esta regla quedaría así:

Firewall: NAT: Port Forward ?

Port Forward **1:1** Outbound NPT

	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	8080	192.168.10.3	8080	NAT	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.10.2	80 (HTTP)	Nat	

pass
 linked rule

Figura 23 Reglas de la interfaz WAN firewall perimetral, pfSense

Como se aprecia la regla es la siguiente:

- ✓ WAN TCP ** WAN address 8080 192.168.10.3 8080

- ✓ WAN TCP ** WAN address 80 (HTTP) 192.168.10.2 80 (HTTP)

Se trabaja con el protocolo IPV4 y se permite conexiones desde cualquier destino a cualquier puerto eso no se puede controlar, pero al momento de entrar a la IP pública solo aceptara peticiones de conexión a los puertos 80 y 8080 que apuntarán a las direcciones de cada servidor 192.168.10.2 que es la dirección del servidor web puerto 80 y 192.168.10.3 que es la dirección del servidor de aplicaciones web puerto 8080.

Esta regla del NAT: Port Forward que tiene la interface WAN redirecciona las peticiones de conexión hacia el servidor web y servidor de aplicaciones; por ejemplo si en un navegador web ajeno a la institución y con acceso a internet se escribe www.coacvisionintegral.com el navegador busca la IP pública y el Port Forward al fijarse que es una petición de puerto 80 redirecciona automáticamente al servidor web.

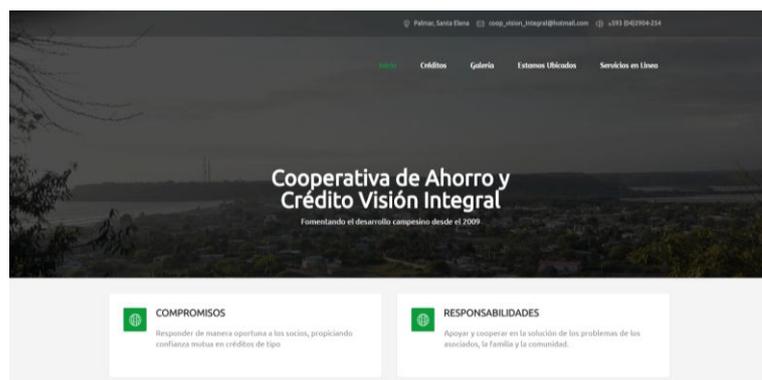


Figura 24 Página web de la cooperativa

Si en el mismo navegador web se digita www.coacvisionintegral.com:8080 o en su defecto en la página web se selecciona la opción *Servicios en Línea*, el Port Forward al fijarse que es una petición de puerto 8080 redirecciona automáticamente al servidor de aplicaciones.

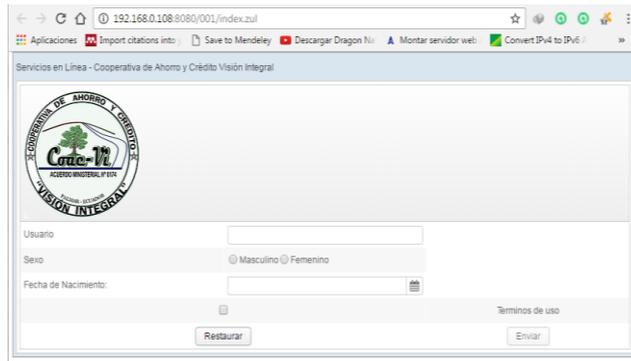


Figura 25 Aplicación web de la cooperativa, formulario de ejemplo

La configuración hecha permite la interacción entre la IP pública que está asignada a la interface WAN con la IP de servidor web y el servidor de aplicación, el resultado de implementar estas reglas es ya tener acceso a la página web y a la aplicación de la COACVI desde cualquier dispositivo que tenga una conexión a internet.

Se prosigue con la configuración de la RED_SERVIDORES que tiene el segmento de red 192.168.10.0/24; en esta se va a permitir conexiones solo del puerto 80, 8080 y del puerto 22 para administración remota del servidor web.

Se crea una regla que permite conexiones de todo tipo a cualquier puerto esta regla tiene como fin hacer pruebas y de dar mantenimiento a la red es caso hubiera algún error.

Un dato adicional de esta configuración es que la última regla permite conexión vía SSH a toda la RED_SERVIDORES desde la RED_INTERNA.

Firewall: Rules

Rules for interface: **RED_SERVIDORES**

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
1	IPv4 *	*	*	*	*	*	none		
2	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Conexiones Internet
3	IPv4 TCP	RED_INTERNA net	22 (SSH)	*	22 (SSH)	*	none		Bloqueo Conexiones Remotas
4	IPv4 TCP	*	*	*	8080	*	none		
5	IPv4 TCP	RED_INTERNA net	8080	*	8080	*	none		

Figura 26 Reglas de interface RED_SERVIDORES, pfsense

Continuando con la configuración de RED_INTERNA que tiene el segmento de red 192.168.11.0/24, esta red es la encargada del trabajo más “pesado”, por el hecho que es la que mayor cantidad de reglas tiene dentro de este estudio porque contiene todos los usuarios de la red.

Firewall: Rules 🔍 🔄 📄 ?

Floating WAN **RED_INTERNA** RED_SERVIDORES

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	*	*	RED_INTERNA Address	80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	IPv4 *	*	*	*	*	*	none		
<input checked="" type="checkbox"/>	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Puerto 80 Internet
<input checked="" type="checkbox"/>	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		Puerto DNS
<input checked="" type="checkbox"/>	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Navegacion Segura Internet
<input checked="" type="checkbox"/>	IPv4 *	192.168.11.3	*	*	*	*	none		Exepcion de Regla

Figura 27 Reglas de la interface RED_INTERNA, pfSense

Cada regla tiene una función específica, la principal es proveer de internet a toda la empresa y esto se logra con tres reglas que trabajan de manera conjunta:

- ✓ La primera es la IPV4 TCP * * * 80 (HTTP), esta permite acceso al puerto 80 para navegación web normal.
- ✓ La segunda es la IPV4 TCP/UDP * * * 53 (DNS), este permite la resolución de nombres para la navegación web.
- ✓ La tercera es la IPV4 TCP * * * 443 (HTTPS), esta permite la navegación segura, en la actualidad existen muchas páginas que usan este protocolo.

Con estas tres reglas definidas se tiene acceso a navegación web a toda la red, la última regla permite la administración de los servidores desde una IP definida en otra red.

La RED_INTERNA tiene 2 divisiones que se las denomina Administrativo con el segmento de red 192.168.5.0/28 y Usuarios con el segmento de red 192.168.6.0/28; para cada división se ha configurado un proxy basado también en pfSense que administrará el acceso a la navegación web y que también tendrá reglas de firewall para acceder a ciertas partes de la red de la empresa que es dominio del administrador de red.

2.3.9 Proxy Administrativo

El proxy administrativo está encargado de proveer servicios al área administrativa tales como el acceso a ciertas páginas de internet y el bloqueo de puertos.

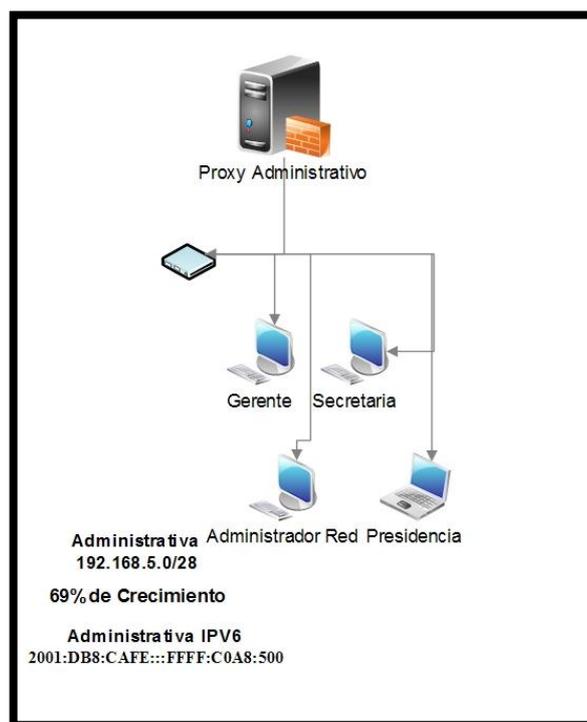


Figura 28 Esquema proxy administrativo

Proxy al igual que todos los de este proyecto esta virtualizado pero una de sus interfaces de red ya sale a la red física, entonces esto quedaría de la siguiente forma:

- ✓ La interface em0 o WAN esta Red Interna (intnet)

- ✓ La interface em1 o LAN como Adaptador Puente

```
FreeBSD/i386 (proxy.localdomain) (ttyv0)
*** Welcome to pfSense 2.1.5-RELEASE-pfSense (i386) on proxy ***

WAN (wan)      -> em0      -> v4: 192.168.11.2/29
LAN (lan)      -> em1      -> v4: 192.168.5.14/28

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults   12) pfSense Developer Shell
5) Reboot system              13) Upgrade from console
6) Halt system                 14) Enable Secure Shell (sshd)
7) Ping host                   15) Restore recent configuration

Enter an option: |
```

Figura 29 Proxy Administrativo

La instalación, asignación de interface y su respectiva dirección IP ya fueron tema tratado con anterioridad así que en este apartado se irá directamente a la configuración del proxy.

El proxy administrativo como ya se mencionó tiene 2 tarjetas de red con una IP fija respectivamente que son:

- ✓ 192.168.11.2: está conectada a la red virtual y que será la interface WAN
- ✓ 192.168.5.14: está conectada a la red física y que será la interface LAN

Con estos datos se procede a la configuración de reglas, la instalación de Squid y SquidGuard que controlarán la navegación de los usuarios de la red.

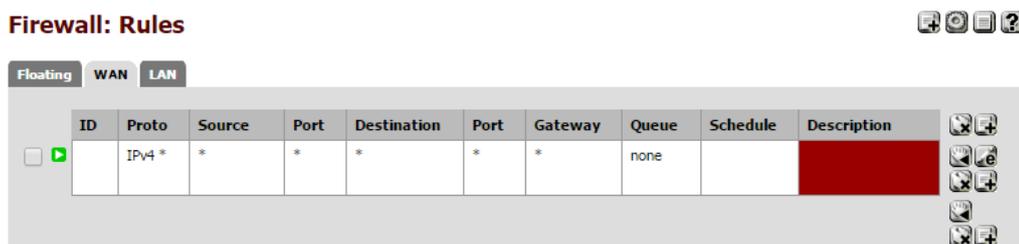


Figura 30 Reglas interface WAN proxy Administrativo, pfSense

La regla asignada para la interface WAN permite el libre tráfico de información dentro de la RED_INTERNA.

Firewall: Rules

Floating | WAN | LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
▶	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
▶	IPv4 *	*	*	*	*	*	none		DNS
▶	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Navegacion WEB
▶	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Navegacion WEB SEGURA

Figura 31 Reglas interface LAN proxy Administrativo, pfSense

En el caso de la interface LAN se tienen tres reglas de salida ya utilizadas anteriormente que permiten la navegación web, lo nuevo en esta parte será la instalación y configuración de Squid que es un proxy, su función principal es la de bloquea páginas por su dirección web y luego se tiene SquidGuard que es un bloqueador de contenido.

2.3.9.1 Instalación de Squid proxy Administrativo y proxy Usuarios

- ✓ Se inicia instalando el paquete Squid desde el menú System – Packages

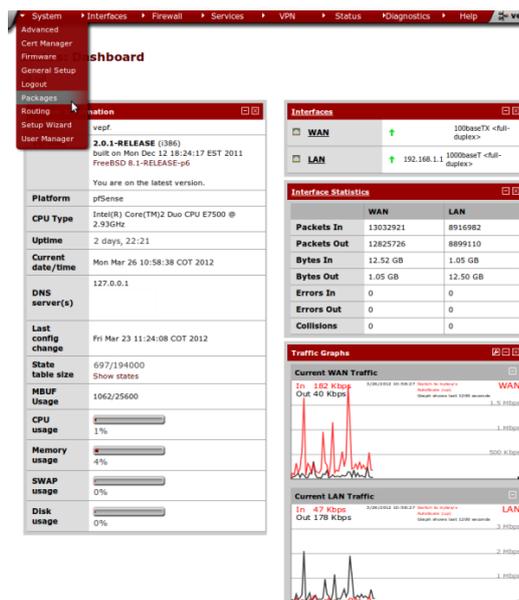


Figura 32 Instalación Squid paso 1, ("Squid en pfSense," 2012)

- ✓ Se busca Squid en la pestaña que se llama "Available Packages"

System: Package Manager

Available Packages | Installed Packages

Package Name	Category	Status	Package Info	Description
Asterisk	Services	Beta 1.8.8.1 pkg v 0.1 platform: 2.0	Package Info	Asterisk is an open source framework for building communications applications. Asterisk turns an ordinary computer into a communications server.
anyterm	Diagnostics	BETA 0.5 platform: 1.2.3	Package Info	Ajax Interactive Shell - Have you ever wanted SSH or telnet access to your system from an internet desk? - from behind a speed firewall, from an internet cafe, or even from a mobile phone? Anyterm is a combination of a web page and a process that runs on your web server that provides this access. WARNING! We suggest using Stunnel in combination with this package!
Avahi	Network Management	ALPHA 0.6.25_2 platform: 1.2.3	Package Info	Avahi is a system which facilitates service discovery on a local network. This means that you can plug your laptop or computer into a network and instantly be able to view other people who you can chat with, find printers to print to or find files being shared. This kind of technology is already found in Apple MacOS X (branded Rendezvous, Bonjour and sometimes Zeroconf) and is very convenient. Avahi is mainly based on Lennart Poettering's Flexmdns mDNS implementation for Linux, which has been discontinued in favour of Avahi.
AutoConfigBackup	Services	Stable 1.19 platform: 1.2	Package Info	Automatically backs up your pfSense configuration. All contents are encrypted on the server. Requires pfSense Premium Support Portal Subscription from https://portal.pfsense.org
arping	Services	Stable 2.00.1 platform: 1.0.1	Package Info	Broadcasts a who-has ARP packet on the network and prints answers.
arpwatch	Security	ALPHA 2.1.414.4 platform: 2.0	No info, check the forum	Arpwatch monitors ethernet/ip address changes. It also logs certain changes to syslog.
Backup	System	Beta 0.1.5 check the platform: 1.2	No info, check the forum	Tool to Backup and Restore files and directories.
bandwidthd	System	BETA 2.0.1.3 platform: 1.2.1	No info, check the forum	BandwidthD tracks usage of TCP/IP network subnets and builds html files with graphs to display utilization. Charts are built by individual IPs, and by default display utilization over 2 day, 8 day, 40 day, and 400 day periods. Furthermore, each ip address's utilization can be logged out at intervals of 3.3 minutes, 10 minutes, 1 hour or 12 hours in csv format, or to a backed database server. HTTP, TCP, UDP, ICMP, VPN, and P2P traffic are color coded.

Figura 33 Instalación Squid paso2, ("Squid en pfsense," 2012)

- ✓ Se instala dándole click al botón + a la derecha de su descripción, luego de esto se espera mientras instala todo el paquete.

System: Package Manager: Install Package

Available packages | Installed packages | Package Installer

```

Installing squid and its dependencies.
Beginning package installation for squid...
Downloading package configuration file... done.
Saving updated package information... done.
Downloading squid and its dependencies...
Checking for package installation...
Downloading http://files.pfsense.org/packages/8/all/squid-2.7.9_1.tbz ...
(extracting)
Downloading http://files.pfsense.org/packages/8/all/cyrus-sasl-2.1.25_1.tbz
... (extracting)
Downloading http://files.pfsense.org/packages/8/all/openldap-client-
2.4.26.tbz ... (extracting)
Downloading http://files.pfsense.org/packages/8/all/perl-5.12.4_3.tbz ... 17%
  
```

Figura 34 Instalación de Squid paso 3, ("Squid en pfsense," 2012)

- ✓ Concluida la instalación de Squid y luego de verificar que la instalación haya sido correcta se prosigue a la configuración de Squid dando click en "Services - Proxy server"

Proxy server: General settings



General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Proxy interface
The interface(s) the proxy server will bind to.

Allow users on interface
If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.

Transparent proxy
If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy server without any additional configuration necessary.

Bypass proxy for Private Address Space (RFC 1918) destination
Do not forward traffic to Private Address Space (RFC 1918) destination through the proxy server but directly through the firewall.

Bypass proxy for these source IPs
Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but directly through the firewall. Separate by semi-colons (;). [Applies only to transparent mode]

Bypass proxy for these destination IPs
Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. Separate by semi-colons (;). [Applies only to transparent mode]

Enable logging
This will enable the access log. Don't switch this on if you don't have much disk space left.

Log store directory
The directory where the log will be stored (note: do not end with a / mark)

Log rotate
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Proxy port
This is the port the proxy server will listen on.

ICP port
This is the port the Proxy Server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Visible hostname
This is the URL to be displayed in proxy server error messages.

Figura 35 Configuración de Squid ajustes generales

En la pestaña “General” se habilitan algunos cambios.

- ✓ Proxy Interface: LAN, que será la red intervenida.
- ✓ Seleccionamos Allow users on interface.
- ✓ Seleccionamos Transparent Proxy, para no usar configuraciones adicionales en los usuarios finales esto en la red Administrativa, en la red Usuarios deshabilitamos esta opción por motivos de administración.
- ✓ Enabled logging, para registrar el acceso a páginas.
- ✓ Log Store Directory: /var/squid/logs viene por defecto.
- ✓ Proxy Port: 3128.
- ✓ Administrator email: *email del administrador*.

- ✓ Language: Spanish.

Al final se da click en save.

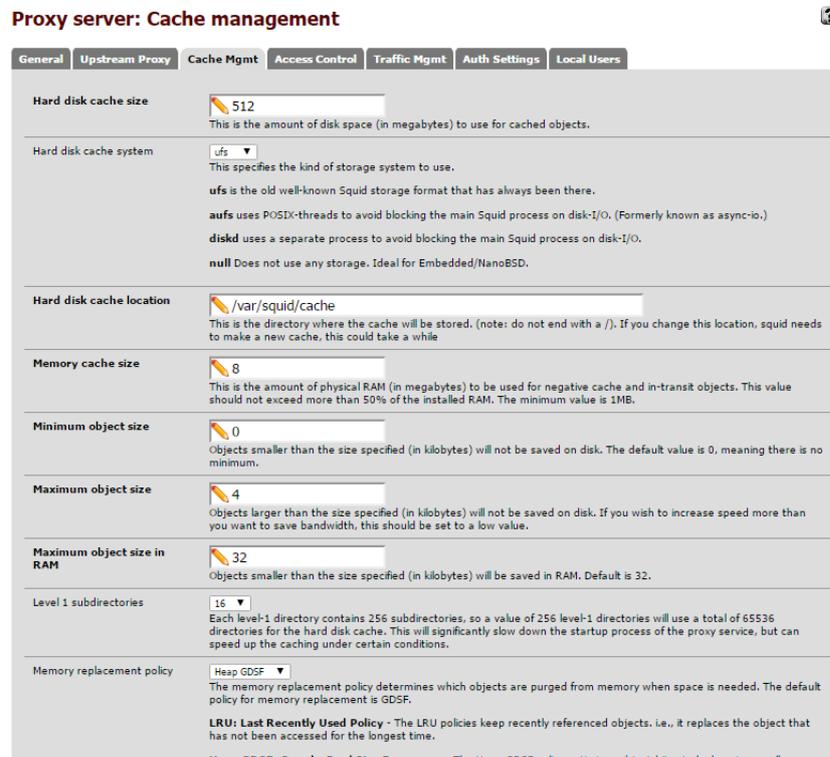


Figura 36 Configuración Squid administración de cache

En la pestaña "Cache Mgmt" se realizan cambios de este tipo.

- ✓ Hard disk cache size: 512, se hace el cambio para aumentar la capacidad de almacenamiento

El resto se deja tal como está, a continuación se da click en save y para finalizar la configuración se va a la pestaña "Access Control" y se hace lo siguiente:

- ✓ Allowed subnets, ponemos el segmento de la red en este caso 192.168.5.0/28 para red Administrativa y 192.168.6.0/28 para red Usuarios
- ✓ En Blacklist, se ingresa los sitios web a los que no se permitirá acceso.

Proxy server: Access control



General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Allowed subnets
192.168.5.0/28
Enter each subnet on a new line that is allowed to use the proxy. The subnets must be expressed as CIDR ranges (e.g.: 192.168.1.0/24). Note that the proxy interface subnet is already an allowed subnet. All the other subnets won't be able to use the proxy.

Unrestricted IPs
Enter each unrestricted IP address on a new line that is not to be filtered out by the other access control directives set in this page.

Banned host addresses
Enter each IP address on a new line that is not to be allowed to use the proxy.

Whitelist
Enter each destination domain on a new line that will be accessible to the users that are allowed to use the proxy. You also can use regular expressions.

Blacklist
www.youporn.com
www.redtube.com
Enter each destination domain on a new line that will be blocked to the users that are allowed to use the proxy. You also can use regular expressions.

External Cache-Managers
Enter the IPs for the external Cache Managers to be allowed here, separated by semi-colons (;).

Figura 37 Configuración de Squid control de acceso red Administrativo

Proxy server: Access control



General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Allowed subnets
192.168.6.0/28
Enter each subnet on a new line that is allowed to use the proxy. The subnets must be expressed as CIDR ranges (e.g.: 192.168.1.0/24). Note that the proxy interface subnet is already an allowed subnet. All the other subnets won't be able to use the proxy.

Unrestricted IPs
Enter each unrestricted IP address on a new line that is not to be filtered out by the other access control directives set in this page.

Banned host addresses
Enter each IP address on a new line that is not to be allowed to use the proxy.

Whitelist
Enter each destination domain on a new line that will be accessible to the users that are allowed to use the proxy. You also can use regular expressions.

Blacklist
.youporn.com
.redtube.com
.cinecalidad.com
.facebook.com
31.13.73.36
Enter each destination domain on a new line that will be blocked to the users that are allowed to use the proxy. You also can use regular expressions.

External Cache-Managers
Enter the IPs for the external Cache Managers to be allowed here, separated by semi-colons (;).

acl safeports

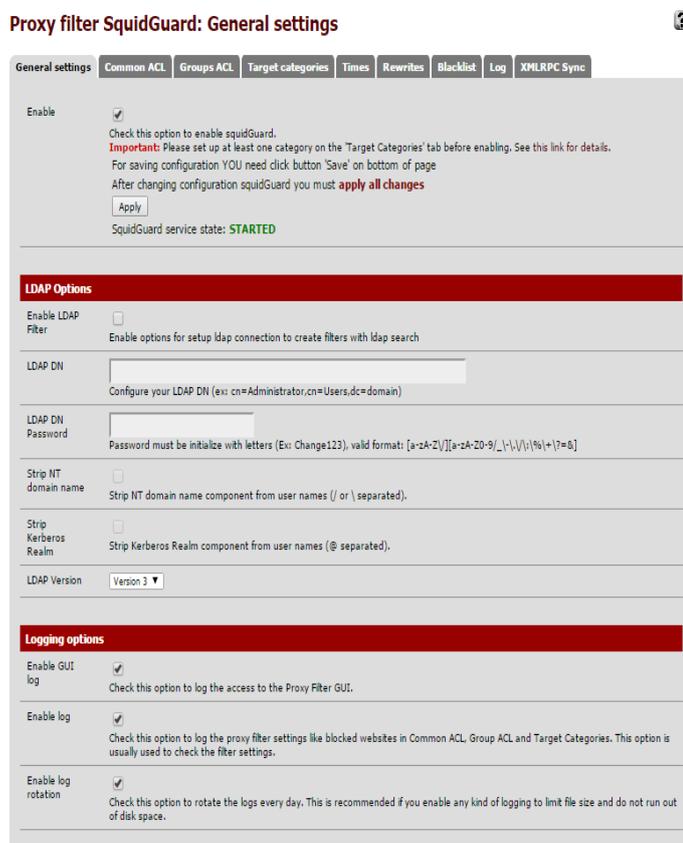
Figura 38 Configuración de Squid control de acceso red Usuarios

2.3.9.2 Instalación de SquidGuard proxy Administrativo y proxy Usuarios

Para una oficina, siempre es bueno tener la posibilidad de filtrar páginas por contenido, este es el propósito de SquidGuard; los primero pasos son idénticos a la instalación de Squid así que solo se detallarán paso a paso.

- ✓ Primero se instala el paquete SquidGuard desde el menú System – Packages.
- ✓ Se instala dándole click al botón + a la derecha de su descripción, luego de esto se espera mientras instala todo el paquete.
- ✓ Luego entramos a Services - Proxy filter.

En este punto las configuraciones que se realizarán son nuevas.



The screenshot displays the 'Proxy filter SquidGuard: General settings' configuration page. At the top, there are several tabs: 'General settings', 'Common ACL', 'Groups ACL', 'Target categories', 'Times', 'Rewrites', 'Blacklist', 'Log', and 'XMLRPC Sync'. The 'General settings' tab is active. Below the tabs, there is a section for enabling SquidGuard. The 'Enable' checkbox is checked. A note states: 'Check this option to enable squidGuard. Important: Please set up at least one category on the Target Categories' tab before enabling. See this link for details. For saving configuration YOU need click button 'Save' on bottom of page. After changing configuration squidGuard you must apply all changes'. Below this note is an 'Apply' button and the status 'SquidGuard service state: STARTED'. The next section is 'LDAP Options', which includes: 'Enable LDAP Filter' (checkbox unchecked), 'LDAP DN' (input field with placeholder 'Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)'), 'LDAP DN Password' (input field with placeholder 'Password must be initialize with letters (Ex: Change123), valid format: [a-zA-Z][a-zA-Z0-9_!@#%&*~\.\-|/]{7=8}'), 'Strip NT domain name' (checkbox unchecked), 'Strip Kerberos Realm' (checkbox unchecked), and 'LDAP Version' (dropdown menu set to 'Version 3'). The final section is 'Logging options', which includes: 'Enable GUI log' (checkbox checked), 'Enable log' (checkbox checked), and 'Enable log rotation' (checkbox checked).

Figura 39 Configuración SquidGuard ajustes generales

- ✓ Lo primero que se hará será activar SquidGuard activando la casilla de enable.
- ✓ Se activan todas las opciones de Logging options, para tener registros de ingresos.

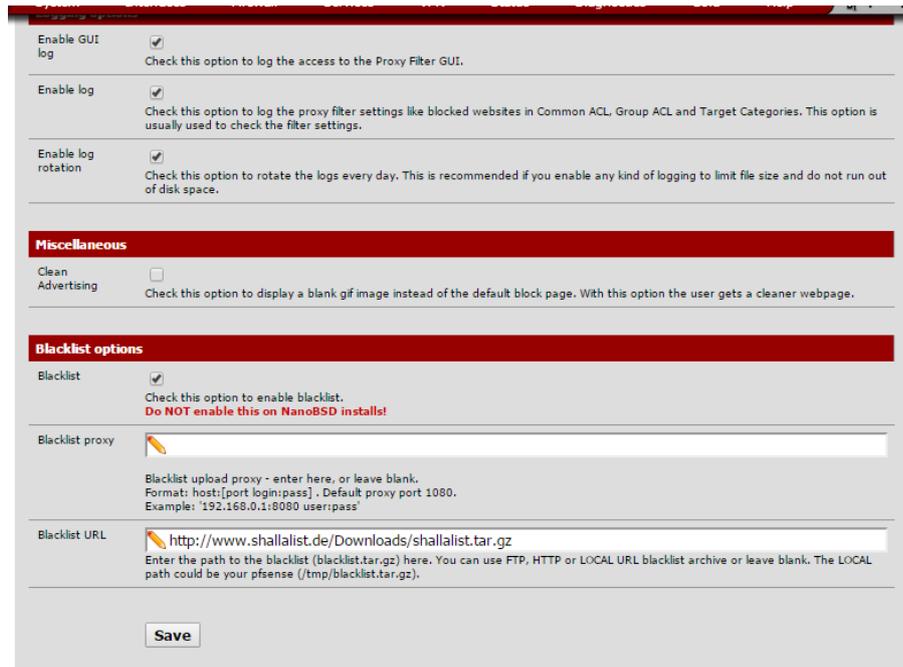


Figura 40 Configuración SquidGuard ajustes generales

- ✓ En la sección Blacklist option se activa Blacklist y a continuación se ingresa en Blacklist URL la siguiente dirección <http://www.shallalist.de/Downloads/shallalist.tar.gz>, que permite el bloqueo de contenido específico.

Click en save para guardar la configuración y se continua a la pestaña Blacklist.

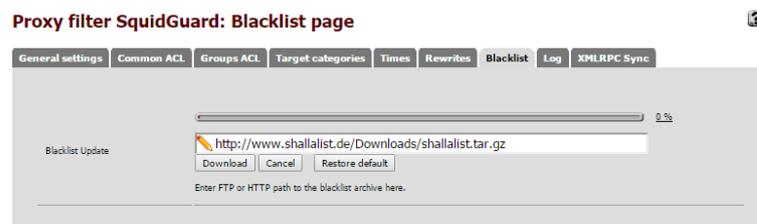


Figura 41 Descarga del paquete Shallalist para bloquear contenido web

- ✓ Se da click en download y se espera a que se complete la descarga.
- ✓ Se ingresa a la pestaña Common ACL.
- ✓ Click en target rules, esta opción es la permitire filtrar las paginas por contenido y ayudara a la administración de la navegación de todos los usuarios.

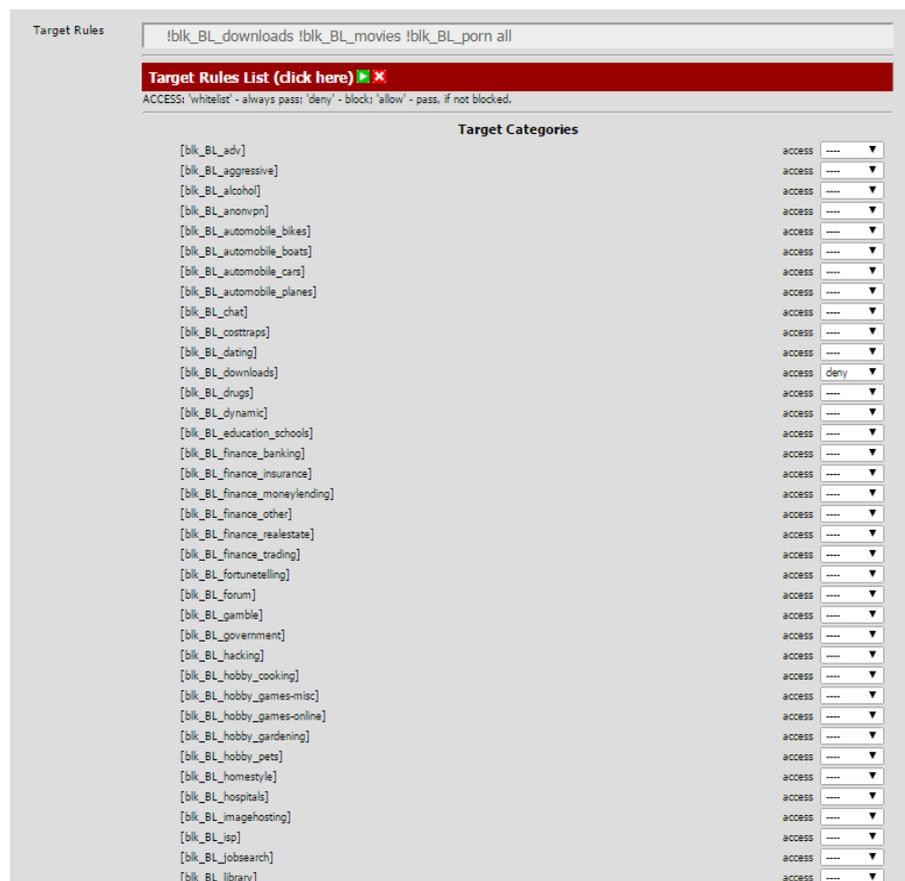


Figura 42 Bloqueo de sitios por su contenido en SquidGuard

Como se ve existe gran variedad de tópicos de contenido a escoger los cuales por defecto ya vienen con el acceso permitido y lo que se hace es denegar ciertas funciones tales como:

- ✓ Descargas.
- ✓ Acceso a pornografía.

- ✓ Acceso a música

- ✓ Acceso a películas online

The screenshot shows the SquidGuard configuration page with the following settings:

- A list of content categories with their access levels:

[blk_BL_tracker]	access	----	▼
[blk_BL_updatedates]	access	----	▼
[blk_BL_urlshortener]	access	----	▼
[blk_BL_violence]	access	----	▼
[blk_BL_warez]	access	----	▼
[blk_BL_weapons]	access	----	▼
[blk_BL_webmail]	access	----	▼
[blk_BL_webphone]	access	----	▼
[blk_BL_webradio]	access	----	▼
[blk_BL_webtv]	access	----	▼
Default access [all]	access	allow	▼
- Do not allow IP-Addresses in URL:** (unchecked). Description: To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.
- Proxy Denied Error:** Text input field containing "Request denied by Sg[product_name] proxy". Description: The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by Sg[product_name] proxy".
- Redirect mode:** Dropdown menu set to "int error page (enter error message)". Description: Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not be accessible. Options: ext url err page, ext url redirect, ext url as 'move', ext url as 'found'.
- Redirect info:** Text input field. Description: Enter external redirection URL, error message or size (bytes) here.
- Use SafeSearch engine:** (unchecked). Description: To protect your children from adult content you can use the protected mode of search engines. At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search and Bing. Make sure that the search engines can be accessed. It is recommended to prohibit access to others. **Note:** This option overrides 'Rewrite' setting.
- Rewrite:** Dropdown menu set to "none (rewrite not defined)". Description: Enter the rewrite condition name for this rule or leave it blank.
- Log:** (checked). Description: Check this option to enable logging for this ACL.

A "Save" button is located at the bottom of the configuration area.

Figura 43 Bloqueo de sitios por su contenido en SquidGuard

Para la demás opciones se dejará tal como está y al final de la lista en la opción Default Access se pone allow que permite acceso a lo demás.

Se habilita la opción log y se guarda la configuración con save.

Como se usa un proxy transparente no se necesita usar ninguna otra configuración dentro del navegador web, puesto que el proxy hace todo el trabajo.

En el caso de la red Usuarios se denegarán más funciones tales como:

- ✓ Descargas.

- ✓ Acceso a pornografía.
- ✓ Acceso a música.
- ✓ Acceso a películas online.
- ✓ Noticias.
- ✓ Política.
- ✓ Educación Sexual.
- ✓ Radio online.
- ✓ TV online

2.3.10 Proxy Usuarios

El proxy usuarios está encargado de proveer servicios al área de usuarios tales como el acceso a ciertas páginas de internet y el bloqueo de puertos.

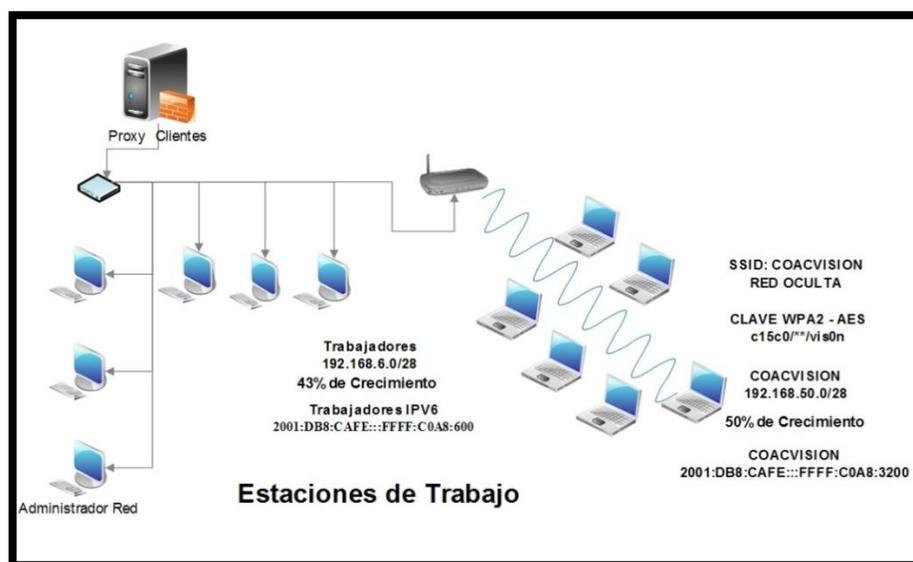


Figura 44 Esquema proxy usuarios

Este proxy al igual que todos los de este proyecto esta virtualizado pero una de sus interfaces de red ya sale a la red física, entonces esto quedaría de esta manera:

- ✓ La interface em0 o WAN esta Red Interna (intnet)
- ✓ La interface em1 o LAN como Adaptador Puente

```
FreeBSD/i386 (prince.developmen) (ttyv0)
*** Welcome to pfSense 2.1.5-RELEASE-pfSense (i386) on prince ***

WAN (wan)      -> em0      -> v4: 192.168.11.3/29
LAN (lan)      -> em1      -> v4: 192.168.6.14/28

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults  12) pfSense Developer Shell
5) Reboot system              13) Upgrade from console
6) Halt system                 14) Enable Secure Shell (sshd)
7) Ping host                   15) Restore recent configuration

Enter an option: █
```

Figura 45 Proxy usuarios

Se pasará directamente a la configuración del proxy.

El proxy usuarios como ya se menciona tiene 2 tarjetas de red con una IP fija respectivamente que son:

- ✓ 192.168.11.3: está conectada a la red virtual y que será la interface WAN.
- ✓ 192.168.6.14: está conectada a la red física y que será la interface LAN.

Con estos datos se procede a la configuración de reglas, la instalación de Squid y SquidGuard que controlarán la navegación de los usuarios de la red.



Figura 46 Reglas interface WAN proxy usuarios

La regla asignada para la interface WAN permite el libre tráfico de información dentro de la RED_INTERNA.

Firewall: Rules

Floating WAN LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	IPv4 *	*	*	*	*	*	none		
<input checked="" type="checkbox"/>	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		DNS
<input checked="" type="checkbox"/>	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Navegacion WEB
<input checked="" type="checkbox"/>	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Navegacion WEB SEGURA
<input type="checkbox"/>	IPv4 TCP	LAN address	*	LAN address	443 (HTTPS)	*	none		Bloqueo
<input checked="" type="checkbox"/>	IPv4 *	192.168.6.2	*	*	*	*	none		Administrador
<input checked="" type="checkbox"/>	IPv4 TCP	192.168.6.0/28	*	192.168.6.0/28	*	*	none		Permite el correcto trabajo del proxy

Figura 47 Reglas interface LAN proxy usuarios

En el caso de la interface LAN existen tres reglas de salida ya utilizadas anteriormente que permiten la navegación web, una regla de excepción para el administrador de red:

✓ IPV4 * 192.168.6.2 * * * *

Esta regla nos da acceso total a todos los puertos de toda la red y si se retrocede un poco hasta las configuraciones del firewall perimetral en donde previamente se dejado establecido permisos para manipular todos los puertos de una IP determinada en este momento todo se concatena y da una regla de acceso total al administrador de red.

✓ IPV4 TCP 192.168.6.0/28 * 192.168.6.0/28 * *

La regla da acceso a todos los puertos que se pudieran utilizar pero únicamente dentro del rango de red establecido, esto permite usar cualquier puerto posible para configurar el proxy a los terminales que estarán dentro de la red con el fin de bloquear las redes sociales por el hecho de que un proxy transparente no está en posibilidad de hacerlo.

Y para finalizar dentro de los usuarios se abre el centro de recursos y de redes, opciones de internet, conexiones y se hace lo siguiente.

En conexiones se selecciona configuración LAN y luego usar servidor proxy para la LAN se pone la dirección de la puerta de enlace 192.168.6.14 y el puerto 3128.

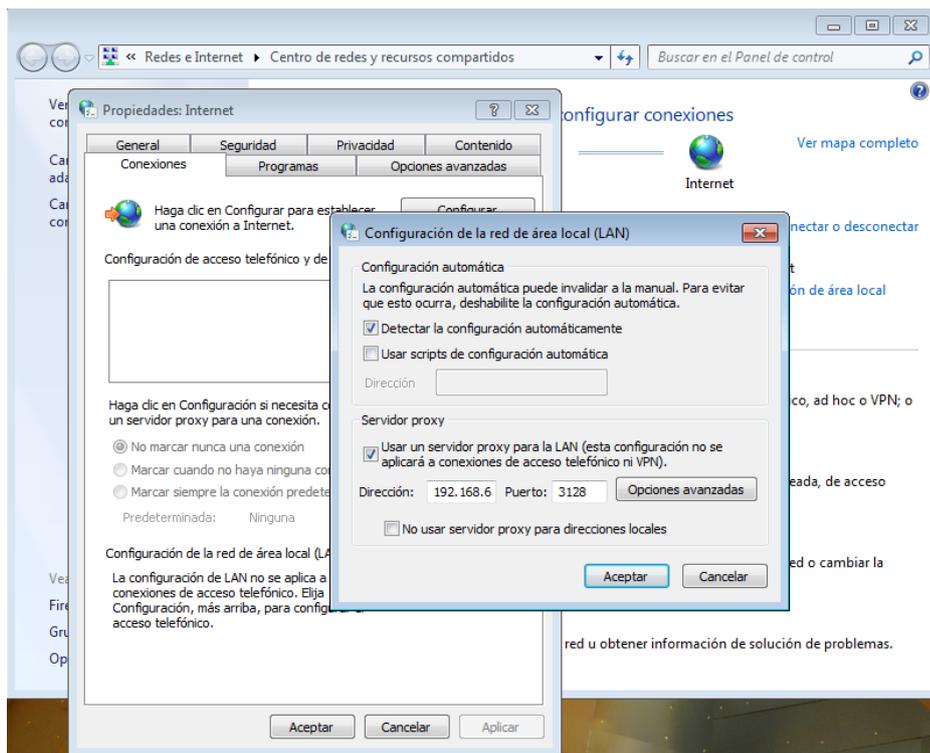


Figura 48 Configuración de Windows para trabajar con el proxy usuarios

Con esto se finaliza el aseguramiento de toda la red de la Cooperativa de Ahorro y Crédito “Visión Integral”.

Adicionalmente se pueden bloquear la configuración de área local para que ningún usuario de la red realice cambios.

Se hace lo siguiente Inicio->Ejecutar->gpedit.msc

Buscamos "Deshabilitar el cambio de configuración proxy" y se lo pone en habilitado en las directivas de la Configuración de Equipo -> Plantillas Administrativas -> Componentes de Windows -> Internet Explorer

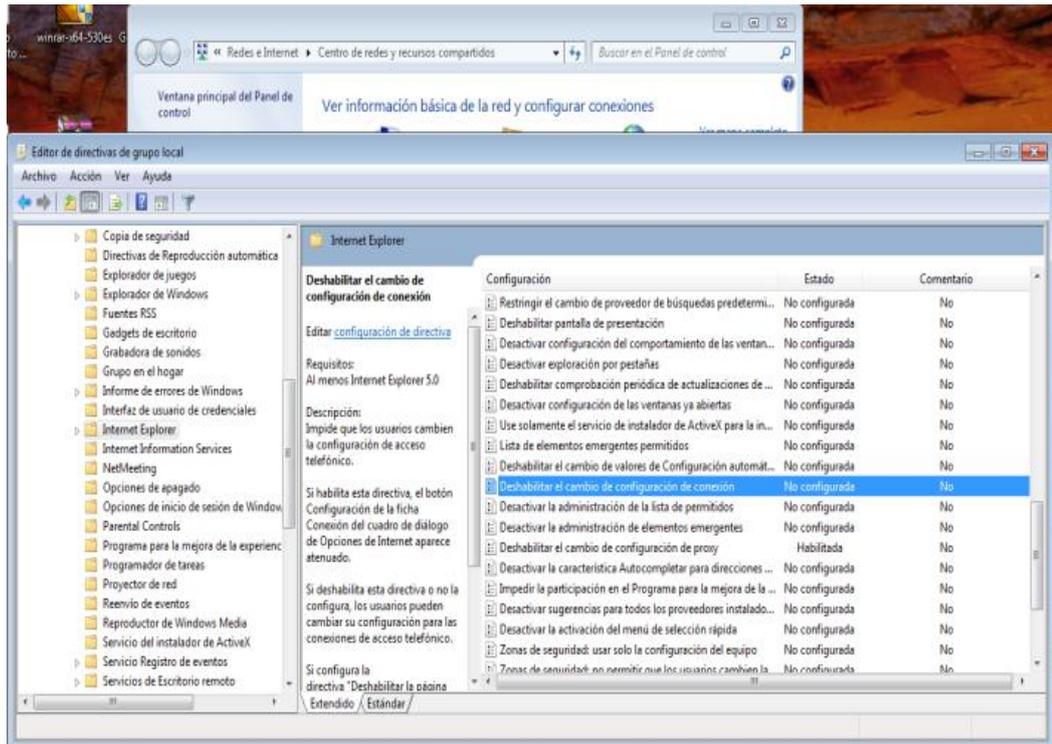


Figura 49 Bloqueo de configuración de las opciones de internet

Una vez hecho esto el resultado será el siguiente.

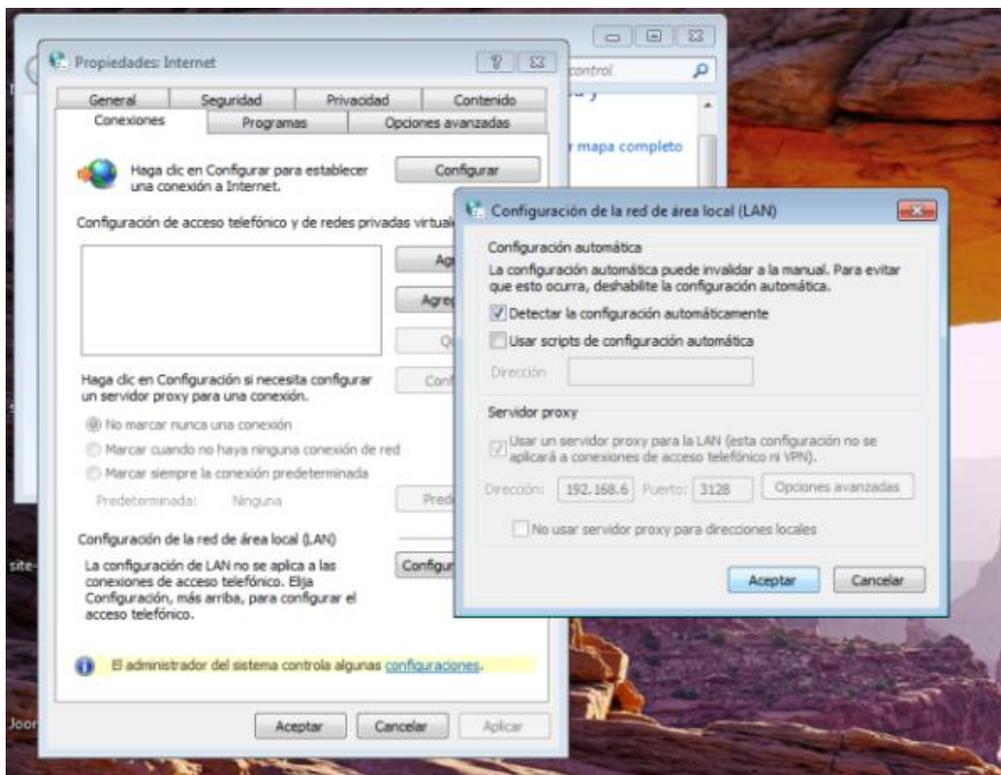


Figura 50 Opciones de internet bloqueadas

2.4 ESTUDIO DE FACTIBILIDAD

2.4.1 Factibilidad Técnica

El estudio es posible gracias a que la mayoría de las herramientas que se proponen son de distribución libre, lo que a su vez ofrece una amplia gama de opciones a utilizar.

Para el Servidor WEB se utilizará CentOS7 como el sistema operativo base, Apache y MySQL como la plataforma que va a soportar la página web y Joomla como el gestor de la página.

Para el Servidor de Aplicaciones se utilizará CentOS7 como el sistema operativo base, Java 1.7.0 y Tomcat 8 como plataforma para las aplicaciones web.

Para el Servidor de Bases de Datos se utilizará Windows Server 2012 como el sistema operativo base y SQL SERVER 2012 como gestor de base de datos.

El Firewall perimetral y los proxys que se proponen serán implementados con el sistema operativo BSD y su distribución llamada PfSense, esta distribución integra herramientas las mismas que hacen que esta distribución trabaje de distintas maneras destacando su uso como proxy, firewall, servidor DHCP, etc.

Gran parte del hardware utilizado para la implementación de este proyecto será con los recursos con los que ya cuenta la empresa, pero dentro de este estudio se hará proyecciones a futuro sobre que equipos son necesarios para tener una infraestructura acorde con lo que la empresa necesita.

El diseño que se utilizó para el aseguramiento de este sistema de comunicaciones permite el crecimiento tanto en los servidores que darán servicios a nivel web como de los usuarios que tendrá la red internamente.

El proyecto es factible operacionalmente debido a que la administración del firewall y de los proxys es de manera web y se puede acceder desde cualquier navegador que tenga el administrador, siempre y cuando se encuentre dentro de red.

2.4.2 Factibilidad Económica

En esta factibilidad se especifica los recursos tanto de hardware como de software y sus costos respectivos para la ejecución del proyecto, los materiales de oficina, el personal y también los gastos de servicios básicos.

Cantidad	Descripción	Uso	Precio Unitario	Precio final
1	Laptop Asus ROG 74SX	Simulación	\$ 1650.00	\$1.650,00
1	Impresora Epson L365 con sistema de tinta continua	Documentación	\$ 350.00	\$ 365,00
2	Servidor Hp Proliant D1380 Gen9 Xeon E5-2640V3 16GB ram Modelo 803420-005	Servidores de virtualización	\$ 5350.00	\$ 10.700,00
1	Switch Cisco Smb S1m2024t Admin. L2 De 24 Puertos Gigabit + 2 puertos de Fibra Optica	Conexión entre servidor de virtualización y servidor espejo	\$740,00	\$740,00
1	Cpu Intel Core I3-4170-3.7 4ta Gene. 1000gb 4gb	Respaldo Servidor	\$356,00	\$356,00

1	Disco duro externo 2TB	Respaldo Externo	\$125,00	\$125,00
6	Disco Duro Hp 1.2tb 10k Sas 2.5 Hotplug 6g 718292-001 G8 G9	Array de Datos Servidores	\$937,00	\$5.622,00
2	Fuente De Poder Servidor Hp G6 G7 750w	Fuente Redundante	\$337,00	\$674,00
1	Patch Panel Categoría 6 Cat6 24 Puertos Con Jacks Para Rack	Conexiones Físicas	\$35,00	\$35,00
1	Gabinete Rack Cerrado De Pared	Alojamiento de los Servidores	\$250,00	\$250,00
1	Ups Tripp-lite 1.5 Kva 1500va Omniv1500 940w Usb Lan	Sistema de alimentación ininterrumpida de energía	\$300,00	\$300,00
Total				\$ 20.817,00

Tabla 8 Costo de hardware

Descripción	Costo	Cantidad	Total
CENTOS7	\$ 0.00	1	\$ 0.00
pfSense	\$ 0.00	3	\$ 0.00
W. Server 2012	\$ 1.400,00	1	\$ 1.400,00
SQL Licencia	\$ 950,00	1	\$ 950,00
Total			\$ 2.350,00

Tabla 9 Costos de software

Descripción	Costo/mes	Meses	Total
Analista Networking	\$800,00	2	\$ 1.600,00
Asesor de implementación servidores	\$1.000,00	1	\$ 1.000,00
Total			\$ 2.600,00

Tabla 10 Costo del personal

Descripción	Costo	Cantidad	Total
Resma de papel	\$ 5,00	2	\$ 10,00
Tinta Epson	\$ 18,00	2	\$ 36,00
Total			\$ 46,00

Tabla 11 Costo de materiales de oficina

Descripción	Costo/Mes	Meses	Total
Internet	\$ 50,00	6	\$ 300,00
Energía Eléctrica	\$ 48,00	6	\$ 288,00
Total			\$ 588,00

Tabla 12 Costos servicios básicos

Descripción	Costo/Mes	Meses	Total
Transporte	\$ 100,00	6	\$ 600,00
Alimentación	\$ 30,00	6	\$ 180,00
Total			\$ 780,00

Tabla 13 Costos movilización y alimentación

Descripción	Precio	Cantidad	Total
Instalación Servidores	\$ 1.800,00	2	\$ 3.600,00
Total			\$ 3.600,00

Tabla 14 Costos de implementación

Descripción	Costos
Hardware	\$ 20.817,00
Software	\$ 2.350,00
Costos de personal	\$ 2.600,00
Materiales de oficina	\$ 46,00
Servicios básicos	\$ 588,00
Movilización y alimentación	\$ 780,00
Costos implementación	\$ 3.600,00
Total	\$ 30.781,00

Tabla 15 Costo del proyecto

El costo de implementación del aseguramiento de la infraestructura de comunicaciones de la Cooperativa de Ahorro y Crédito “Visión Integral” es de \$ 30.781,00

Como se aprecia en las tablas anteriores, para ejecutar este proyecto se necesitaría una inversión de \$30.781,00, la misma que desglosan los gastos hardware, software, personal, materiales de oficina, servicios básicos, movilización alimentación e implementación.

El costo del hardware es determinado por la persona que está encargada de desarrollar todo el proyecto previo a un estudio ya realizado con anterioridad de que es lo que necesita la empresa estos datos los encuentra en la Tabla 8.

Se utilizarán herramientas basadas en software libre y licenciadas en consecuencia el gasto de licenciamiento para este proyecto tienen un costo que se detalla en la Tabla 9.

Los costos de análisis, materiales de oficina, servicios básicos, movilización, alimentación e implementación serán solventados por el desarrollador del proyecto.

La COACVI tiene un cuarto que está destinado exclusivamente para ubicar toda la infraestructura de comunicaciones, así también cuenta con un aire acondicionado destinado a mantener los servidores a una temperatura de operación adecuada.

Se reutilizarán los switches de capa 2, gestionan el tráfico de red de manera óptima y porque su tecnología es 10/100/1000 Mbps, los routers inalámbricos para la red WIFI de la empresa y todo el cableado de red que es UTP categoría 6a.

El costo del personal y la implementación es asumido por el desarrollador del proyecto, en consecuencia la inversión que haría la empresa para este proyecto es la compra de todo el hardware y software que se recomendó en la Tabla 8 y 9.

Luego de haber elaborado el análisis de factor económico del proyecto, se logra indicar que es factible económicamente debido a que la empresa solo invertirá en equipos y en 2 licencias (SQL 2012 y Windows Server 2012), que aunque su precio es elevado nos garantizan un tiempo de vida útil superior a los 5 años y ayudara a subir de categoría en el ranking nacional de cooperativas que emite la SEPS.

2.4.3 VAN y TIR

	Ingresos Trimestrales	Egresos Trimestrales	total
1	\$6.300,00	\$5.100,00	\$1.200,00
2	\$7.000,00	\$4.200,00	\$2.800,00
3	\$8.500,00	\$3.800,00	\$4.700,00
4	\$9.000,00	\$4.000,00	\$5.000,00
TOTAL PRIMER AÑO			\$13.700,00

Tabla 16 Ingresos primer año

	Ingresos Trimestrales	Egresos Trimestrales	Total
1	\$6.500,00	\$4.000,00	\$2.500,00
2	\$7.800,00	\$4.000,00	\$3.800,00
3	\$9.200,00	\$4.000,00	\$5.200,00
4	\$9.600,00	\$4.000,00	\$5.600,00
TOTAL SEGUNDO AÑO			\$17.100,00

Tabla 17 Ingresos segundo año

	Ingresos Trimestrales	Egresos Trimestrales	Total
1	\$6.800,00	\$4.000,00	\$2.800,00
2	\$7.900,00	\$4.000,00	\$3.900,00
3	\$8.800,00	\$4.000,00	\$4.800,00
4	\$9.900,00	\$4.000,00	\$5.900,00
TOTAL TERCER AÑO			\$17.400,00

Tabla 18 Ingresos tercer año

	Ingresos Trimestrales	Egresos Trimestrales	Total
1	\$7.800,00	\$4.000,00	\$3.800,00
2	\$8.200,00	\$4.000,00	\$4.200,00
3	\$8.900,00	\$4.000,00	\$4.900,00
4	\$10.000,00	\$4.000,00	\$6.000,00
TOTAL CUARTO AÑO			\$18.900,00

Tabla 19 Ingresos cuarto año

	Ingresos Trimestrales	Egresos Trimestrales	Total
1	\$8.300,00	\$4.000,00	\$4.300,00
2	\$8.600,00	\$4.000,00	\$4.600,00
3	\$9.500,00	\$4.000,00	\$5.500,00
4	\$10.450,00	\$4.000,00	\$6.450,00
TOTAL QUINTO AÑO			\$20.850,00

Tabla 20 Ingresos quinto año

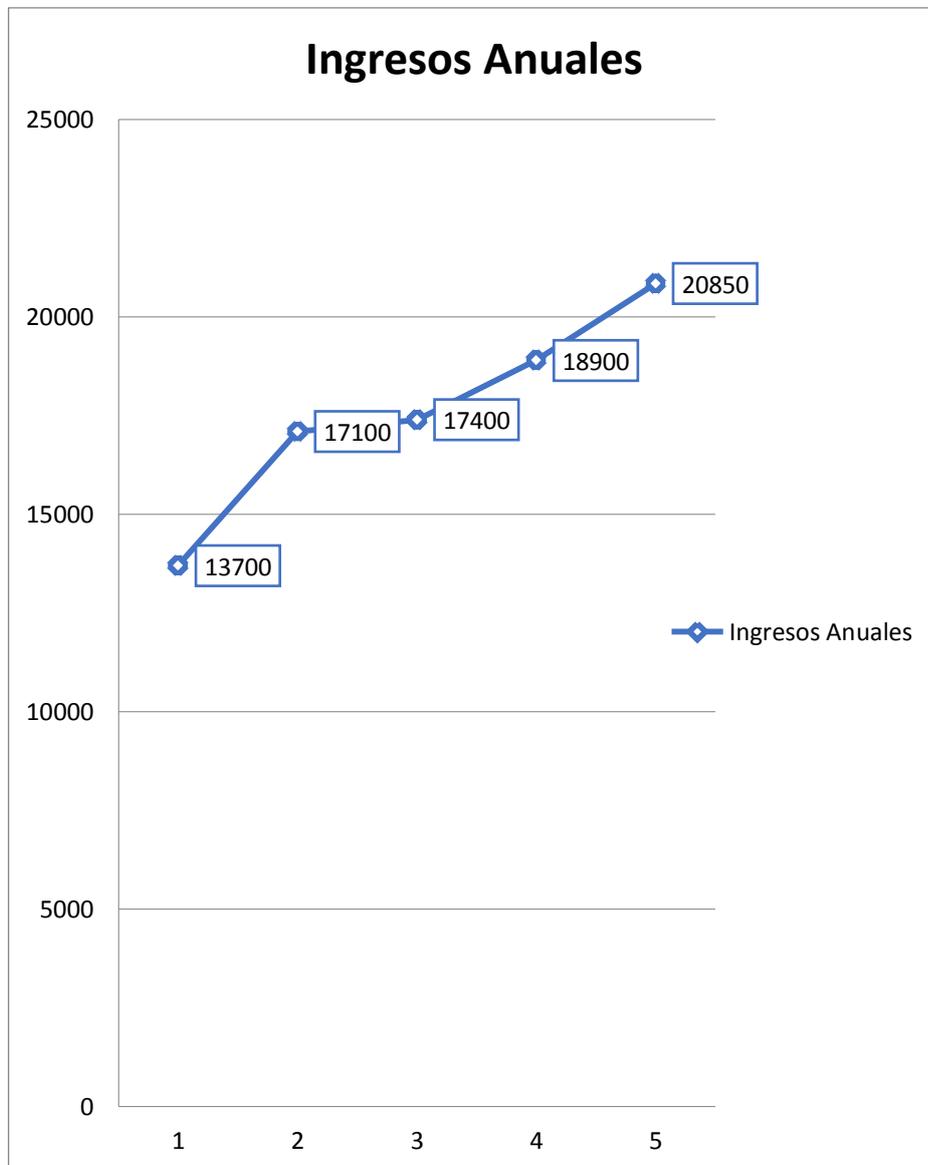


Figura 51 Ingresos anuales

Proyecto DMZ	Proyección
Tasa de descuento	10%
	Proyecto DMZ
Período	Flujo de Fondos
0	-\$30.781,00
1	\$13.700
2	\$17.100
3	\$17.400
4	\$18.900
5	\$20.850

Tabla 21 Proyecciones proyecto DMZ

Proyecto DMZ	
TIR	45,07 %
VAN	\$ 34.733,82

Tabla 22 Resultados proyecciones del proyecto al 10%

Las proyecciones del proyecto son a 5 años pero por la rentabilidad del proyecto al 3er período se estaría recuperando la inversión inicial.

2.4.4 Pentesting

Una vez concluida la simulación en la parte de seguridad de este proyecto se hacen las respectivas pruebas para verificar que las configuraciones han sido exitosas y cumplen a cabalidad con los resultados esperados.

Un gran porcentaje de ataques que ocurren a las empresas son de origen interno, esto por lo general es consecuencia de que los administradores de red centran la mayoría de sus esfuerzos en asegurar la conexión a internet que es la parte más

visible de la red filtrando y bloqueando algunos puertos, de esta manera se asegura de que ningún intruso pueda acceder a la empresa de manera externa, pero se omiten muchas veces las restricciones a nivel interno que debería tener una importancia igual al aseguramiento externo, he aquí el grave problema y las consecuencias de descuidar estas políticas de seguridad que aparentemente no son importantes.

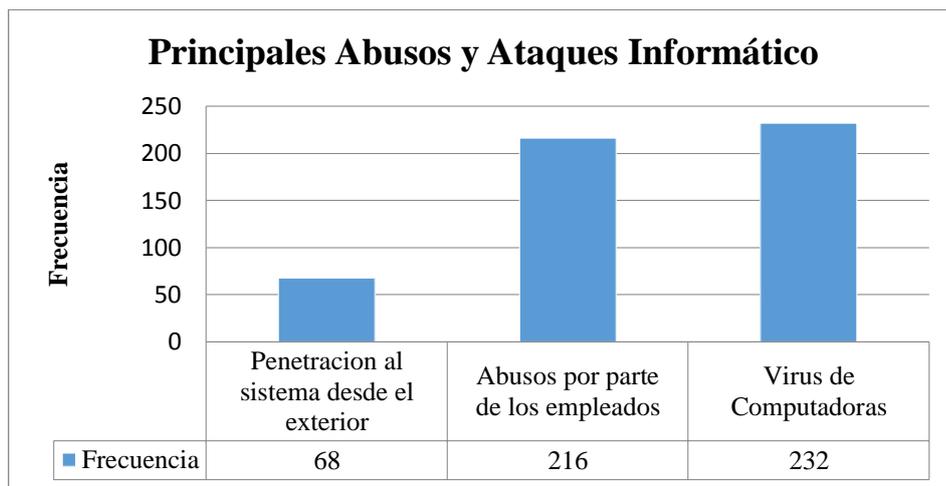


Figura 52 Ataques a redes. Fuente: "Seguridad Informática, UNAM"

Se realizaron una cantidad de pruebas de manera interna y externa usando Zenmap, Putty y NetScan en ambiente Windows y Kali en Linux, para comprobar que tan robusta es la seguridad de la simulación.

Equipos Testeados	Segmento Red	Máscara de Red	Dirección IP
Red WAN	192.168.0.58	255.255.255.0	192.168.0.1
Servidor Web	192.168.10.0	255.255.255.240	192.168.10.2
Red Interna	192.168.11.0	255.255.255.248	192.168.11.3
Red Trabajadores	192.168.6.0	255.255.255.240	192.168.6.2
Gateway Red Trabajadores	192.168.6.0	255.255.255.240	192.168.6.14

Tabla 23 Equipos Testeados

Mapeo Externo

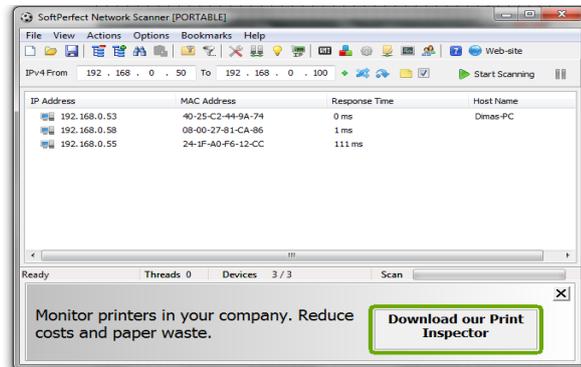


Figura 53 Mapeo Externo

En este proceso se puede apreciar que la IP externa 192.168.0.58 no posee ningún banner, no se identifican si las máquinas son servidores o son pc, a excepción de una pero que la información corrobora que es una pc de escritorio, para este proceso se ha usado el programa Nmap.

Identificación y estados de los puertos externos

Al momento de usar el software de escaneo de puertos Zenmap para una revisión de estos se puede verificar que la configuración es la correcta.

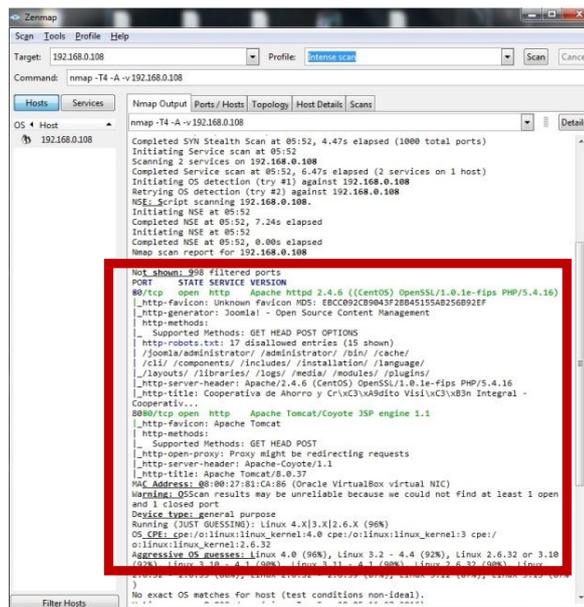


Figura 54 Escaneo de puertos de la interface WAN

En este reporte se puede observar que se tiene únicamente habilitado el puerto 80 y 8080 para la interface WAN para corroborar esta información se utilizará putty.

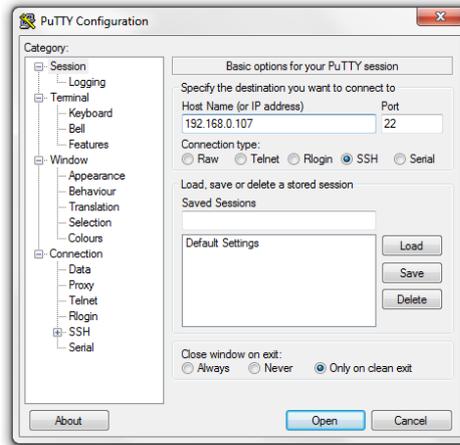


Figura 55 Putty hacia la interface WAN

El resultado de esto es lo siguiente:



Figura 56 Conexión fallida a la interface WAN

El time out o tiempo fuera significa que se envía la petición de conexión pero no hay una respuesta favorable del destino por lo que no regresa ninguna trama de respuesta y se presenta un error, es decir no se puede acceder a la interface WAN por otro puerto que no sea el 80.

Identificación de Sistema Operativo

Por excelencia para este procedimiento se usa Kali Linux y dentro de este la herramienta Nmap, por el hecho que la información que muestra es más detallada que la herramienta Zenmap que se usan en ambiente Windows.

```

root@kali: ~
File Edit View Search Terminal Help
Scanned at 2016-10-20 16:11:04 UTC for 19s
PORT STATE SERVICE REASON VERSION
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16)
|_ http-favicon: Unknown favicon MD5: EBCC092CB9043F2BB45155AB256B92EF
|_ http-generator: Joomla! - Open Source Content Management
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-robots.txt: 17 disallowed entries
|_ /joomla/administrator/ /administrator/ /bin/ /cache/
|_ /cli/ /components/ /includes/ /installation/ /language/
|_ /layouts/ /libraries/ /logs/ /media/ /modules/ /plugins/
|_ /templates/ /tmp/
|_ http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16
|_ http-title: Cooperativa de Ahorro y Cr\xC3\xA9dito Visi\xC3\xB3n Integral - Cooperativ...
MAC Address: 08:00:27:81:CA:86 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSTING): Linux 4.X|3.X|2.6.X (98%)
OS CPE: cpe:/o:linux:linux_kernel:4.0 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6.32
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 4.0 (98%), Linux 3.10 - 4.1 (92%), Linux 3.11 - 4.1 (92%), Linux 3.2 -
.4 (92%), Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (92%), Linux 3.10 - 3.12 (91%), Linux 3.10 (90%),
Linux 3.13 (89%), Linux 2.6.32 - 2.6.35 (88%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.25BETA1%E=4%D=10/20%OT=80%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=080027%TM=5808ECAA%P=i686-pc-linux-gn
u)
SEQ(SP=102%GCD=1%ISR=10C%TI=Z%TS=A)
OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)
WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)
ECN(R=Y%DF=Y%TG=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=0%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)

```

Figura 57 Identificación sistema operativo

Luego del escaneo se puede apreciar los puertos que se encuentran abiertos y también el sistema operativo del servidor, los resultados que se observan indican que es un Linux pero no detallan con exactitud la distribución y el Kernel.

Identificación de Servicios

```

root@kali:~# nmap -sV 192.168.0.58
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-20 16:13 UTC
Nmap scan report for 192.168.0.58
Host is up (0.00045s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16)
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:81:CA:86 (Oracle VirtualBox virtual NIC)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds
root@kali:~#

```

Figura 58 Identificación de servicios

Se procede a la identificación de servicios de cada puerto usando Nmap en Kali Linux y la información que se aprecia indica que los servicios que la red muestra que solo están habilitados los servicios HTTP

Mapeo Interno

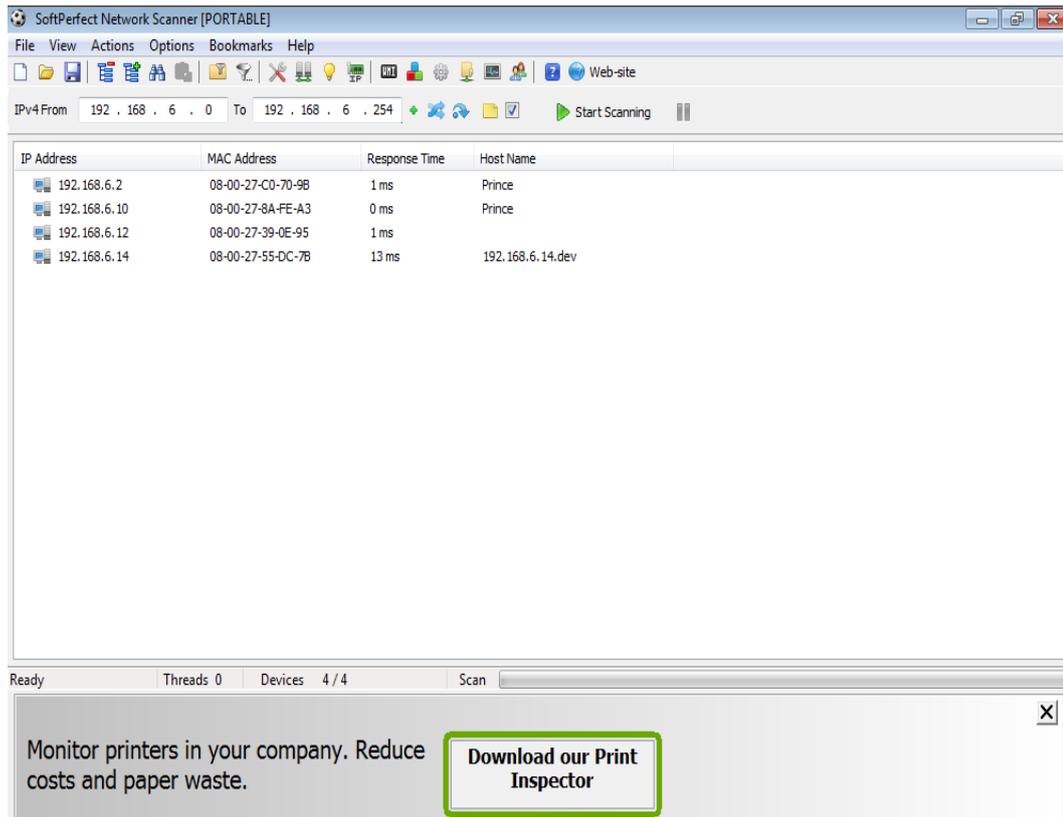


Figura 59 Mapeo Interno

Este proceso se usa NetScan en la red que está más expuesta a recibir un ataque la que identificamos como la red trabajadores, iniciado el proceso de mapeo se puede apreciar algunas máquinas y la mayoría poseen banners que las identifican pero como se modificó la información de los proxys no aparece ningún nombre que pueda indicar que existe un servidor dentro de la red.

Identificación y estados de los puertos internos

Para este proceso de identificar puertos y estados dentro de la red trabajadores se usa Nmap de Kali Linux.

```

Nmap scan report for 192.168.6.2
Host is up (0.00019s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
1027/tcp  open  IIS
1028/tcp  open  unknown
1029/tcp  open  ms-lsa
1030/tcp  open  iad1
2869/tcp  open  iclslap
10243/tcp open  unknown
MAC Address: 08:00:27:C0:70:9B (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   0.19 ms  192.168.6.2

Nmap scan report for prince.developmen (192.168.6.14)
Host is up (0.00031s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
3128/tcp  open  squid-http
MAC Address: 08:00:27:55:DC:7B (Oracle VirtualBox virtual NIC)

```

Figura 60 Nmap interno

En el proceso de escaneo de puertos se encuentra una dirección IP con una gran cantidad de puertos abiertos, luego de verificar la dirección se confirma que esa máquina es la del administrador de red y que los mantiene en ese estado por motivos de mantenimiento, luego se prosigue con la revisión de siguiente dirección que se encuentra activa e identificamos que es la puerta de enlace.

```

Nmap done: 16 IP addresses (2 hosts up) scanned in 17.08 seconds
root@kali:~# nmap 192.168.10.0/28 -traceroute

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-20 16:44 UTC
Nmap scan report for 192.168.10.2
Host is up (0.0024s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   1.68 ms  192.168.6.14.dev (192.168.6.14)
2   1.42 ms  192.168.11.1.dev (192.168.11.1)
3   ... 5
6   3.20 ms  192.168.10.2

Nmap scan report for 192.168.10.3
Host is up (0.0024s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
53/tcp    closed domain
80/tcp    closed http
443/tcp   closed https

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
-   Hops 1-2 are the same as for 192.168.10.2
3   2.65 ms  192.168.10.3

Nmap done: 16 IP addresses (2 hosts up) scanned in 17.99 seconds

```

Figura 61 Traceroute hacia los servidores

A continuación se realiza un Traceroute tal como se aprecia en el figura 61, hacia la red de servidores, este comando permite hacer captura de banners, verificar los puertos e identificar cuantos segmentos o saltos hace, en cuanto a los banner grabbing o "Captura de Banners" como se les conoce no se pueden identificar aun los servidores proxy y el servidor solo permite conexiones del puerto 80.

```
root@kali:~# nmap -O 192.168.10.2
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-20 17:21:15 UTC
Nmap scan report for 192.168.10.2
Host is up (0.00068s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): OpenBSD 4.X (95%), Comau embedded (91%), Linux 2.6.X (89%), FreeBSD 6.X (86%)
OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:linux:linux_kernel:2.6.29 cpe:/o:freebsd:freebsd:6.3
Aggressive OS guesses: OpenBSD 4.0 (95%), Comau C4G robot control unit (91%), Linux 2.6.29 (89%), FreeBSD 6.3-RELEASE (86%), OpenBSD 4.3 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.98 seconds
```

Figura 62 Buscando el sistema operativo del servidor

Ya usando un comando más avanzado se puede identificar en parte el sistema operativo pero aun sin datos concretos.

Se realiza un escaneo para verificar si la red está protegida por algún firewall

```
root@kali:~# nmap -sA 192.168.10.0/28
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-23 20:22 UTC
Nmap scan report for 192.168.10.2
Host is up (0.0025s latency).
All 1000 scanned ports on 192.168.10.2 are filtered

Nmap scan report for 192.168.10.3
Host is up (0.0017s latency).
All 1000 scanned ports on 192.168.10.3 are filtered

Nmap done: 16 IP addresses (2 hosts up) scanned in 11.21 seconds
```

Figura 63 Búsqueda de firewalls activos

Como paso final se realiza un escaneo, en caso existan puertos UDP abiertos

```
root@kali:~# nmap -PU 192.168.10.0/28
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-23 20:25 UTC
Nmap done: 16 IP addresses (0 hosts up) scanned in 4.11 seconds
root@kali:~#
```

Figura 64 Búsqueda de puertos UDP

Se usa Putty para comprobar si se puede acceder al servidor y también un servidor de FTP como FileZilla para verificar conexiones remotas.

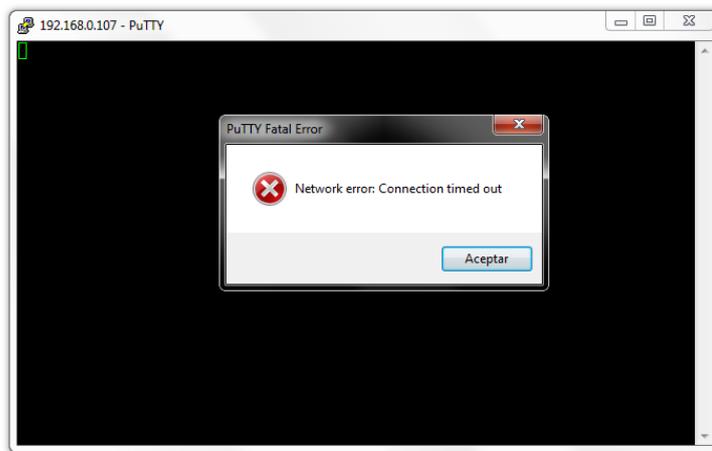


Figura 65 Conexión al servidor web con Putty

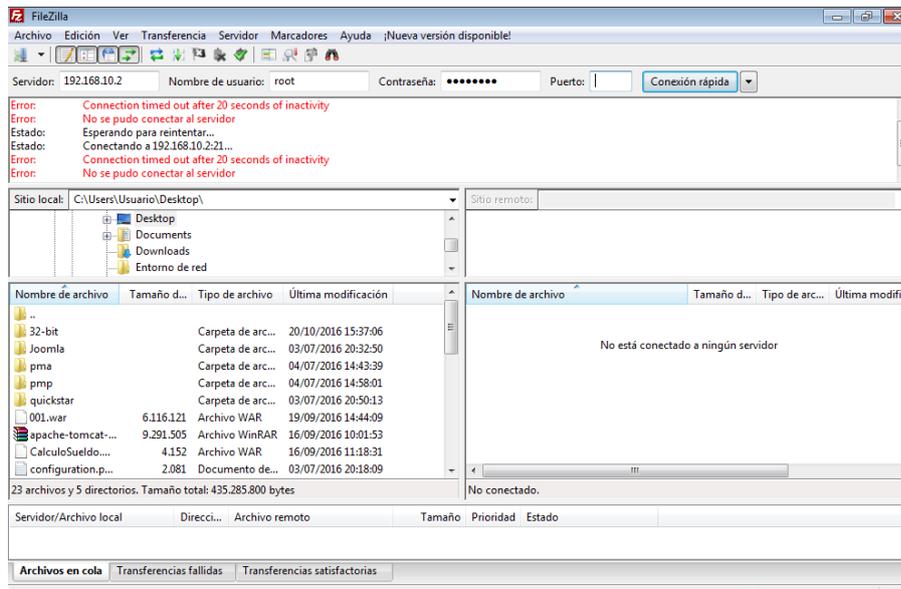


Figura 66 Conexión al servidor web con FileZilla

Al no haber respuesta de conexión, la DMZ cumple su función a cabalidad.

2.5 RESULTADOS

Luego del análisis, diseño y finalmente la implementación del aseguramiento de la red, los resultados fueron inmediatos puesto que se obtuvo una red con un mayor control de acceso tanto de entrada de datos como de salida.

Así mismo se gestionaron permisos en el firewall perimetral en cada una de sus interfaces, para la navegación web del área de servidores y usuarios se abrieron los puertos necesarios y adicional a esto se dieron permisos especiales al administrador de red para que pueda dar el respectivo mantenimiento.

En referencia a la navegación web, en los servidores proxys basados en pfSense se instalaron complementos tales como Squid y SquidGuard, que permiten el bloqueó páginas y de contenido por ejemplo: pornografía, acceso a videos en línea, redes sociales, etc.

En cuanto a las pruebas con los servidores se implementó la página web del proyecto, el servidor de aplicaciones se lo enlazó a la página principal consiguiendo correcta comunicación entre ambas, la aplicación de ejemplo se comunica correctamente al servidor de base de datos por lo que la estructura esta funcional y lista para implementar en producción.

Se realizaron también proyecciones a largo plazo de como crecería la red si la empresa lo amerita y debido al diseño de esta el crecimiento de la misma puede ser de manera exponencial usando tecnología IPV4 o IPV6 por el hecho que esta red está diseñada para soportar ambas.

Se realizó un pentesting a los equipos de red críticos para lograr identificar si las configuraciones realizadas fueron exitosas.

CONCLUSIONES

- ✓ El gasto de la compra de equipos para el proyecto se verá como una inversión puesto que todo lo que se hará en este proyecto será en beneficio de la misma y por esta razón se lo considera rentable.
- ✓ Al estar trabajando en base al Sistema de Gestión de la Seguridad de la Información (SGSI), se garantizará que se va a velar por la protección de la información de la empresa, en consecuencia la infraestructura de comunicaciones estaría encaminada a tener una certificación de calidad.
- ✓ La simulación de este proyecto permitió en ambiente de pruebas crear muchas restricciones a nivel de navegación web, en consecuencia se obtiene un consumo eficiente del ancho de banda que brinda el proveedor de internet de esta manera se aprovecha al máximo la conexión que se tiene disponible dentro de la empresa.
- ✓ El proyecto es muy versátil, puede expandir sus servicios de manera exponencial todo esto a mediano plazo tanto en la implementación de más servidores, en la administración de más redes de usuarios, las reglas a implementar dentro de cada red, permisos de navegación, etc. Pero esto depende del aumento de la capacidad física de cada servidor con respecto al hardware.
- ✓ La difusión comunicacional de la institución mejorará mediante su página web oficial y su aplicación en línea, que en consecuencia dará más confianza y ayudará a la captación de clientes.
- ✓ Subir peldaños dentro del ranking nacional de todas las Cooperativas de Ahorro y Crédito registradas dentro de la SEPS, lo que a su vez significaría en un incremento de los servicios que la cooperativa puede ofrecer a sus clientes.

RECOMENDACIONES

- ✓ Mantener los niveles de seguridad siempre monitorizados y actualizados, haciendo pruebas periódicas de los puertos que están ofreciendo servicios a la red.
- ✓ Revisar periódicamente las actualizaciones de Blacklist para los servidores proxys, ver qué novedades trae y que nuevo contenido se puede bloquear.
- ✓ Dar charlas sobre técnicas de seguridad a todos los usuarios, para evitar caer en lo que se conoce como Ingeniería Social.
- ✓ La generación de planes de contingencia por cualquier evento que se presentará, tales como desastres naturales o fallos del hardware.
- ✓ Mantener actualizado los paquetes de Squid y SquidGuard porque de estos depende la administración de la navegación web dentro de la empresa.
- ✓ Mantener la empresa al tanto de ataques que se hayan realizado a otros sistemas de comunicaciones y a partir de estos establecer nuevos controles y estrategias de seguridad si la empresa no los tuviera.
- ✓ Al ser una institución que maneja cantidades de dinero es imperativo la adquisición de un firewall físico.

GLOSARIO

PfSense: Sistema operativo de código abierto basado en BSD que puede usarse de Proxy – Firewall.

Squid: Es un servidor proxy con caché. Es una de las aplicaciones más populares y de referencia para esta función está basada en código abierto muy completo y robusto.

SquidGuard: Es una extensión de Squid que sirve para filtrar contenido usando listas negras.

Hipervisor: Monitor de máquinas virtuales que permite distintos sistemas operativos.

Blacklist: Son filtros url para la navegación web siempre se están actualizando.

Proxy: Intercepta conexiones desde un cliente a un servidor destino.

Firewall Perimetral: La primera barrera de defensa de una red diseñada para bloquear accesos no autorizados y permitiendo al mismo tiempo comunicaciones autorizadas en reglas ya definidas.

FTP: Protocolo de red para la transferencia de archivos.

SSH: Permite acceder a máquinas remotas a través de la red usando comandos.

Joomla: Sistema de gestión de contenidos para crear páginas web dinámicas e interactivas.

DMZ: Zona segura que generalmente está ubicada entre la red interna de una organización y una red externa que por lo general siempre es el Internet.

WAN: Red de área amplia que se caracteriza por tener conexiones a nivel global

LAN: Red de área local se la puede definir como una red interna que utiliza sus propios medios para interconectarse.

IPV4: Protocolo de internet versión 4 que usa direcciones de 32 bits.

IPV6: Protocolo de internet versión 6 que usa direcciones de 128 bits.

Nmap: Software que permite exploración de red.

Putty: Software de administración remota de servidores.

NAT: Intercambiar paquetes entre dos redes que son incompatibles.

Paquetes: bloques en que se divide la información que se envía por una red

Proxmox: Software de virtualización robusto usado en grandes empresas e instituciones, tiene licencia GPL

VirtualBox: Software de virtualización que se usa mayoritariamente para pruebas, tiene licencia GPL

BIBLIOGRAFÍA

- ✓ Cisco. (2016). Direccionamiento de IP y conexión en subredes, p. 4.
- ✓ David, M. J., Jordi, M. H., Enric, P. O., María, B. O. J., Griera, I. J., Ramon, M. E., & Xavier, P. T. (2004). Redes de computadores. *Editora Campus*.
- ✓ Dussan Clavijo, C. A. (2006). Políticas de Seguridad Informática. *Entramado*, 2(1), 86–92. Retrieved from http://www.unilibrecali.edu.co/entramado/images/stories/pdf_articulos/volumen2/Políticas_de_seguridad_informtica.pdf
- ✓ Erb, Markus; Flores, Carolina; Chub, Arturo; Kurzen, Adrian; Sarantes, D. (2010). Definición de Seguridad Informática | Gestión de Riesgo en la Seguridad Informática. Retrieved from https://protejete.wordpress.com/gdr_principal/definicion_si/
- ✓ Fernandez, J. (2013). Seguridad en Informatica, 1–218.
- ✓ Gómez Vieites, A. (2009). Tipos de Ataques e Intrusos en las Redes Informáticas. Retrieved from agomez@simce.com
- ✓ Hernandez, R. (2000). Seguridad Informatica / Firewall / Cortafuegos. Retrieved from <http://www.segu-info.com.ar/firewall/firewall.htm>
- ✓ ISO27000.es Gestión de Seguridad de la Información. (2012). Retrieved from <http://www.iso27000.es/otros.html>
- ✓ Joomla en CentOS 7. (2015). Retrieved from <https://linuxservices.wikispaces.com/Joomla+en+CentOS+7>
- ✓ Marchionni, A. (2011). *Administración de Servidores*.
- ✓ Squid en pfsense. (2012). Retrieved from <http://drivemeca.blogspot.com/2012/03/como-instalar-y-configurar-squid-en.html>
- ✓ Tanenbaum, A. S., & Wetherall, D. J. (2012). *Redes De Computadoras. Redes de computadoras*.
- ✓ TCP/IP y el modelo OSI | Textos Científicos. (2015). Retrieved from <http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi>
- ✓ TP-LINK. (2016). DMZ. Retrieved from <http://www.tp-link.es/FAQ-28.html>
- ✓ Urrego, J. (2013). Tipos de ataque y cómo prevenirlos. Retrieved from <https://colombiadigital.net/actualidad/articulos-informativos/item/4801-tipos-de-ataque-y-como-prevenirlos.html>

- ✓ Urueña León, E. E. (2006). Direccionamiento IP.
- ✓ userservers. (2016). Dirección IP. Retrieved from http://web.userservers.net/ayuda/soluciones/dominios/que-es-una-direccion-ip_NTk.html
- ✓ VmWare. (2016). Virtualización de VMware. Retrieved from <http://www.vmware.com/latam/solutions/virtualization.html>

ANEXOS

1 Formato de la entrevista

**UNIVERSIDAD ESTATAL
PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

La siguiente entrevista es con la finalidad de facilitar información de la estructura la red de la empresa y toda la información que facilite la Implementación de una DMZ (Zona Desmilitarizada).

DATOS DE IDENTIFICACION

Nombre de la Empresa:
Nombre del Entrevistado:
Cargo Del Entrevistado:
e-mail:
Dirección:
Teléfono:
Sitio web:

1. ¿Cuáles son sus responsabilidades en la empresa?
2. ¿Cómo está estructurado el Departamento de Sistemas?
3. ¿Cómo está estructurada la Red de la empresa?
4. Tienen implementada una DMZ en la Red y cómo está diseñada la DMZ?
5. ¿Cuántos Firewall tienen en la Red y de qué forma está estructurado cada Firewall?
6. ¿En qué plataforma trabaja el Firewall?
7. ¿Qué versión o Distribución utiliza la plataforma del firewall?
8. ¿Cuáles son las políticas de seguridad implementadas en el firewall?
9. ¿Qué accesos están configurados en el firewall?
10. ¿Cuál es el ancho de banda que tiene la red?
11. La red de la empresa esta segmentada
12. ¿Con qué frecuencia los usuarios externos acceden a la red y qué cantidad de usuarios acceden?
13. ¿Cuán beneficioso es para la empresa contar con una DMZ?
14. ¿Cuál es el nivel de inversión anual de hardware/software en la empresa?

2 Formato de la encuesta

**UNIVERSIDAD ESTATAL
PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

Anote una "X" en la respuesta que usted considere más adecuada, solo seleccione una opción.
No deje respuestas en blanco.

1. ¿Cómo califica usted que una PYME (Pequeña y Mediana Empresa) no posea DMZ dentro de su diseño de red?
Buena ()
Regular ()
Mala ()
2. ¿Cómo considera usted la implementación de una DMZ dentro del diseño de red de una PYME (Pequeña y Mediana Empresa)?
Muy prioritario ()
Medianamente prioritario ()
No prioritario ()
3. En caso de que una PYME (Pequeña y Mediana Empresa) no cuente con una DMZ, considera usted que la inversión y reestructuración del diseño de red es:
Muy prioritario ()
Medianamente prioritario ()
No prioritario ()

3 Carta Aval de la Cooperativa de Ahorro y Crédito “Visión Integral”



COOPERATIVA DE AHORRO Y CREDITO
VISION INTEGRAL
ACUERDO Ministerial N° 0174
PALMAR - ECUADOR
Promoviendo el Desarrollo Campesino

Palmar, 18 de octubre del 2016

Ing.
Mariuxi de la Cruz
DIRECTORA DE LA CARRERA DE INFORMATICA-UPSE
La Libertad

De mi consideración.-

Reciba un cordial saludo de quienes formamos parte de la Cooperativa de Ahorro y Crédito “Visión Integral” de la comuna Palmar.

La presente es para darle a conocer que se aprobó la ejecución del proyecto que el Sr. Dimas Fernando Mendoza González, con C. I. 0924925647, y el cual tiene como tema “ESTUDIO DE ASEGURAMIENTO DE LA INFRAESTRUCTURA DE COMUNICACIONES IMPLEMENTANDO UNA DMZ Y FIREWALL PERIMETRAL EN LA COOPERATIVA DE AHORRO Y CRÉDITO VISION INTEGRAL, SANTA ELENA”, dentro de esta Institución.

Es de señalar que esta organización está controlada por la Superintendencia de la Economía Popular y Solidaria (SEPS) dedicada a brindar servicios financieros en beneficio al desarrollo de la economía local.

Certificación que damos en honor a la verdad. El interesado podrá hacer el uso legal que bien tuviere, a lo que me remitiré en caso necesario.

Atentamente,


Ing. Fidel Narea Sánchez, MSc
PRESIDENTE
C.I. 0914734173



4 Instalación y configuración del servidor web

Ya instalado el Centos7 en modo mínimo se ingresa en modo super usuario.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-327.el7.x86_64 on an x86_64

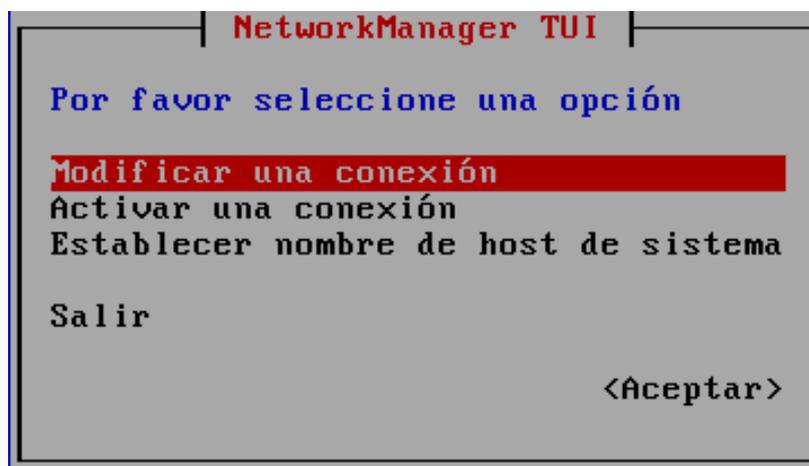
localhost login: root
Password: _
```

Lo siguiente es configurar la tarjeta de red del servidor usando el comando *nmtui*.

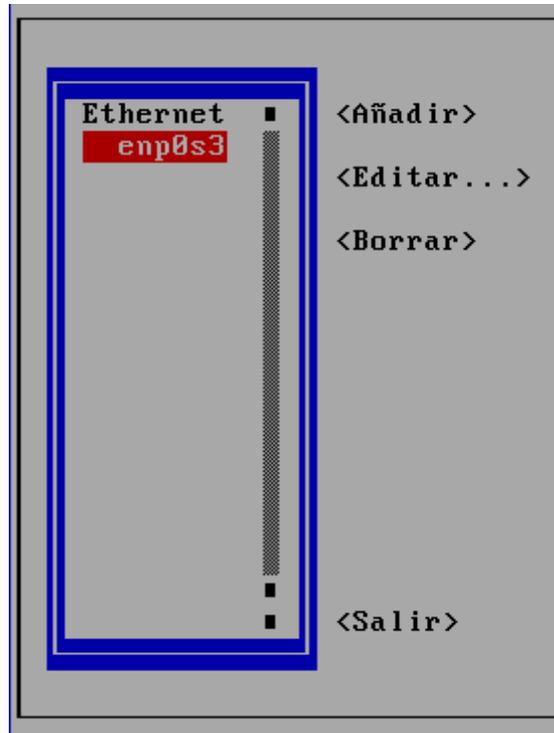
```
CentOS Linux 7 (Core)
Kernel 3.10.0-327.el7.x86_64 on an x86_64

lserver login: root
Password:
Last login: Wed Aug 31 11:29:22 from 192.168.11.3
[root@lserver ~]# nmtui_
```

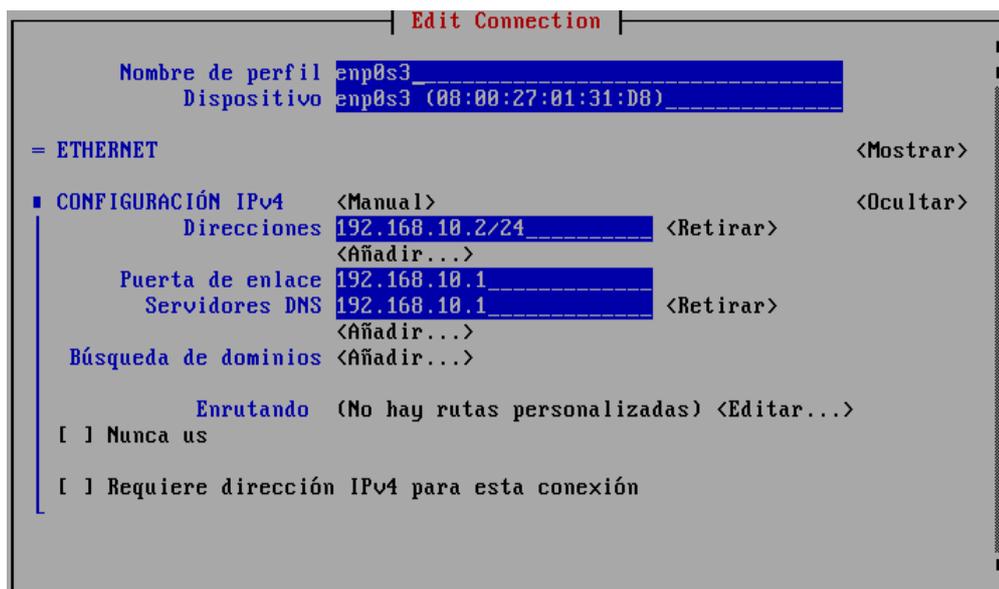
Se abrirá una ventana de configuración en modo gráfico que tiene algunas opciones, se ingresa a modificar una conexión.



Aparece la tarjeta de red pero el nombre de esta no es eth0 como en versiones anteriores, ahora se denomina enp0s3.



Se ingresa y configura el direccionamiento IP de acuerdo al diseño propuesto de la red.



Se guardan los cambios y se reinicia la red usando el comando *service network restart*.

```
[root@server ~]# service network restart
Restarting network (via systemctl): [ OK ]
[root@server ~]# _
```

Lo siguiente a hacer es instalar apache con el comando *yum -y install httpd*.

```
Desde      : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Instalando      : apr-1.4.8-3.el7.x86_64                1/5
  Instalando      : apr-util-1.5.2-6.el7.x86_64           2/5
  Instalando      : httpd-tools-2.4.6-40.el7.centos.1.x86_64 3/5
  Instalando      : mailcap-2.1.41-2.el7.noarch           4/5
  Instalando      : httpd-2.4.6-40.el7.centos.1.x86_64    5/5
  Comprobando     : mailcap-2.1.41-2.el7.noarch           1/5
  Comprobando     : httpd-2.4.6-40.el7.centos.1.x86_64    2/5
  Comprobando     : apr-util-1.5.2-6.el7.x86_64           3/5
  Comprobando     : apr-1.4.8-3.el7.x86_64                4/5
  Comprobando     : httpd-tools-2.4.6-40.el7.centos.1.x86_64 5/5

Instalado:
  httpd.x86_64 0:2.4.6-40.el7.centos.1

Dependencia(s) instalada(s):
  apr.x86_64 0:1.4.8-3.el7                apr-util.x86_64 0:1.5.2-6.el7
  httpd-tools.x86_64 0:2.4.6-40.el7.centos.1  mailcap.noarch 0:2.1.41-2.el7

¡Listo!
[root@localhost ~]# _
```

Se prosigue ahora con la instalación de MySQL, existe una variación en la instalación de este paquete puesto que se tiene que agregar repositorios, el primer paso es instalar *wget*.

```
=====
Instalando:
  wget          x86_64          1.14-10.el7_0.1          base          545 k

Resumen de la transacción
=====
Instalar 1 Paquete

Tamaño total de la descarga: 545 k
Tamaño instalado: 2.0 M
Is this ok [y/d/N]: y
Downloading packages:
  wget-1.14-10.el7_0.1.x86_64.rpm          | 545 kB    00:05
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Instalando      : wget-1.14-10.el7_0.1.x86_64          1/1
  Comprobando     : wget-1.14-10.el7_0.1.x86_64          1/1

Instalado:
  wget.x86_64 0:1.14-10.el7_0.1

¡Listo!
[root@localhost ~]# _
```

Se agregan los repositorios siguiendo los pasos que indica la página oficial de mysql.

```
wget http://repo.mysql.com/mysql-community-release-el7-5.noarch.rpm  
rpm -ivh mysql-community-release-el7-5.noarch.rpm  
yum update  
install mysql-server  
systemctl start mysqld
```

Luego de instalar MySQL y reiniciar el servidor web se instala Joomla.

El primer paso para esto es dirigirse a la página web oficial obtener la dirección de descarga del .zip; usando el wget se descarga el paquete.

```
[root@localhost joomla]# ll  
total 9612  
-rw-r--r--. 1 root root 9842386 oct 31 14:21 Joomla_3.3.1-Spanish-Pack_Completo.  
zip
```

Se instala *unzip* usando el comando `yum -y install unzip` y se lo ejecuta para descomprimir el paquete que hemos descargado. Usando el comando “*unzip Joomla_3.3.1-Spanish-Pack_Completo.zip*”

```
total 9788  
drwxr-xr-x. 10 root root 4896 jun 13 17:48 administrator  
drwxr-xr-x. 2 root root 42 jun 13 17:48 bin  
drwxr-xr-x. 2 root root 23 jun 13 17:48 cache  
drwxr-xr-x. 2 root root 4896 jun 13 17:48 cli  
drwxr-xr-x. 17 root root 4896 jun 13 17:48 components  
-rw-r--r--. 1 root root 1764 jun 11 07:46 CONTRIBUTING.md  
-rw-r--r--. 1 root root 2859 jun 11 07:46 htaccess.txt  
drwxr-xr-x. 5 root root 4896 jun 13 17:48 images  
drwxr-xr-x. 2 root root 61 jun 13 17:48 includes  
-rw-r--r--. 1 root root 1813 jun 11 07:46 index.php  
drwxr-xr-x. 11 root root 4896 abr 30 2014 installation  
-rw-r--r--. 1 root root 9842386 oct 31 14:21 Joomla_3.3.1-Spanish-Pack_Completo.  
zip  
-rw-r--r--. 1 root root 1985 jun 11 07:47 joomla.xml  
drwxr-xr-x. 5 root root 63 jun 13 17:48 language  
drwxr-xr-x. 4 root root 52 jun 13 17:48 layouts  
drwxr-xr-x. 13 root root 4896 jun 13 17:48 libraries  
-rw-r--r--. 1 root root 17816 jun 11 07:46 LICENSE.txt  
drwxr-xr-x. 2 root root 23 jun 13 17:48 logs  
drwxr-xr-x. 18 root root 4896 jun 13 17:48 media  
drwxr-xr-x. 28 root root 4896 jun 13 17:48 modules  
drwxr-xr-x. 14 root root 4896 jun 13 17:48 plugins  
-rw-r--r--. 1 root root 4968 jun 11 07:46 README.md
```

Luego se extraen los datos del archivo .zip por seguridad se elimina el paquete original usando el comando `“rm Joomla_3.3.1-Spanish-Pack_Completo.zip”` y se mueve todo lo extraído a la carpeta `“/var/www/html/”`, con el comando `“mv * /var/www/html/”`.

Se dan permisos a la carpeta html

```
[root@localhost html]# chown -R apache:apache *
[root@localhost html]# chmod -R 750 *
[root@localhost html]# _
```

Finalmente se habilita una función para que MySQL y PHP se entiendan instalando el modulo php-mysql.

```
[root@localhost www]# yum install php-mysql
```

Se dan permisos a apache sobre la carpeta html.

```
[root@localhost www]# ll
total 4
drwxr-xr-x. 2 root root 6 jul 23 16:48 cgi-bin
drwxr-xr-x. 18 apache root 4096 oct 31 12:11 html
[root@localhost www]# chown apache html
```

Luego se reinicia apache y se tiene listo Joomla en el servidor web.

5 Configuración del servidor de aplicaciones

Ya instalado el Centos7 en modo mínimo se ingresa en modo super usuario.

```
lserver login: root
Password:
Last login: Sun Sep 11 14:24:06 on tty1
[root@lserver ~]#
[root@lserver ~]# . _
```

Se instalan dependencias yum -y install wget java-1.7.0-openjdk-devel

```
[root@localhost ~]# yum install java-1.7.0-openjdk-devel _
```

Se descarga Tomcat. En este momento la última versión es la 8.0.37 se usa el comando `wget -c http://apache.mirrors.tds.net/tomcat/tomcat-v8.0.37/bin/apache-tomcat-8.0.37.tar.gz`

Se descomprime el archivo usando `tar xzvf apache-tomcat-8.0.15.tar.gz`.

Se activan permisos de lectura `chmod +r apache-tomcat-8.0.15/conf/*`

```
[root@localhost bin]# chmod +r apache-tomcat-8.0.37/conf/* _
```

Se edita el archivo `tomcat-users.xml` ubicado en `/opt/apache-tomcat-8.0.37/conf/` y luego se agrega un usuario con una contraseña y sus respectivos permisos.

```
<role rolename="manager-gui"/>
<user username="root" password="21065dfg" roles="manager-gui"/>
```

Para culminar con todos los pasos se inicia tomcat haciendo lo siguiente:

- ✓ Se accede a la carpeta bin ubicada en el directorio `/opt/apache-tomcat-8.0.37/bin`
- ✓ Se Introduce el siguiente comando `“./startup.sh”`, si todo está correcto aparecerá una línea de comandos y al final dirá que tomcat está iniciado

```

[root@localhost bin]# ./startup.sh
Using CATALINA_BASE:   /opt/apache-tomcat-8.0.37
Using CATALINA_HOME:   /opt/apache-tomcat-8.0.37
Using CATALINA_TMPDIR: /opt/apache-tomcat-8.0.37/temp
Using JRE_HOME:        /
Using CLASSPATH:       /opt/apache-tomcat-8.0.37/bin/bootstrap.jar:/opt/apache-tomcat-8.0.37/bin/tomcat-juli.jar
Tomcat started.

```

Como paso final se abrirá una pestaña en el navegador web con la dirección IP del servidor en este caso 192.168.10.3:8080 y se observará lo siguiente.

192.168.10.3:8080

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/8.0.37

The Apache Software Foundation
http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat. Congratulations!

 Recommended Reading:

- [Security Considerations HOW-TO](#)
- [Manager Application HOW-TO](#)
- [Clustering/Session Replication HOW-TO](#)

Server Status
Manager App
Host Manager

Developer Quick Start

- [Tomcat Setup](#)
- [Realms & AAA](#)
- [Examples](#)
- [Servlet Specifications](#)
- [First Web Application](#)
- [JDBC DataSources](#)
- [Tomcat Versions](#)

Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 8.0 access to the manager application is split between different users. [Read more...](#)

[Release Notes](#)

[Changelog](#)

[Migration Guide](#)

[Security Notices](#)

Documentation

[Tomcat 8.0 Documentation](#)

[Tomcat 8.0 Configuration](#)

[Tomcat Wiki](#)

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

- [Tomcat 8.0 Bug Database](#)
- [Tomcat 8.0 JavaDocs](#)
- [Tomcat 8.0 SVN Repository](#)

Getting Help

[FAQ and Mailing Lists](#)

The following mailing lists are available:

- [tomcat-announce](#)
Important announcements, releases, security vulnerability notifications. (Low volume).
- [tomcat-users](#)
User support and discussion
- [taglibs-user](#)
User support and discussion for Apache Taglibs
- [tomcat-dev](#)
Development mailing list, including commit messages

6 Instalación de SQL 2012

Se instaló SQL 2012.

