

ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

**CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES Y
COMUICACIÓN DE DATOS**

**PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE
INGENIERÍA**

**IMPLEMENTACIÓN DE CLOUD SECURITY EN UN SISTEMA
BASADO EN XEN CLOUD PLATFORM**

NATALIA CAROLINA MATIZ MOYA

SANGOLQUI – ECUADOR

2013

DECLARACIÓN DE RESPONSABILIDAD

NATALIA CAROLINA MATIZ MOYA

DECLARO QUE:

El proyecto denominado “IMPLEMENTACIÓN DE CLOUD SECURITY PARA UN SISTEMA BASADO EN CLOUD PLATFORM”, ha sido desarrollado en base a una investigación exhaustiva, respetando los derechos intelectuales de terceros, conforme a las fuentes que se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 03 de Mayo de 2013.

Natalia Carolina Matiz Moya

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado: IMPLEMENTACIÓN DE CLOUD SECURITY EN UN SISTEMA BASADO EN XEN CLOUD PLATFORM, ha sido desarrollado en su totalidad por la señorita NATALIA CAROLINA MATIZ MOYA, bajo nuestra dirección.

Atentamente

Ing. Carlos Romero G.

DIRECTOR

Ing. Rodolfo Gordillo O.

CODIRECTOR

AUTORIZACIÓN

NATALIA CAROLINA MATIZ MOYA

Autorizo a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la Institución del trabajo “IMPLEMENTACIÓN DE CLOUD SECURITY EN UN SISTEMA BASADO EN XEN CLOUD PLATFORM”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, 03 de Mayo de 2013.

Natalia Carolina Matiz Moya

RESUMEN

Actualmente, *Cloud Computing* es considerada como una tecnología moderna en donde se tiene la posibilidad de consumir servicios de TI¹ y aplicaciones de una forma ágil y flexible. Por esta razón las grandes y pequeñas empresas han optado por implementar esta solución dependiendo de sus necesidades y requerimientos, ya que al ser un recurso tecnológico que contiene varios tipos de soluciones, las empresas pueden tener el procesamiento y la información en datacenters dentro de su misma empresa, o bien fuera de esta mediante la contratación de una nube pública.

Cloud Computing, al ser una tecnología tan cotizada en el mercado, también demanda la necesidad por parte del proveedor; de, además de ofrecer servicios en la nube, ofrecer que estos sean seguros y que los usuarios tengan la confianza de acceder a ellos con total confianza.

Por esta razón, nace el concepto de *Cloud Security*, con lo cual el proveedor garantiza dar servicios y aplicaciones cloud; y por su parte, el cliente se compromete en cumplir con las normas de seguridad en lo que se refiere al trato de su información e identidad.

El presente proyecto se ha desarrollado específicamente para implementar *Cloud Security* en una nube montada bajo la plataforma de virtualización llamada Xen Cloud Platform. Esta nube provee específicamente de Software como Servicio (SAAS) a los usuarios de los Laboratorios del DEEE de la Escuela Politécnica del Ejército; pero al ser una nube que cuenta con toda la Infraestructura necesaria para implementar los tres modelos de servicios que ofrece *Cloud Computing*, se han protegido justamente los tres modelos de servicios (Infraestructura, Plataforma y Software como Servicio) que pueden ser ofertados a los usuarios.

¹ Tecnologías de la información

AGRADECIMIENTOS

A DIOS por haber sido mi motor, mi guía y por llenarme con su inmensa sabiduría todos estos años de vida. Gracias a ti mi Divino Niño por escucharme siempre con cada oración, y ser tan bueno y bondadoso conmigo. Te Amo profundamente.

A quienes siempre han sido mi mayor apoyo, mi fuerza; y de quienes siempre recibí las palabras más sabias y oportunas, para enfrentar la vida y lo que venía con ella; como no agradecerles todas las palabras de aliento, cariño y motivación, los abrazos y besos; y por estar siempre ahí, junto a mí. Este logro no solo es mío, gracias a ustedes Papi y Mami, que siempre me enseñaron a valorar las pequeñas cosas que da la vida, que a la final terminan siendo los tesoros más grandes que uno puede tener, porque siempre me enseñaron que más allá de crecer profesionalmente, es más importante crecer como persona. Los amo inmensamente.

A mi hermano que desde niño fue un complemento en mi vida; gracias por tu compañía, tus bromas, tu forma tan peculiar de ser; gracias por formar parte de mi vida y porque a pesar de las peleas de hermanos, siempre estás ahí para apoyarme. Te quiero Muchísimo, Ñaño.

A ti amor mío, Adrián, como no agradecerte que formes parte de mi vida desde hace tantos años, y que seas el complemento ideal. Gracias por ser esa persona tan especial, cariñosa y maravillosa, gracias por todo tu amor y apoyo incondicional cada día en esta aventura. Por tu comprensión y consejos; por ser mí soporte en los momentos más duros y difíciles. Te amo.

A mis amados abuelitos maternos, Mamita y Papito; porque tengo la dicha de tenerlos junto a mí, y poder compartir este logro alcanzado junto a ustedes. Gracias por haber cumplido muchas veces las funciones de padres. Los amo mucho y los recordaré siempre con enorme gratitud.

A mis queridos abuelos paternos, Abuelita Marina y Abuelito Jaime, por todo su cariño, preocupación y admiración. Los quiero mucho.

A mis queridos tíos, Verito, Carlitos, Gualita, Angelita, Sergio y Gaby; gracias por sus palabras de aliento, por todo su cariño y apoyo incondicional en cada etapa de mi vida. Los quiero mucho.

A todas y cada una de las personas que ocupan un lugar en mi corazón y que hacen de cada momento vivido en la Universidad, un bonito recuerdo que lo llevaré por siempre en mi memoria. Gracias amigos por estos cinco años de esfuerzo, sacrificio, malas noches, y buenos momentos compartidos, los quiero con todo mi corazón. A ustedes que fueron, son y serán mis mejores amigos; a ti Vini por ser un amigo incondicional y único, te re quiero. A mis mejores amigas, Alex, Yes y Lore. Gracias por estar siempre apoyando mis locuras, mis buenos y malos momentos; las re quiero. A Ricky, Juan y David, por ser únicos y hacerme reír siempre con sus locuras y bromas. A ustedes; Astu, Filito, Andresito Vaca, Patito, Lenin, Fer y Brian, por ser especiales y maravillosas personas; los quiero mucho.

A ti Andresito Revelo por todo tu apoyo y ayuda para llevar a cabo el desarrollo de este proyecto. Eres una persona maravillosa. Gracias.

A mi querido Ing. Fabián Sáenz, por todo su apoyo y cariño durante los últimos meses. Gracias Inge por ser no solo un orientador más, sino un amigo incondicional.

A mis queridos Ingenieros orientadores de tesis, Ing. Carlos Romero e Ing. Rodolfo Gordillo, porque además del apoyo brindado para el desarrollo del presente proyecto, pusieron en mí su confianza y me enseñaron a explotar todas mis capacidades para culminar con éxito mi carrera profesional. Para ustedes mi aprecio incondicional.

DEDICATORIA

A mis padres por ser lo más importante en mi vida, y porque gracias a su esfuerzo y dedicación me convertí en la mujer y profesional que ahora soy.

A ti mami, por enseñarme siempre, a ser constante, perseverante, y buscar la excelencia en las cosas que hago, a no ser conformista, sino responsable con mis obligaciones. Por todos tus consejos, mimos y abrazos. Por todo tu esfuerzo por formar y mantener la familia tan unida que ahora somos; y por enseñarme a valorar que el regalo y lo más importante que uno tiene en la vida es la familia. Te amo MA.

A ti papi, por enseñarme a ser correcta, honesta y siempre brillar con luz propia; por enseñarme a nunca bajar los brazos, y volver a levantarme si alguna vez tropiezo y fallo. Por todos tus consejos e inmenso amor; por tu sacrificio cada mañana para hacerme cumplir con mis obligaciones. Por tu amor, preocupación y paciencia para enseñarme a hacer las cosas de la mejor manera. Te amo PA.

Les dedico este nuevo logro, porque gracias a ustedes llegué hasta este punto y me siento orgullosa y privilegiada de haberlos tenido a mi lado. Los amo con todo mi corazón.

Natalia Matiz Moya.

PRÓLOGO

Las nuevas tendencias tecnológicas han impulsado y motivado a las empresas a optar por soluciones que simplifiquen la administración y puesta en marcha de sus recursos, además de que deben generar beneficios como tener acceso a los servicios y las aplicaciones de la forma más rápida, eficiente y con plena confianza en sus datos e identidad se encuentran protegidos ante cualquier posible amenaza.

En base a la necesidad de tener los recursos, servicios y aplicaciones en una nube cuyo fin es que el usuario pueda tener acceso y hacer uso seguro de los mismos, según sus necesidades, nace el concepto y la necesidad de implementar *Cloud Computing* y *Cloud Security* a nivel de empresas, hospitales, universidades, corporaciones, etc.

Los Laboratorios del Departamento de Eléctrica y Electrónica, cuentan con una nube privada diseñada bajo la plataforma de virtualización Open Source “Xen Cloud Platform”; por lo que se estudió la necesidad de implementar *Cloud Security* en dicha nube para garantizar el acceso seguro a las aplicaciones y servicios que esta ofrece a los usuarios del Departamento.

El presente trabajo se basó en un rediseño de la nube e implementación de políticas y métodos de seguridad sobre los diferentes modelos de servicio que esta ofrece.

El **Capítulo 1**, contiene una introducción sobre lo que es *Cloud Computing*, su definición y conceptos; es decir una visión general de todo lo referente a esta nueva solución tecnológica.

El **Capítulo 2**, trata sobre todos los aspectos concernientes a la seguridad que se debe tener en una nube de *Cloud Computing*. En donde, se realiza un análisis de los riesgos y las vulnerabilidades que pueden presentarse en un entorno Cloud y las responsabilidades y obligaciones que recaen tanto el proveedor como en el cliente para ofertar y hacer uso de una nube de servicios.

El **Capítulo 3**, presenta un análisis profundo realizado a la nube implementada en los Laboratorios del DEEE; y, en base a este, se determinan las vulnerabilidades que presentan los tres modelos de servicios de la nube, IAAS, PAAS y SAAS.

En el **Capítulo 4**, se plantea un nuevo diseño para la nube implementada, con un plan de *Cloud Security* para la misma. Este diseño contempla todas las medidas de seguridad necesarias y que se deben implementar dependiendo de cada modelo de servicio que ofrece la nube.

En el **Capítulo 5**, se detallan los procesos realizados en la implementación de *Cloud Security* en la nube. Es decir, todas las soluciones escogidas para dotar de seguridad a todas las máquinas virtuales, los servicios y las aplicaciones que forman parte de la nube en Xen Cloud Platform.

Finalmente, en el **Capítulo 6**, se presentan las conclusiones y recomendaciones obtenidas de todo el proceso de análisis, diseño, desarrollo e implementación del presente proyecto.

Adicionalmente, en los **Anexos** se encuentra resumida la norma ISO/IEC 27001, que trata sobre Tecnología de la información, Técnicas de seguridad, Sistemas de gestión de seguridad de la información y los requerimientos, necesarios para dotar de seguridad a un sistema de información. Cabe recalcar, que en base a esta norma se propusieron las soluciones de seguridad en lo que se refiere a seguridad física de la nube implementada.

ÍNDICE DE CONTENIDOS

GLOSARIO	xix
CAPÍTULO I.....	1
INTRODUCCIÓN	1
1.1 ANTECEDENTES	1
1.2 JUSTIFICACION E IMPORTANCIA	3
1.3 OBJETIVOS	6
1.4 MARCO TEORICO.....	7
1.4.1 ¿Qué es Cloud Computing?	7
1.4.2 Características.....	8
1.4.3 Ventajas y Desventajas	10
1.4.4 Tipos de Infraestructura Cloud	11
CAPÍTULO II.....	22
SEGURIDAD EN LA NUBE	22
2.1 SEGURIDAD EN CLOUD COMPUTING.....	22
2.1.1 Riesgos del Cloud Computing	22
2.2 SEGURIDAD POR PARTE DEL PROVEEDOR	32
2.3 SEGURIDAD POR PARTE DEL CLIENTE	36
2.3.1 Nube Privada Comunitaria e Híbrida	36
2.3.2 Nube Pública	38
2.4 PRINCIPIOS PARA LA PROTECCION DE LA NUBE	39
2.4.1 Seguridad de la Identidad.....	40
2.4.2 Seguridad de la Infraestructura.....	40
2.4.3 Seguridad de la Información.....	41
CAPÍTULO III.....	45
ANÁLISIS DE LA NUBE EN XEN CLOUD PLATFORM.....	45
3.1 INFRAESTRUCTURA COMO SERVICIO.....	45

3.1.1	Características de los elementos Hardware de IAAS	46
3.1.2	Topología IAAS.....	47
3.2	SOFTWARE COMO SERVICIO.....	52
3.2.1	Servicio de Firewall.....	52
3.2.2	Servidor DNS.....	60
3.2.3	Servidor de Correo Electronico.....	62
3.2.4	Servidor Almacenamiento (OWNCLOUD) y Servidor Web.....	63
3.2.5	Servidor FREENAS	63
3.3	ANÁLISIS DE LA SEGURIDAD DE LA NUBE	64
3.3.1	Vulnerabilidades en IAAS	65
3.3.2	Vulnerabilidades en PAAS.....	67
3.3.3	Vulnerabilidades en SAAS.....	68
CAPÍTULO IV.....		70
DISEÑO DE LA SOLUCIÓN.....		70
4.1	DISEÑO DE LAS SOLUCIONES DE SEGURIDAD EN IAAS	70
4.1.1	Seguridad Física.....	71
4.1.2	Seguridad Lógica (Infraestructura Virtual)	76
4.2	SOLUCIONES DE SEGURIDAD EN PAAS	85
4.3	SOLUCIONES DE SEGURIDAD EN SAAS	89
4.3.1	Servicio de Correo Electrónico Zimbra	89
4.3.2	Servicio OwnCloud	90
CAPÍTULO V.....		91
IMPLEMENTACIÓN DE CLOUD SECURITY.....		91
5.1	IMPLEMENTACIÓN DE CLOUD SECURITY EN IAAS	91
5.1.1	Implementación de la SOLUCIÓN A: Alta Disponibilidad de Servidores Físicos	91
5.1.2	Implementación de la SOLUCIÓN B: Firewalls de Alta Disponibilidad.....	96

5.1.3	Implementación de la SOLUCION C: Redistribución de Recursos de la Nube.....	116
5.2	IMPLEMENTACIÓN DE CLOUD SECURITY EN PAAS.....	128
5.2.1	Implementación de la SOLUCIÓN A.....	128
5.2.2	Implementación de la SOLUCIÓN B.....	130
5.2.3	Implementación de la SOLUCIÓN C	133
	CAPÍTULO VI.....	142
	CONCLUSIONES Y RECOMENDACIONES	142
6.1	CONCLUSIONES.....	142
6.2	RECOMENDACIONES	144
	REFERENCIAS BIBLIOGRÁFICAS	145

ÍNDICE DE FIGURAS

Figura 1. 1 Nube Pública [8].....	12
Figura 1. 2 Nube Privada	13
Figura 1. 3 Nube Comunitaria	15
Figura 1. 4 Nube Hibrida	16
Figura 1. 5 Ejemplos de servicios en los niveles de Cloud Computing [4]	20
Figura 1. 6 Niveles de servicio del Cloud Computing [29]	21
Figura 2. 1 Tipos de ataques	24
Figura 2. 2 Cómo funciona una botnet. Caso 1	26
Figura 2. 3 Cómo funciona una botnet. Caso 2	26
Figura 2. 4 Causas de pérdida de datos	29
Figura 2. 5 Robo de Identidad.....	31
Figura 2. 6 Certificado de conexión segura a la página del banco de Guayaquil.....	34
Figura 2. 7 Ejemplo de conexión segura mediante SSH y VPN.....	35
Figura 2. 8 Firewall Perimetral.....	37
Figura 2. 9 Sistema de protección de una red mediante IDS, firewall	38
Figura 2. 10 Retos de seguridad en la nube	39
Figura 2. 11 Elementos principales para proteger la nube	40
Figura 3. 1 Topología IAAS. Hardware	48
Figura 3. 2 Topología IAAS. Virtualizado	50
Figura 3. 3 Topología Firewall-Endian.....	54
Figura 3. 4 Tráfico de entrada Firewall-Endian.....	55
Figura 3. 5 Tráfico de salida Firewall-Endian	56
Figura 3. 6 Trafico de Interno entre zonas. Firewall-Endian.....	58
Figura 3. 7 Prueba del Servidor DNS	61
Figura 3. 8 Registros Configurados en el servidor DNS.....	61
Figura 3. 9 Servidor de Correo Zimbra.....	62
Figura 3. 10 Servidor FreeNAS	64
Figura 4. 1 Diseño de Alta Disponibilidad de Servidores XCP	79

Figura 4. 2 Alta Disponibilidad de Firewall PFSENSE	82
Figura 4. 3 Diseño de Redistribución de la nube. Servidor FreeNAS.....	84
Figura 4. 4 Diseño de la solución PAAS.....	88
Figura 5. 1 Características de XCP vs. Xen Server	92
Figura 5. 2 Clúster de servidores XCP	93
Figura 5. 3 Configuración de Alta Disponibilidad.....	95
Figura 5. 4 Alta Disponibilidad configurada	95
Figura 5. 5 Creación de nueva Máquina Virtual	97
Figura 5. 6 Selección de tipo de VM.....	97
Figura 5. 7 Nombre de la VM	98
Figura 5. 8 Selección de ubicación de imagen iso	98
Figura 5. 9 Selección de Servidor en donde se instalará la MV	99
Figura 5. 10 Selección de cantidad de CPU's y memoria de la VM	99
Figura 5. 11 Selección de Virtual Disk y tamaño del mismo.....	100
Figura 5. 12 Selección de interfaces virtuales de la VM.....	100
Figura 5. 13 Creación de la VM.....	101
Figura 5. 14 Creación de nueva interfaz	102
Figura 5. 15 Creación de la interfaz	102
Figura 5. 16 Interfaz de Sincronización añadida en PFSense.....	103
Figura 5. 17 Interfaz de configuración de PFSense	103
Figura 5. 18 Asignación de tarjetas de red a Interfaces de PFSense.....	104
Figura 5. 19 Configuración de Interfaces de red. PFSense Master.....	104
Figura 5. 20 Configuración de Interfaces de red. PFSense Slave.....	105
Figura 5. 21 Configuración básica de PFSense	105
Figura 5. 22 Configuración de Interface LAN. PFSense Master.....	106
Figura 5. 23 Configuración de Interface DMZ. PFSense Master.....	106
Figura 5. 24 Configuración de Interface WAN. PFSense Master	107
Figura 5. 25 Configuración de Interface de sincronización. PFSense Master	107
Figura 5. 26 Configuración de NAT: Port Forward	108
Figura 5. 27 Configuración de NAT: Outbound	108
Figura 5. 28 Configuración Reglas para la WAN.....	109

Figura 5. 29 Configuración Reglas para la LAN	110
Figura 5. 30 Configuración Reglas para la DMZ	110
Figura 5. 31 Configuración Reglas para la interfaz de Sincronización	111
Figura 5. 32 Configuración Virtual IP para CARP en WAN	112
Figura 5. 33 Virtual IP's para configuración de CARP	113
Figura 5. 34 Configuración de CARP Setting MASTER	114
Figura 5. 35 Configuración de CARP Setting SLAVE.....	115
Figura 5. 36 Status de Configuración de CARP en MASTER	116
Figura 5. 37 Status de Configuración de CARP en SLAVE.....	116
Figura 5. 38 Configuración de nueva Red en XCP.....	117
Figura 5. 39 Parámetros de VLAN	118
Figura 5. 40 VLAN's creadas (LAN y DMZ).....	118
Figura 5. 41 VLAN's creadas Switch 3Com.....	119
Figura 5. 42 Nuevas interfaces asignadas a PFSense.....	120
Figura 5. 43 VLAN's creadas en PFSense.....	120
Figura 5. 44 Configuración IP FreeNAS	121
Figura 5. 45 Configuración de rutas estáticas.....	122
Figura 5. 46 Ingreso de IP's permitidas	121
Figura 5. 47 Configuración de rutas estáticas en XCP.....	122
Figura 5. 48 Pruebas de conectividad entre XCP y FreeNAS	122
Figura 5. 49 Almacenamiento CIFS y NFS de FreeNAS en XCP.....	123
Figura 5. 50 Características de la versión de XCP instalada	124
Figura 5. 51 Características de las versiones de XenCenter	126
Figura 5. 52 Características y costos de las versiones de XenCenter	127
Figura 5. 53 Código Oinkcode. Actualización de reglas	129
Figura 5. 54 Configuración de interfaces a monitorear.....	129
Figura 5. 55 Configuración de HAVP	130
Figura 5. 56 Configuración de proxy y actualizaciones	131
Figura 5. 57 IP de PC conectada a la LAN.....	131
Figura 5. 58 Bloqueo de página con virus por HAVP	132
Figura 5. 59 Lista de virus detectados por HAVP	132

Figura 5. 60 Prueba hacia IP de Zimbra.....	133
Figura 5. 61 Servidor DNS en Windows Server 2008	134
Figura 5. 62 Grupos Creados	135
Figura 5. 63 Usuarios asignados a Grupos Creados.....	135
Figura 5. 64 Usuarios y roles en XenCenter.....	137
Figura 5. 65 Consola de WSS	138
Figura 5. 66 Usuarios de AD	139
Figura 5. 67 Máquinas virtuales de XCP	139
Figura 5. 68 Usuario UserW1 realizando una petición	140
Figura 5. 69 Petición recibida por el administrador y asignación de requerimiento a Usuario	141
Figura 5. 70 Máquina virtual asignada a Usuario	141

ÍNDICE DE TABLAS

Tabla 1. 1 Ventajas y desventajas de los modelos de Despliegue.....	17
Tabla 2. 1 Mecanismos de Seguridad: Proveedor vs. Cliente	43
Tabla 3. 1 Características de los equipos hardware	47
Tabla 3. 2 Direccionamiento IP de la Topología IAAS.....	49
Tabla 3. 3 Vulnerabilidades en IAAS.....	67
Tabla 3. 4 Vulnerabilidades en PAAS	68
Tabla 5. 1 Usuarios y roles	136

GLOSARIO

- Spam** Correo basura, mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, enviados en grandes cantidades (masivas) que perjudican de alguna o varias maneras al receptor.
- DDoS** Conocido como Ataque de denegación de servicios. Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios.
- ICMP** Es el Protocolo de Mensajes de Control de Internet, el cual da control y notificación de errores del Protocolo de Internet (IP). Es decir, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.
- DNS** Sistema de nombres de dominio.
- API** Interfaz de programación de aplicaciones, es el conjunto de funciones y procedimientos (programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.
- Malware** También llamado badware, código maligno, o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.
- Phishing** Es un término informático que denomina un tipo de delito dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso

de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria.

- Hipervisor** Es una plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos en una misma computadora.
- SSL, TLS** Son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.
- SSH** Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.
- VPN** Es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada.
- UDP** Es un protocolo del nivel de transporte basado en el intercambio de datagramas
- HTTP** Protocolo de transferencia de hipertexto. El propósito del protocolo es permitir la transferencia de archivos entre un navegador y un servidor web.
- HTTPS** Protocolo de transferencia de hipertexto de forma segura. A diferencia de HTTP utiliza un cifrado basado en SSL (**Secure Socket Layers**), creando un canal de transferencia cifrado para aumentar la seguridad en la transferencia de datos.

- IP** Protocolo de Transferencia de Archivos entre sistemas conectados a una red TCP, funciona en la capa de red del modelo OSI.
- SMTP** Protocolo para la transferencia simple de correo electrónico entre ordenadores o dispositivos, que funciona en la capa de aplicación.
- POP** Protocolo de Oficina de Correo, en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de la capa de aplicación del modelo OSI.
- IMAP** Internet Message Access Protocol, es un protocolo de la capa de aplicación, que permite el acceso a mensajes electrónicos almacenados en un servidor.
- POP3s** Post Office Protocol versión 3, dirigido a través de la capa SSL que permite la obtención de correo electrónico de manera segura.
- IMAPs** Internet Message Access Protocol dirigido a través de la capa SSL.
- TI** Tecnologías de Información.

CAPÍTULO I

INTRODUCCIÓN

1.1 ANTECEDENTES

El concepto de “*Cloud Computing*” ha ganado popularidad debido a que las infraestructuras de TI² se han vuelto demasiado complejas y frágiles para soportar el ritmo y el dinamismo de la empresa actual [1]., es decir, debido a la gran demanda de aplicaciones comerciales tradicionales, ya que al ser costosas y cada una con requerimientos específicos necesarios de hardware y de software para ejecutarlas, se requiere de cierto conocimiento para la instalación, configuración, pruebas de funcionamiento y ejecución, seguridad y actualizaciones, o bien de un técnico que realice el trabajo.

Por esta razón el uso de “*Cloud Computing*” cada vez es mayor no solo por parte de grandes empresas, sino también por parte de pequeñas y medianas empresas y usuarios independientes.

Se puede definir a “*Cloud Computing*” como una solución para tener los servicios y las aplicaciones requeridas por el usuario a través de internet; es decir, es **un nuevo concepto tecnológico que se basa en que las aplicaciones de software** y los equipos (hardware) con capacidad de proceso y almacenaje de datos no están en el PC o equipos del usuario, sino que están ubicados en un

² TI: Tecnologías de Información

Datacenter que permite a los usuarios acceder a las aplicaciones y los servicios disponibles a través de Internet [2].

Al tener las aplicaciones y los servicios en una nube, es importante tomar en cuenta ciertas consideraciones de seguridad de los datos y la información que se montarán sobre la nube para precautelar la privacidad de los usuarios y su información, ya que la mayoría de empresas manejan datos de vital importancia y de suma confidencialidad, por lo tanto es un riesgo que la información caiga en manos malintencionadas que puedan alterar o hacer uso erróneo de la misma.

Dar toda la seguridad posible y necesaria en la nube para proteger la información y la integridad de los datos del usuario se conoce como *Cloud Security*.

Según la Enciclopedia Libre Wikipedia, *Cloud Security* se define como: **“Cloud Security es una evolución de la seguridad informática, seguridad de la red y seguridad de la información. Se refiere a un amplio conjunto de políticas, tecnologías y controles implementados para proteger los datos, las aplicaciones y la infraestructura asociada de la computación en nube.”**³

[3]

Como toda tecnología, el “*Cloud Computing*” no está exento de riesgos. Cuanto más compleja es la infraestructura informática utilizada, más vulnerabilidades aparecen [3], por lo que es importante conocer los principales riesgos de seguridad y privacidad que pueden generar un impacto en los recursos en la nube, y como dar protección o seguridad a la nube.

Según un estudio realizado por INTECO⁴, utilizar los servicios en la nube conlleva un cambio en la forma de entender la seguridad informática. Deja de existir la imagen tradicional en la que todos los servidores de la empresa están en

³ Enciclopedia Libre Wikipedia. Cloud Computing Security. Septiembre 2012.

⁴ INTECO: Instituto Nacional de Tecnologías de la Comunicación. España.

el sótano del edificio donde solo pueden acceder los administradores informáticos. Al hacer uso del “*Cloud Computing*”, una parte importante de la seguridad del sistema recae sobre la empresa que provee los servicios en la nube.[4]; por lo que podemos concluir que, así como “*Cloud Computing*” es considerada como una solución tecnológica importante que proporciona una fórmula mucho más eficaz, flexible y rentable para las empresas en constante crecimiento; es también vulnerable a obstáculos y amenazas que puedan frenar su avance tecnológico y pongan en riesgo la privacidad de los usuarios.

1.2 JUSTIFICACION E IMPORTANCIA

Al tener en la nube innumerables aplicaciones que albergan una cantidad considerable de datos, tanto las empresas proveedoras del servicio como las empresas que hacen uso de la nube deben implementar controles de seguridad al igual que en sistemas tradicionales, sin embargo debido a los modelos operacionales y tecnologías usadas para activar los servicios Cloud, se presentan riesgos y amenazas de diferente índole que se debe tomar en cuenta para implementar distintas soluciones de seguridad.

Por ejemplo, el control de acceso a los servidores, la gestión de identidades y el acceso a las aplicaciones, la protección de la información de cada usuario, y el uso de estándares.

Una de las desventajas de “*Cloud Computing*” respecto a la seguridad es que, con excepción de las Cloud privadas, los clientes no son propietarios de la infraestructura física y, por tanto, se produce una pérdida de control sobre los activos de la nube.

En los tres modelos de servicio en la nube, Infraestructura como Servicio, Plataforma como Servicio y Software como Servicio (IaaS, PaaS y SaaS), los

servidores reales son controlados y operados por el “*Cloud Provider*”⁵, por lo que dependiendo del servicio que nos brinde la nube se debe considerar algunos aspectos de seguridad para precautelar la información.

A nivel de proveedor Cloud, si se oferta un servicio IaaS se debe considerar capacidad de almacenamiento y procesamiento en la nube por lo que es importante controlar la carga en los servidores y precautelar la información como por ejemplo, montando servidores de respaldo para que la información este salvaguardada en caso de pérdida de la misma.

En el caso SaaS, al tener aplicaciones de diferente índole para el usuario montadas en la nube, es importante controlar la disponibilidad de los servicios montados en la nube, realizar balanceo de carga⁶ y redundancia para tener disponibilidad de los servicios al cien por ciento.

Y, en el caso de PaaS, permite al usuario desarrollar e implementar aplicaciones desde el internet, por lo que es importante tomar en cuenta los servicios de integración de la base de datos, escalabilidad, almacenaje, copias de seguridad, para precautelar las aplicaciones realizadas por los usuarios.

A nivel de cliente, es importante, definir claramente los roles y derechos de los usuarios, además de poner en orden los sistemas de la empresa, con la ayuda de soluciones de modelado de roles automatizadas antes de adoptar soluciones en la nube, ya sean privadas, públicas o híbridas.

En general, los controles de seguridad en la nube se implementan a nivel físico, de red, del sistema y de las aplicaciones. Para la seguridad de los sistemas tradicionales típicamente se incluye un firewall, zonas delimitadas, segmentación de redes, detección de intrusos y herramientas de monitoreo de red, y “*Cloud Computing*” vuelve a tomar como referencia a éstas técnicas, pero la

⁵ **Cloud Provider:** Proveedor de Cloud Computing.

⁶ **Balanceo de Carga:** técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos.

responsabilidad de la seguridad es tanto del proveedor como del consumidor dependiendo de los modelos utilizados.

Por ejemplo, la infraestructura AWS EC2 de Amazon como oferta de servicios, incluye responsabilidad de seguridad por parte del proveedor hasta el hypervisor, lo que significa que solo tiene control sobre seguridad física, ambiental y de virtualización [5].

El consumidor, a su vez, es responsable de los controles de seguridad que se relacionan con el sistema informático, incluyendo el sistema operativo, aplicaciones y datos.

Debido a las razones expuestas, las empresas o usuarios que hagan uso o sean proveedores de esta solución tecnológica deben tomar en cuenta criterios básicos de seguridad para que puedan hacer uso de las ventajas de la nube de una forma segura.

La importancia de la seguridad de la información hoy en día, es fundamental, por lo que es necesario realizar el estudio de las vulnerabilidades y amenazas a las que se enfrenta cualquier sistema Cloud Computing.

Por lo tanto, con el presente proyecto se dará seguridad al sistema Cloud Computing en la plataforma Xen Cloud para el Departamento de Eléctrica y Electrónica de la Escuela Politécnica del Ejército; de tal manera que su uso por parte de los diferentes usuarios sea totalmente confiable y con la tranquilidad de que su información tendrá un respaldo en caso de pérdida de la misma.

1.3 OBJETIVOS

General

- Implementar *Cloud Security* para un sistema basado en Xen Cloud Platform, a fin de garantizar la seguridad y la integridad de la información y sus respectivos usuarios.

Específicos

- Investigar las vulnerabilidades, riesgos y amenazas a las que se debe enfrentar un sistema de Cloud Computing.
- Analizar el sistema Cloud basado en Xen Cloud Platform, y las diferentes vulnerabilidades a las que está expuesto.
- Rediseñar la nube implementada de tal manera que cuente con todas las medidas de seguridad necesarias para prevenir ataques y posibles vulnerabilidades.
- Implementar *Cloud Security* en la nube para robustecer el sistema y dar mayor seguridad a los datos y la información de los usuarios, así como la integridad de los mismos.

1.4 MARCO TEORICO

1.4.1 ¿Qué es *Cloud Computing*?

Cloud Computing es conocida como una nueva tecnología **que permite ofrecer servicios de computación a través de Internet, es decir, servicios que sean solicitados por usuarios como almacenamiento, correo, aplicaciones, etc., que estén disponibles en la nube de internet.**

Según NIST⁷ (Instituto Nacional de Estándares y Tecnología, EEUU), *Cloud Computing* es: **“Un modelo para permitir un acceso conveniente a la red y bajo demanda, a un conjunto de recursos de computación configurables y compartidos (por ejemplo, redes, servidores, almacenamientos, aplicaciones y servicios) que pueden proporcionarse rápidamente con un mínimo de esfuerzo de gestión o de interacción del proveedor del servicio. Este modelo o paradigma de nube promueve la disponibilidad.”** [6]

Con esta definición se puede decir que *Cloud Computing* es un nuevo modelo de tecnología avanzada en el cual se tiene la prestación de servicios informáticos según las necesidades del usuario, con el propósito de ser escalable, flexible y con alta disponibilidad.

Gracias a esta nueva tecnología el usuario puede manejar los servicios que oferte la nube según sus requerimientos. Al ser tan versátil y flexible, proporciona herramientas como software, infraestructura o plataforma como servicio según sea la necesidad del usuario.

No obstante, si *Cloud Computing* pretende satisfacer las necesidades de los usuarios de una manera eficaz, es importante también la confidencialidad de los datos del Cliente y el cumplimiento de las directivas legales, por lo que es

⁷ NIST (Instituto Nacional de estándares y tecnología). NIST Special Publication 500 a 291, NIST Cloud Computing Normas Hoja de Ruta, julio de 2011.

indispensable proporcionar niveles más altos de seguridad para brindar soporte a las aplicaciones y los servicios requeridos por los clientes.

1.4.2 Características

La principal característica de *Cloud Computing* es el acceso ubicuo⁸, es decir que se puede acceder a la nube desde cualquier parte y al momento que el usuario así lo requiera; sin necesidad de instalar un software específico o un sistema operativo determinado; simplemente se requiere de un dispositivo con acceso a internet con un navegador web.

A pesar de que esta característica significa una gran ventaja para los clientes, es importante considerar que la velocidad de conexión a internet que el usuario tenga, debe ser alta y de buena calidad, ya que de esto dependerá la rapidez con la cual pueda acceder a las aplicaciones y utilizar el servicio de forma correcta. [4]

Cloud Computing tiene cinco características esenciales definidas por NIST[6]:

6.1 Rapidez y Elasticidad: Esta característica permite el crecimiento de la capacidad de los recursos que provee la nube al cliente, es decir, tener la posibilidad de añadir o eliminar recursos según las necesidades del cliente, realizando el redimensionamiento correspondiente de una manera rápida y efectiva. Por ejemplo, aumento de almacenamiento o número de procesadores sin que la aplicación se vea afectada, o reducción de recursos para adecuarlos a las necesidades del cliente.

6.2 Servicio Supervisado: Dependiendo del tipo de nube que tenga el cliente, la empresa que lo provea de los servicios tendrá control y

⁸ **Ubicuo:** Que está presente a un mismo tiempo en todas partes.

supervisión de todos los aspectos que encierran las nube, como mantenimiento de hardware, recintos especializados para procesamiento de datos, suministro eléctrico, conectividad a internet, copias de seguridad, etc.[4]. Además de que se encargarán del control y optimización de los recursos, para monitorearlos brindando transparencia tanto para el proveedor como para el cliente, a fin de mantener la facturación del servicio.

- 6.3 Auto-servicio bajo Demanda:** El cliente puede hacer uso de mecanismos para adquirir recursos según sean sus necesidades de manera automática, es decir, sin la necesidad de un proveedor de servicios en la nube. De tal manera que pueda añadir o disminuir el volumen de recursos contratados en función a sus necesidades, sin necesidad de interacción humana con el proveedor.
- 6.4 Amplio acceso a la red:** El cliente tiene la posibilidad de acceder a los recursos de la nube a través de una conexión a internet desde cualquier dispositivo con la suficiente capacidad de procesamiento, como por ejemplo teléfonos móviles, computadoras portátiles, PDA's,etc.
- 6.5 Fondo común de recursos:** Los servicios informáticos del proveedor son agrupados de tal manera que puedan ser usados por múltiples clientes, usando un modelo multi-arrendatario según las necesidades del cliente. Es decir, recursos físicos y virtuales que incluyen: procesamiento, memoria, ancho de banda y máquinas virtuales: asignados de forma dinámica y reasignados según las necesidades del cliente.

1.4.3 Ventajas y Desventajas

Cloud Computing al ser una tecnología flexible y rentable, presenta ventajas que permiten a los clientes y grandes empresas a usar frecuentemente los servicios y recursos que provee la nube. Las ventajas son:

- **Accesibilidad:** Tener la posibilidad de acceder a la información y los servicios desde cualquier lugar según las necesidades del cliente.
- **Disponibilidad del servicio,** aplicación web y recursos todos los días y a cualquier hora del día, según sea el requerimiento del cliente.
- **Reducción de gastos** en infraestructura, mantenimiento y servicios, ya que al ser una tecnología montada en la nube de internet, no se requiere de mano de obra para mantenimiento de equipos o instalación de aplicaciones o servicios.
- **Servicios gratuitos y de pago** según las necesidades del usuario.
- **Capacidad de procesamiento y almacenamiento** sin instalar máquinas localmente, es decir, es escalable ya que mediante la infraestructura que ya está implementada se puede adquirir más servicios o más capacidad según las necesidades del cliente.

Por otro lado, al ser una tecnología relativamente nueva, aún existen algunos inconvenientes en la nube sobre todo en el sentido de seguridad de la información. Entre las desventajas tenemos:

- **Privacidad de los datos** ya que la información estará en servidores ajenos, es decir en los servidores del proveedor de servicios de la nube.

- Dependencia de los servicios en línea y de la disponibilidad de la empresa proveedora. Además de tener siempre un proveedor de internet y de su velocidad de funcionamiento.
- Robo de datos o de información almacenada en los servidores de la empresa, al igual que suplantación de identidad de los clientes y abuso de recursos e información.

1.4.4 Tipos de Infraestructura Cloud

La infraestructura de la nube está compuesta de un conjunto de elementos y recursos que proporcionan servicios que los usuarios pueden usar según sus necesidades, esta infraestructura se la puede categorizar en modelos de despliegue que describen el tipo de nube, es decir como se la crea y se la pone en funcionamiento; y, en modelos de servicios que son todos aquellos que puede proporcionar la nube, como software, plataforma o infraestructura.

A. MODELOS DE DESPLIEGUE

▪ Nube Pública

La nube pública tiene una infraestructura a gran escala que pone a disposición los servicios y recursos de ésta, de forma dinámica a través de internet, para cualquier usuario o grupo empresarial que lo requiera en cualquier momento y lugar.

El proveedor de los servicios de la nube es dueño de la infraestructura física, además de ser el administrador que gestiona los servicios, recursos, procesos y datos. Y es quien cobra por el uso de los recursos de la nube según sea la

demanda del cliente, por lo que es considerado un sistema prepago, en donde el cliente cancela el valor de lo que utiliza en la nube.

Es decir, múltiples usuarios pueden utilizar servicios web que son procesados en el mismo servidor, pueden compartir espacio en discos u otras infraestructuras de red con otros usuarios.



Figura 1. 1 Nube Pública [8]

La ventaja de una nube pública es la capacidad de almacenamiento y procesamiento sin necesidad de instalar máquinas localmente, por lo tanto, el cliente no debe realizar ningún gasto adicional, ni en instalación, ni en mantenimiento; simplemente paga lo que consume.

El manejo de los datos y la respectiva seguridad que se le dé a estos, como copias de seguridad (backups) y seguridad al acceso de los mismos; es responsabilidad del proveedor tanto de hardware como de software.

La desventaja de esta nube es que el cliente depende de una conexión a internet para poder hacer uso de los servicios de la nube, además de dejar toda su información en los servidores de la empresa proveedora.

▪ Nube Privada

La nube privada es aquella que es creada y administrada por una sola organización u empresa; y no ofrece servicios a terceros. Las instalaciones y servidores se encuentran dentro de la misma; es decir, es una plataforma administrada por una sola organización y es utilizada para la obtención de hardware, como máquinas, almacenamiento e infraestructura de red (IaaS), y también aplicaciones como Plataforma como Servicio (PaaS) e incluso aplicaciones Software como Servicio (SaaS).

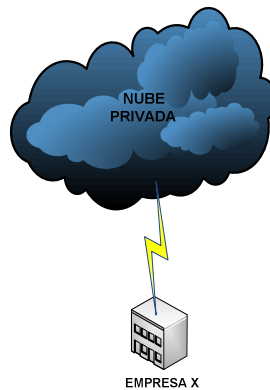


Figura 1. 2 Nube Privada

Este tipo de nube es más segura que la nube pública ya que los datos e información permanecen en la infraestructura de la entidad, y son controlados y gestionados por la misma. Por lo que los usuarios mantienen su privacidad y confidencialidad de los datos, al ser la empresa la encargada de comprar, mantener y administrar la infraestructura hardware y software de la nube.

Por lo tanto la ventaja de esta nube será la mejora en seguridad y protección de los datos por parte de la misma organización; además de la disponibilidad de las aplicaciones y recursos, reducción de costos, etc.

Sin embargo, la desventaja de este tipo de nube es la inversión inicial que le toca cubrir a la empresa para su implementación, es decir, la infraestructura física, sistemas de virtualización, ancho de banda y seguridad, lo que llevará a su vez a pérdida de escalabilidad de las plataformas, sin olvidar el gasto de mantenimiento que requiere. [8]

- **Nube Comunitaria**

Este tipo de nube tiene una infraestructura que es compartida por varias organizaciones o empresas, de tal manera que comparten los servicios y recursos de la nube, a manera de una comunidad en donde los usuarios tienen intereses compartidos y objetivos similares; como por ejemplo, requisitos de seguridad, políticas y condiciones de cumplimiento, privacidad de los datos, etc.

Al ser una nube que comparte sus recursos entre dos entidades o empresas, se puede decir que es considerada como una variación de una nube privada, ya que posee las mismas características de esta con la diferencia de brindar servicios y recursos a dos organizaciones o más, y no solo a una.

Además, este tipo de nube puede ser administrada y gestionada por la comunidad o por un tercero; y puede estar implementada en las instalaciones de una de las compañías, como también fuera de ellas.

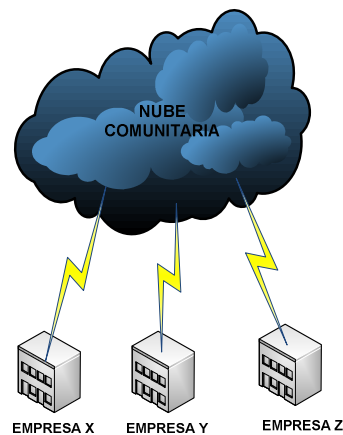


Figura 1. 3 Nube Comunitaria

▪ Nube Híbrida

Este tipo de modelo de nube es considerado como una combinación de los modelos ya descritos.

Según el libro Cloud Application, el modelo de nube híbrida está definida de la siguiente manera:

“El modelo híbrido combina los modelos anteriormente descritos, sobre nubes públicas y privadas, de manera que se aprovecha la ventaja de localización física de la información gestionada por las nubes privadas con la facilidad de ampliación de recursos de las nubes públicas”⁹[9]

Este tipo de nube implica la utilización conjunta de varias infraestructuras que se mantienen como entidades separadas pero que a su vez están unidas por medio de la tecnología propietaria o estandarizada, permitiendo tener portabilidad de los datos y las aplicaciones; además de tener la posibilidad de realizar balanceo de carga entre las nubes cuando una de estas se encuentra ocupada hasta su capacidad máxima.

⁹ GEORGE REESE. Cloud Application Architectures: Building Applications and Infrastructure in the CloudTheory in Practice (o'Reilly) Series. Capítulo 1, páginas 19-21. 2009.

Las empresas que hagan uso de este tipo de nube pueden compartir su información, pero con medidas de seguridad y permisos para el acceso a ellos.

Al ser una nube compuesta por una pública y por otra privada, la administración y gestión de la nube híbrida, se da por parte del proveedor y de la empresa que la utiliza; satisfaciendo así las necesidades de los usuarios.

Por ejemplo, una empresa hace uso de una nube pública para mantener su servidor web, mientras que su servidor de bases de datos se encuentra en su nube privada. Por lo tanto existe un canal de comunicación entre la nube pública y privada mediante el cual los datos sensibles permanecen bajo el control y gestión de la empresa; mientras que el servidor web es administrado por un tercero. [4]

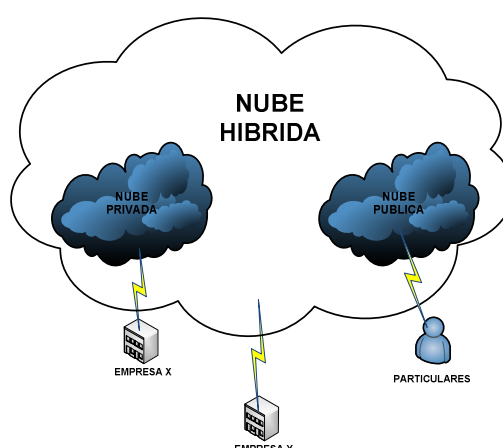


Figura 1. 4 Nube Híbrida

INTECO¹⁰, en su manual “*Amenazas y Riesgos en Cloud Computing*”, resume en un cuadro las ventajas y desventajas de los tres tipos de modelos de despliegue de *Cloud Computing*, público, privado y comunitario. [7]

¹⁰ INTECO: Instituto Nacional de Tecnologías de la Comunicación. España.

Tabla 1. 1 Ventajas y desventajas de los modelos de Despliegue

MODELOS DE DESPLIEGUE	VENTAJAS	DESVENTAJAS
NUBE PÚBLICA	Escalabilidad	Se comparte la infraestructura con varias empresas u organizaciones.
	Recursos eficientes mediante modelos de pago por uso.	Poca transparencia para el cliente, porque no se conoce el resto de servicios que comparten recursos, almacenamiento, etc.
	Ahorro de tiempo y costos de instalación	Seguridad por parte de un tercero.
NUBE PRIVADA	Cumplimiento de las políticas internas	Elevado costo de instalación y equipos
	Facilidad de trabajo en la nube y seguridad en los datos por parte de la empresa	Dependencia de la infraestructura contratada
	Control total de los recursos	Retorno de la inversión lento debido a que su servicio es para la misma empresa
NUBE COMUNITARIA	Cumplimiento de las políticas internas	Seguridad dependiente por parte del administrador de la nube
	Reducción de costos de implementación y uso, al compartir la infraestructura y recursos.	Dependencia de la infraestructura contratada

B. MODELOS DE SERVICIOS

▪ SOFTWARE COMO SERVICIO (SAAS)

Este modelo brinda la capacidad al usuario de tener un despliegue de software como aplicación a través del internet, en el cual las aplicaciones y los recursos computacionales están diseñados para usarlos bajo demanda.

Las aplicaciones se ejecutan en la infraestructura de la nube y son accesibles a los usuarios desde cualquier equipo como pc's, notebooks, teléfonos móviles, etc., según sea la necesidad del cliente a manera de pago por consumo; reduciendo costos de software y hardware, así como también de mantenimiento y operación.

Por lo general la interfaz del cliente para acceder a la aplicación es ligera, a manera de un navegador web, como por ejemplo, el correo electrónico basado en web o web mail; sin la necesidad de instalar programas adicionales para hacer uso del servicio.

La seguridad de este servicio depende del proveedor, ya que el cliente únicamente tiene acceso a la edición de las preferencias de la aplicación y a privilegios administrativos limitados.

Las actualizaciones, mejoras o parches en la aplicación del cliente, deben ser siempre transparente al usuario, y a la vez debe ser automático de tal manera que el cliente no deba hacer ningún tipo de configuración.

Este modelo es muy versátil ya que soporta múltiples usuarios generalmente con un modelo multi-tenant.¹¹

¹¹ **Multi-tenant:** Derivada de la palabra **Multi – tenancy:** Es una arquitectura en la que una sola instancia de una aplicación de software ofrece múltiples clientes.

- **PLATAFORMA COMO SERVICIO (PAAS)**

Este modelo propone un entorno software en el cuál un desarrollador puede crear y gestionar soluciones dentro de un contexto de herramientas de desarrollo que la plataforma proporciona. [10]

Este tipo de nube proporciona al consumidor la capacidad de desplegar aplicaciones creadas por el consumidor de la infraestructura de la nube, utilizando lenguajes de programación específicos y herramientas como java, Python, etc. El servicio de la nube se entrega bajo demanda, desplegando aplicaciones en hardware y software.

Los clientes tienen la posibilidad de interactuar con el software para introducir y recuperar datos, etc. Mientras que el proveedor es el que se encarga de controlar y gestionar la infraestructura de la nube, es decir, todos los aspectos de red, servidores, sistemas operativos, almacenamiento, etc.

Con la plataforma como servicio, se reducen los costes y la complejidad de la compra, el mantenimiento, el almacenamiento y el control del hardware y el software que componen la plataforma.

- **INFRAESTRUCTURA COMO SERVICIO (IAAS)**

Este modelo está definido como un modelo de servicios de computación escalables según sean las necesidades del usuario.

La capacidad que proporciona al cliente es la provisión de procesamiento, almacenamiento, redes y recursos de computación en donde el usuario puede desplegar y ejecutar sistemas operativos y desarrollar o probar aplicaciones.

El usuario dispone de una o varias máquinas virtuales en la nube con las que, puede aumentar el tamaño de disco duro, obtener mayor capacidad de proceso, probar aplicaciones y pagar solamente por los recursos que utilice.

El proveedor se encarga de provisionar, gestionar y controlar los servidores, almacenamiento, red, etc., mientras que los consumidores tienen la capacidad de controlar los sistemas operativos, el almacenamiento y las aplicaciones desplegadas según sean sus necesidades.

En el siguiente gráfico se muestra un ejemplo de los servicios entregados en cada nivel de modelo de servicio de *Cloud Computing*. [4]

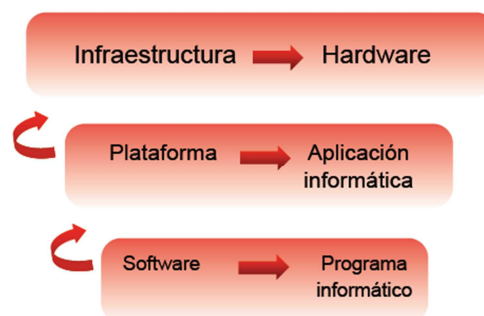


Figura 1. 5 Ejemplos de servicios en los niveles de Cloud Computing [4]

Adicionalmente, en la figura 1.6 se puede observar como se distinguen y caracterizan los tres niveles de servicio; en el lado izquierdo se observa como unos servicios se constituyen sobre los otros, mientras que en el lado derecho se especifican las características de los componentes de cada nivel de servicio.

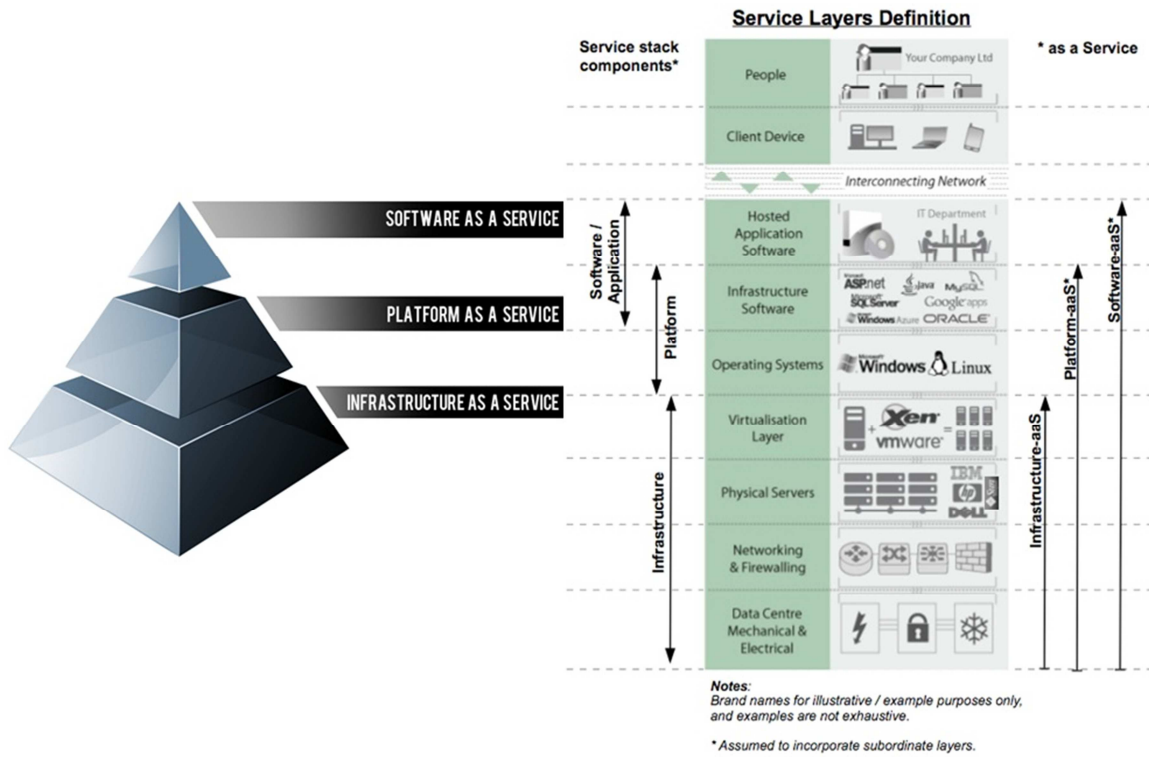


Figura 1. 6 Niveles de servicio del Cloud Computing [29]

CAPÍTULO II

SEGURIDAD EN LA NUBE

2.1 SEGURIDAD EN CLOUD COMPUTING

Cloud Computing al ser uno de los elementos más importante en las TIC's¹² tiene como objetivo principal precautelar la integridad de los datos y la privacidad de los usuarios.

Si la infraestructura informática utilizada es compleja, mas vulnerabilidades y riesgos pueden aparecer, por lo tanto es importante conocer los principales riesgos de seguridad y privacidad que pueden generar un impacto en los recursos de la nube. Además de las medidas de seguridad que deben tomar tanto los proveedores de la nube como los clientes; así como en la virtualización.

2.1.1 Riesgos del Cloud Computing

Como en toda tecnología, existen riesgos en la seguridad de los datos por parte de terceros que mediante aplicaciones y software especiales pueden invadir la privacidad de los usuarios y hacer uso de su información.

¹² TIC'S: Tecnologías de información y comunicación.

La creciente popularidad del *Cloud Computing* y de la virtualización entre las empresas y el mundo de las TIC's, ha provocado que los criminales cibernéticos pongan su atención en la nube para realizar estafas y perjudicar a las miles de empresas que hoy en día utilizan a la nube como una solución tecnológica.

Symantec en su Informe Anual sobre Amenazas a la Seguridad en Internet, publicado en 2011, muestra que mientras el número de vulnerabilidades disminuyó un 20%, la cantidad de ataques maliciosos se incrementó 81%; y más a grandes organizaciones y a pequeñas empresas mediante violación de datos y usurpación de identidad. [15]

Por otro lado según CSI¹³ en su informe "Computer Crime and Security Survey", menciona que los ataques y la seguridad en internet sigue siendo un problema ya que no solo las pc's y ordenadores son víctimas de amenazas, sino también los dispositivos móviles que tienen acceso a la nube de internet. Las encuestas realizadas por CSI desde el año 2004 hasta el 2010 muestran que se ha incrementado el índice de ataques por malware, phishing y botnets, tal como se puede observar en la siguiente figura: [16]

¹³ CSI: Computer Security Institute

Types of Attacks Experienced By Percent of Respondents

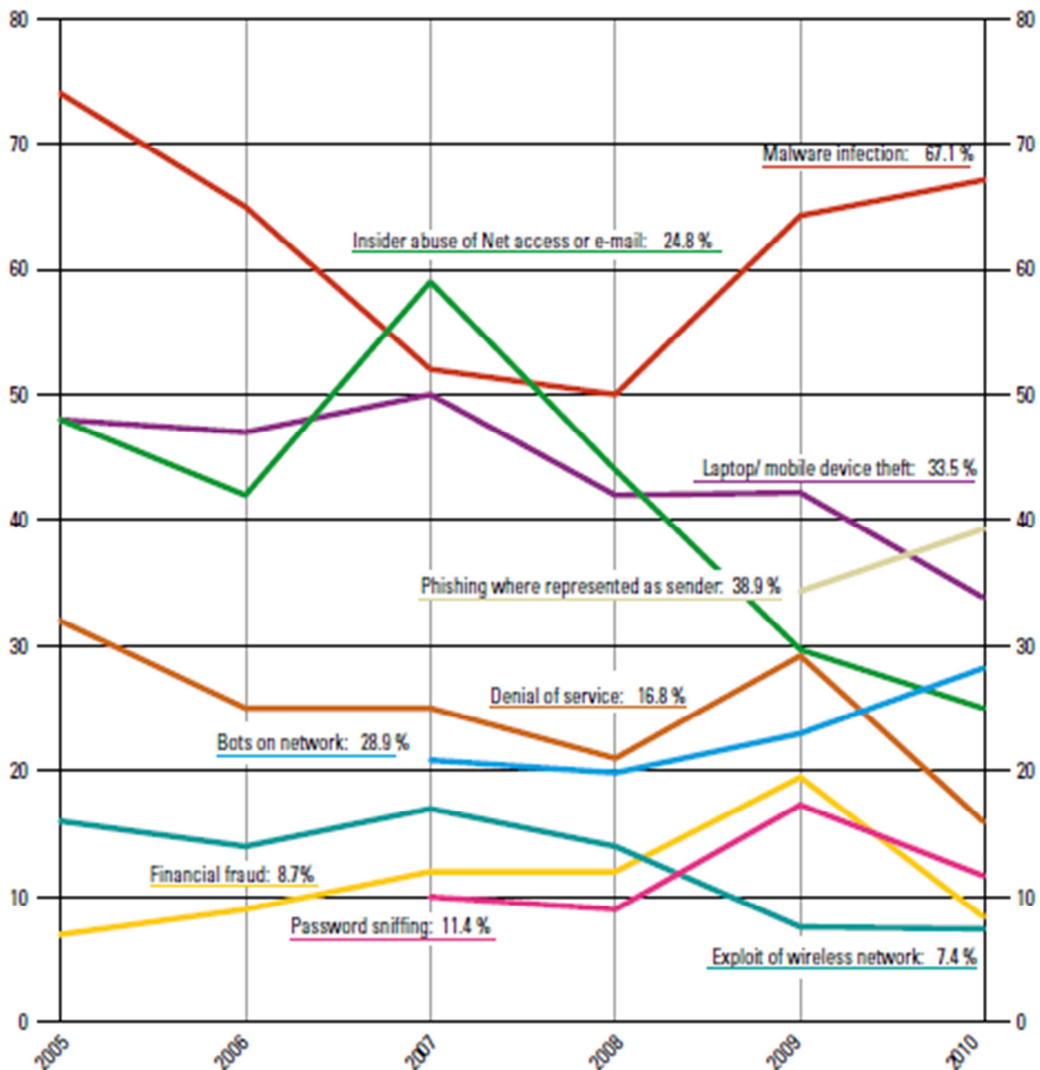


Figura 2. 1 Tipos de ataques [16]

Al ver la figura 2.1, se puede observar que la mayoría de ataques han tenido sus altas y bajas pero que a raíz del 2009 han decrecido considerablemente, tal es el caso de password sniffing¹⁴, fraude financiero, negación de servicio, abuso en el acceso a la red o e-mail, y robo de información a laptops y dispositivos

¹⁴ **Password sniffing:** Técnica para la recolección de contraseñas que implica la supervisión del tráfico en una red para extraer información.

móviles. Mientras que la explotación de redes wireless se ha mantenido en un 7.4% desde el 2009.

Gracias al informe emitido por CSI, se ha determinado que los principales riesgos y amenazas en la red de internet, son los mismos que pueden darse en *Cloud Computing*, por lo tanto las amenazas a las cuales se ve expuesta una nube son:

A. ABUSO Y USO MALINTENCIONADO

Este riesgo afecta principalmente a modelos de servicio IAAS y PAAS y se relaciona con acceso a la infraestructura o plataforma con poca seguridad y restricción, ya que cualquier usuario puede acceder a la nube siempre que pague por su uso. De tal manera que los hackers y piratas informáticos pueden acceder a los recursos de la nube sin ningún inconveniente.

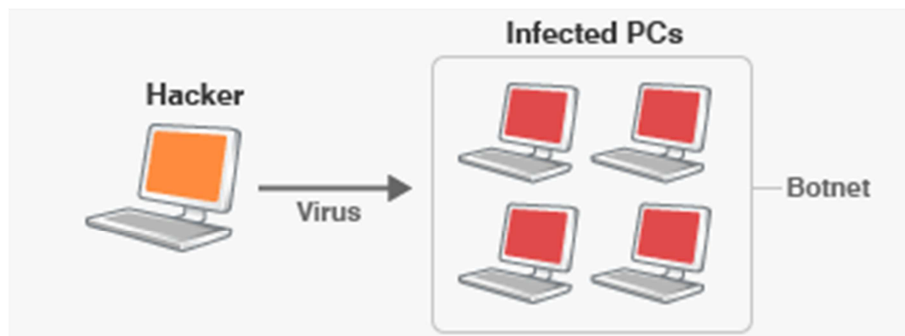
Por lo general, los ataques que realizan los hackers son, el robo de contraseñas, introducción de virus a manera de spam¹⁵, ataques de negación de servicio, creación de códigos maliciosos que inhabilitan los recursos, etc.

La desventaja de estos ataques es que, cuando los delincuentes informáticos contratan el servicio Cloud, pueden iniciar los ataques una vez que se les habilite el servicio, realizando el robo de información o guardando datos maliciosos o robados. Además los recursos que utilicen se borrarán una vez que concluya el ataque, lo que dificulta la identificación y localización de los delincuentes. [4]

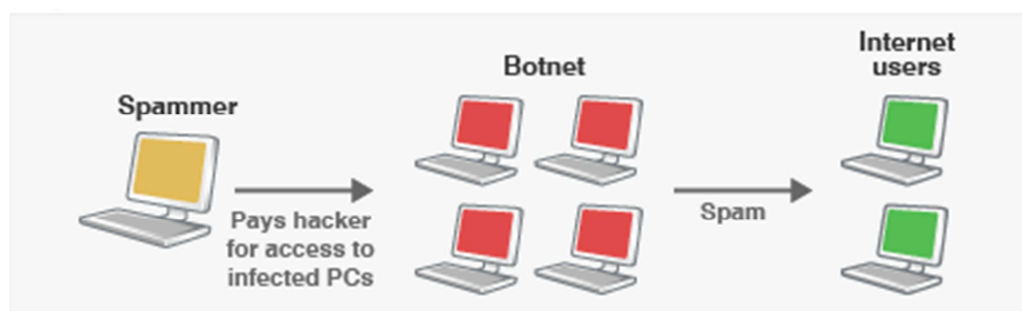
Como ejemplo de este tipo de riesgo en la nube, son conocidos los casos de proveedores IAAS que albergan botnets¹⁶ que han alojado sus centros de control en infraestructuras Cloud.

¹⁵ **Spam:** Correo basura, mensajes no solicitados, no deseados o de remitente no conocido.

¹⁶ **Botnet:** Es un término que hace referencia a un conjunto de robots informáticos que se ejecutan de manera autónoma y automática controlando todos los ordenadores/servidores infectados de forma remota.

CASO 1:**Figura 2. 2 Cómo funciona una botnet. Caso 1. [30]**

En este caso un hacker envía un virus a través de internet que infecta a todas las computadoras y equipos vulnerables que se encuentren conectados a la red, esto a su vez crea una red de máquinas esclavas que son conocidas como botnets, que se ejecutan de manera automática y autónoma, controlando servidores y ordenadores de forma remota.

CASO 2:**Figura 2. 3 Cómo funciona una botnet. Caso 2. [30]**

Para este segundo caso, el hacker vende o alquila la botnet a otros criminales cibernéticos, quienes a su vez la usan para realizar fraude, spamming, ataques DDoS¹⁷ (Denegación de servicios), entre otros crímenes cibernéticos.

Por lo general, los hackers usan las botnets en *Cloud Computing* ya que al tener una nube con servicios u aplicaciones, en donde existen infinidad de máquinas virtuales, es sumamente fácil infectar las máquinas y así expandir el virus, para poder atacar mediante varios métodos a las empresas y organizaciones que albergan su información en la nube.

Según la empresa STRATSEC¹⁸, después de realizar investigaciones y una serie de experimentos sobre la infraestructura de cinco proveedores Cloud cuyos nombres permanecen en el anonimato para precautelar su seguridad; los resultados de realizar pruebas con cibercriminales, determinaron que se podrían crear y utilizar botnets que funcionen en máquinas virtuales de una manera sencilla, ya que llevaría menos tiempo crear una botnet en la nube porque su replicación en las máquinas virtuales sería en un tiempo más corto. Además de que serían más estables y efectivas que en una red normal; ya que se incrementa su disponibilidad y ancho de banda disponible. [11]

Por lo tanto, una botnet en un entorno Cloud puede ser suficiente como para poner en riesgo el contenido de los datos subidos a la nube, ya que además de expandirse a través de toda su infraestructura, esta puede llevar a cabo ataques como:

1. **DDoS:** Denegación de servicio al tener miles de “robots” distribuidos en la nube que pueden lanzar un ataque masivo y coordinado para impedir o reducir los servicios y aplicaciones, saturando el ancho de banda y los recursos del sistema. Como por ejemplo, inundaciones de mensajes

¹⁷ **DDoS:** Conocido como Ataque de denegación de servicios. Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios.

¹⁸ **STRATSEC:** Empresa consultora de seguridad informática en Australia.

ICMP¹⁹, robo de contraseñas del servicio de correo electrónico, ataques al servidor DNS²⁰, etc.

2. **Spyware y Malware:** Robots montados en la nube a manera de espías, que pueden recompilar datos de los usuarios e información confidencial para mal uso de la misma, como por ejemplo venderla o alterar su contenido.
3. **Robo de identidad:** Las botnets son empleadas a menudo para robar información de identidad personal, datos financieros o contraseñas de la computadora de un usuario, para hacer un mal uso de la misma y alterar la información. En una nube este tipo de ataque botnet sería devastador para la empresa u organización que haga uso de los servicios Cloud ya que al tener infinidad de usuarios, el robo de su identidad puede ocasionar el robo de toda la información vital y confidencial de la empresa, y esta información ser usada para negocios ilegales, o a su vez ser vendida a gente inescrupulosa que puede hacer mal uso de la misma.
4. **Adware:** Los “robots” pueden descargar, instalar y exhibir publicidad de ventanas basadas en hábitos de navegación del usuario, es decir, forzar al navegador del usuario a visitar páginas web periódicamente.

En conclusión, existen varias formas de hacer mal uso de la información que se encuentra en la nube, lo importante es que tanto el proveedor de servicios como el cliente tomen las medidas de seguridad necesarias para controlar las diferentes amenazas, como por ejemplo, implementar un sistema de registro de acceso más restrictivo, monitorizar el fraude con tarjetas de crédito en la compra del servicio de la nube, usar sistemas de encriptación de la información e identidad de los usuarios, etc.

¹⁹ **ICMP:** Es el Protocolo de Mensajes de Control de Internet, el cual da control y notificación de errores del Protocolo de Internet (IP). Es decir, se usa para enviar mensajes de error.

²⁰ **DNS:** Sistema de nombres de dominio.

B. PÉRDIDA DE INFORMACIÓN

Este tipo de amenaza se puede dar debido a varias causas entre las cuales están errores humanos o por acciones malogradas por parte del usuario Cloud. Por ejemplo se puede dar pérdida de datos o modificación de los mismos sin tener una copia de seguridad.

Según INTERDOTNET Argentina S.A²¹, un servidor está expuesto a riesgos y amenazas como la caída de conexión a internet falta de redundancia en equipos y conectividad, robo, sabotaje interno, accidentes, hackeo, etc., y lo mismo puede suceder con los servidores que se encuentran virtualmente en la nube, por lo tanto las causas de pérdida de información son similares, por lo que según las estadísticas de un sondeo realizado por la empresa, las principales causas de pérdida de datos son: [13]

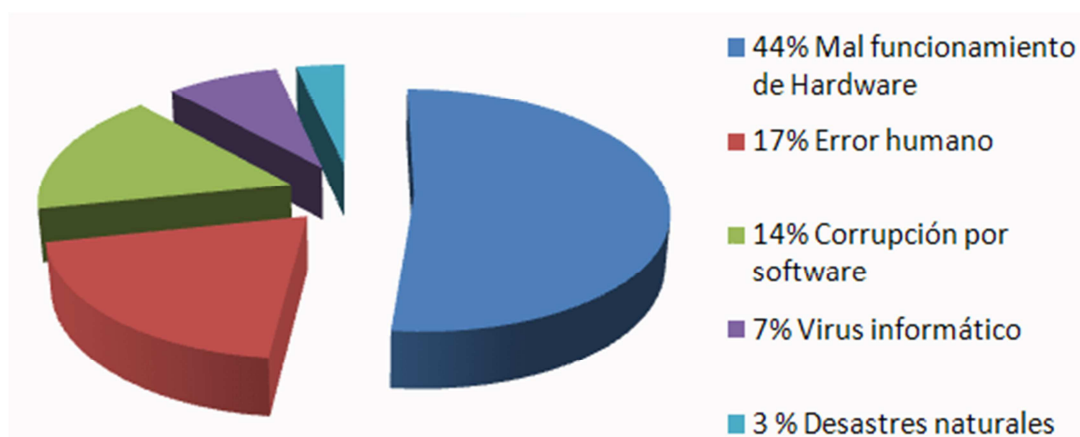


Figura 2. 4 Causas de pérdida de datos [13]

En la nube, aumenta el riesgo de que los datos se vean comprometidos ya que el número de interacciones entre ellos se multiplica debido a la propia arquitectura de la misma. Esto deriva en pérdida de imagen de la compañía,

²¹ INTERDOTNET Argentina S.A: Proveedor Integral de servicios de Internet llave en mano especializado en Pymes.

daños económicos y, si se trata de fugas, problemas legales, infracciones de normas, etc. [7]

Por esta razón, la mayoría de empresas utilizan medidas como la incorporación de cláusulas de confidencialidad en los contratos laborales, o el establecimiento de políticas de seguridad en el uso de los recursos de la nube.

Los problemas más comunes son el mal uso de las claves de los usuarios, autenticación, autorización y cifrado de las claves. Por lo que se podría implementar API's más seguras que hagan un control de acceso a los usuarios de una manera más exhaustiva, protección del tránsito de datos mediante técnicas de cifrado. Además de tener servidores de almacenamiento de información a manera de backups de la información original, y almacenamiento en sistemas seguros con claves encriptadas.

C. API'S INSEGURAS

Las API's²² son una puerta de entrada hacia los servicios de la nube por lo que se convierten en un punto crítico de seguridad y privacidad del sistema. [4]

Los proveedores de servicios Cloud ofrecen interfaces y API's para controlar los recursos de la nube, por lo tanto la monitorización y control se da por medio de una API, en donde esta tiene la potestad de dar permisos para arrancar o parar los servicios de la nube, o aumentar y disminuir los recursos de la misma.

De tal manera que si no existe una correcta política de seguridad las API's pueden sufrir ataques por parte de malware²³ para realizar acciones adicionales malignas que pueden afectar a los sistemas de la nube.

²² **API:** Interfaz de programación de aplicaciones, es el conjunto de funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

²³ **Malware:** También llamado badware, código maligno, o software malintencionado.

Por lo tanto es importante asegurarse que la autenticación y los controles de acceso se implementen teniendo en cuenta el cifrado de datos; que las API's sean desarrolladas incorporando sistemas de autenticación, monitorización de uso y encriptación en la comunicación.

D. SUPLANTACIÓN DE IDENTIDAD



Figura 2. 5 Robo de Identidad [31]

Esta es una de las amenazas más comunes en *Cloud Computing*, ya que no todas las aplicaciones de la nube requieren al usuario introducir su nombre de usuario y la clave de acceso.

Además es común el fraude mediante phishing²⁴ y la explotación de fallas de seguridad para el robo y suplantación de identidad de los usuarios, como también acceder a actividades y aplicaciones a manera de virus, manipulación de datos, intercambio de información falsificada y redirigir a los usuarios a sitios maliciosos.

²⁴ **Phishing:** Es un tipo de delito dentro del ámbito de las estafas cibernéticas, y que intenta adquirir información confidencial de forma fraudulenta, como una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria.

Las investigaciones realizadas por expertos han identificado tres métodos utilizados para realizar el robo de identidad digital:

- **Ataque Phising:** Caracterizador por adquirir información confidencial de forma fraudulenta como contraseñas, tarjetas de crédito, información bancaria, etc. A menudo este tipo de ataque se propaga como spam en la nube y parece ser enviado por otro usuario o un tercero que pertenece a la comunidad Cloud o hace uso de la misma.
- **Malware:** Reúne información confidencial y la alberga en el servidor del cyber delincuente, el mismo que tiene control absoluto sobre esta.
- **Pharming:** En este ataque se aprovechan las vulnerabilidades del servidor DNS y se encuentra el nombre de dominio de un sitio web que permite al atacante redirigir un nombre de dominio a otra máquina distinta.

Por lo que una solución para la suplantación de identidad sería considerar la posibilidad de crear una tarjeta o credencial de identificación personal como una forma de identificación, con medidas criptográficas y biométricas como complemento a las medidas de seguridad. Además de prohibir, mediante políticas compartir credenciales entre los usuarios y monitorizar las sesiones de los clientes en busca de actividades anormales.

2.2 SEGURIDAD POR PARTE DEL PROVEEDOR

El proveedor de servicios y recursos en la nube es el encargado de dar toda la seguridad correspondiente a la parte física y al software de cada aplicación.

En lo que se refiere a la parte física, debe garantizar que los centros de procesos de datos estén protegidos ante cualquier amenaza de robo o daño, además de que deberá mantener los equipos actualizados y con el

correspondiente mantenimiento para evitar cualquier daño y por ende pérdida de información.

Para garantizar el correcto funcionamiento de los servicios en la nube, los proveedores usan mecanismo de virtualización y segmentación de datos para dar una seguridad más completa a los datos y aplicaciones de sus clientes.

La virtualización da la posibilidad de tener varias máquinas virtuales ejecutando diferentes aplicaciones y servicios en un mismo servidor, y cada una ejecutando un sistema operativo diferente de forma aislada.

El espacio de memoria es controlado por un hipervisor²⁵, por lo que el proveedor debe encargarse del control y eliminación del software malintencionado que pretenda burlar la acción del hipervisor para tener acceso a las máquinas virtuales.

Otro punto vulnerable es la localización de los datos de los clientes, por lo que el proveedor debe utilizar mecanismos de protección como servidores de almacenamiento a manera de backups de los originales.

Además, en la parte de Software debe garantizar seguridad a los usuarios que hagan uso de las aplicaciones y programas; por lo tanto, como mecanismos adicionales de seguridad que el proveedor debe garantizar a los clientes, se encuentran los siguientes:

- **Criptografía:** Mediante la técnica de cifrado de datos realizar la protección de las conexiones de red entre los usuarios y las aplicaciones de la nube, permitiendo que todos los datos que viajen en este canal de comunicación se encuentren cifrados, impidiendo su acceso a terceras

²⁵ **Hipervisor:** Es una plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos en una misma computadora.

personas. Mediante el uso de Secure Sockets Layer y Transport Layer Security (SSL, TLS)²⁶.

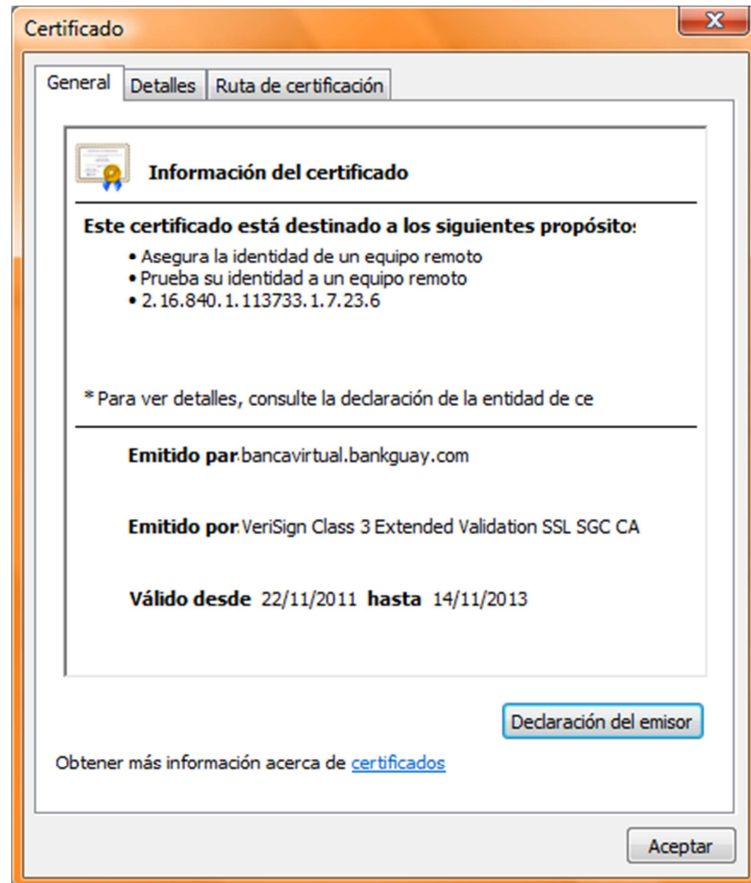


Figura 2. 6 Certificado de conexión segura a la página del banco de Guayaquil [A]

- **Protección entre conexiones:** Seguridad en el canal de comunicación entre las aplicaciones del usuario y los servicios de la nube, mediante el uso de Secure Shell (SSH)²⁷ y Virtual Private Network (VPN)²⁸

²⁶ **SSL, TLS:** Son protocolos criptográficos que proporcionan comunicaciones seguras por una red.

²⁷ **SSH:** Es el nombre de un protocolo que sirve para acceder a máquinas remotas a través de una red.

²⁸ **VPN:** Es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada.

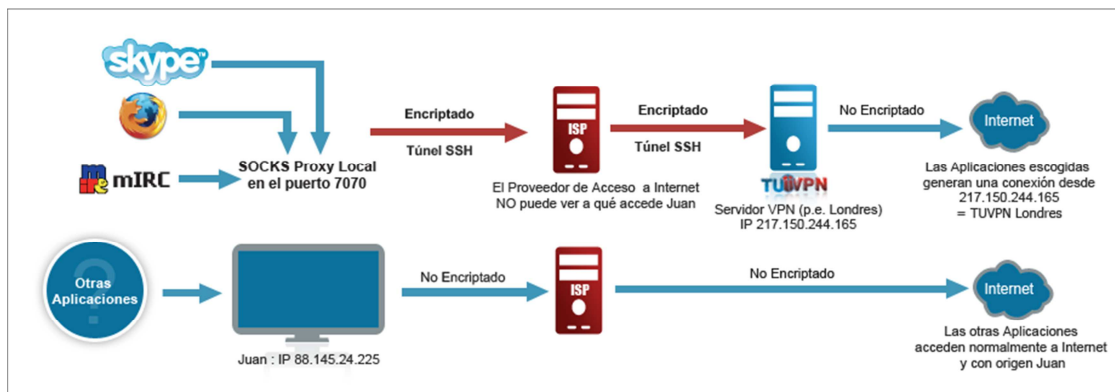


Figura 2. 7 Ejemplo de conexión segura mediante SSH y VPN [19]

Un estudio realizado por CA Technologies y Ponemon Institute²⁹ llamado “Security of Cloud Computing Providers”, muestra que los proveedores de *Cloud Computing* se preocupan más por proporcionar las ventajas de coste y rapidez de implementación antes que sistemas de seguridad para precautelar la información.

“La mayoría de los proveedores de Cloud asignan sólo el 10 por ciento o menos de los recursos de TI a actividades relacionadas con seguridad o control. Esto coincide con otro resultado según el cual menos de la mitad de los encuestados está de acuerdo o muy de acuerdo con que la seguridad es una prioridad.”[14]

Además, el estudio indica que el 69% de los proveedores Cloud creen que la responsabilidad principal de la seguridad la tiene el usuario de Cloud, mientras que sólo el 35% de los usuarios de *Cloud Computing* creen que la seguridad es responsabilidad suya. Sólo el 16% de los proveedores de *Cloud Computing* piensa que la seguridad es una responsabilidad compartida, frente al 33% de los usuarios que creen en ese deber compartido. El 32% de los proveedores y usuarios de *Cloud Computing* coinciden en que la seguridad es responsabilidad del proveedor.

²⁹ CA Technologies y Ponemon Institute: Firma de investigadores independientes especializados en privacidad, protección de datos y políticas de seguridad de la información.

Como conclusión de este estudio realizado, tanto los usuarios como los proveedores de *Cloud Computing* tienen que tener en cuenta que la responsabilidad de la seguridad de la nube debe ser por parte de ambos, ya que es necesario tener un entorno informático seguro para poder trabajar con la garantía de que los datos y aplicaciones en la nube sean seguros y no corran ningún riesgo de plagio o mal uso.

2.3 SEGURIDAD POR PARTE DEL CLIENTE

Como seguridad por parte del cliente, se debe considerar el tipo de nube que contrate según su necesidad:

2.3.1 Nube Privada Comunitaria e Híbrida

En el caso de que una empresa contrate una nube con los servicios que requiera, el cliente se convierte en administrador de la misma y debe encargarse de reforzar la seguridad de la nube ya que, a pesar de la seguridad que brinda el proveedor, existen riesgos que deben ser cubiertos por parte del cliente para evitar infiltraciones y suplantación de identidad

En cuanto al sistema operativo, debe estar siempre actualizado y con los parches necesarios para brindar mayor seguridad; al igual que políticas de seguridad como el control de usuarios, eliminación de cuentas de usuarios que estén inutilizadas y constante control y gestión de las aplicaciones y recursos para monitorear posibles vulnerabilidades que lo puedan afectar.

Entre los mecanismos de seguridad que debería implementar el cliente – Administrador están:

- **Control perimetral:** Mediante la instalación y configuración de un firewall para monitorizar la comunicación de los usuarios de la empresa hacia la nube o viceversa, y decidir si permite o no el paso de información, según las configuraciones realizadas.

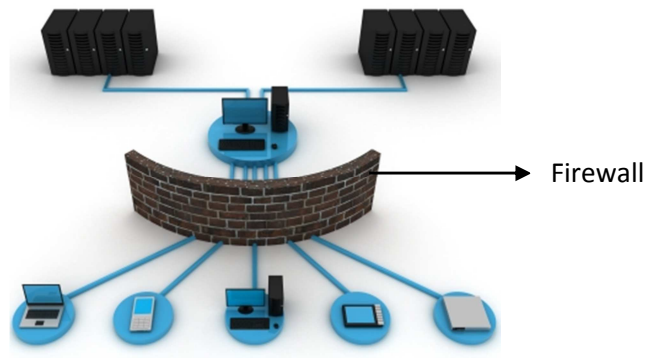


Figura 2. 8 Firewall Perimetral [18]

- **IDS (Intrusion Detection Sistem):** Instalación y configuración de un sistema de detección de intrusos, de manera que bloquee o permita conexiones de los usuarios hacia la nube contratada, de manera que puedan ser analizadas para determinar si alguna conexión es portadora de contenido peligroso para la red.

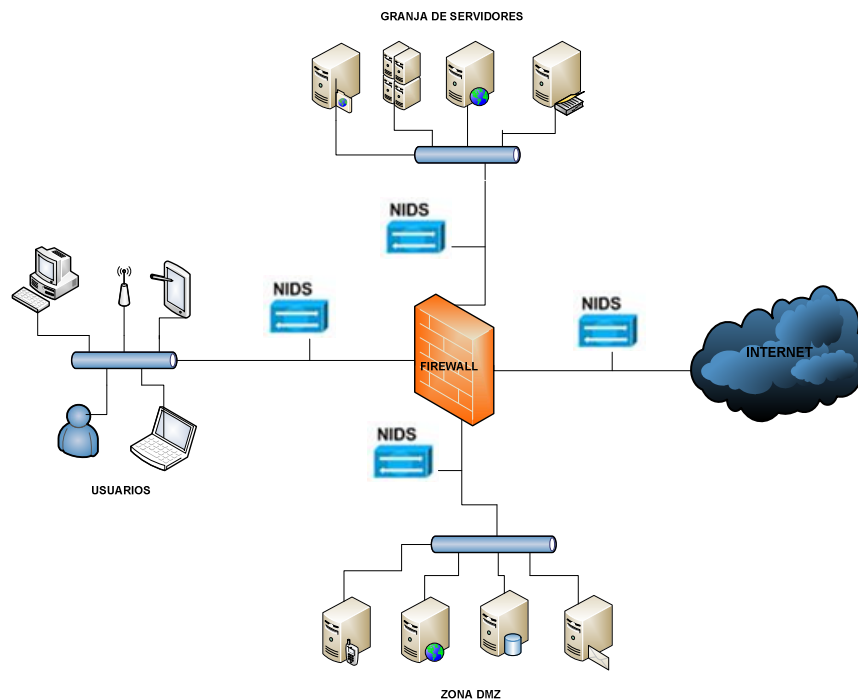


Figura 2. 9 Sistema de protección de una red mediante IDS, firewall. [A]

2.3.2 Nube Pública

Para el caso de que un cliente contrate una nube pública, la seguridad corre enteramente por parte del proveedor, ya que el usuario únicamente hace uso de las aplicaciones o el software contratado.

Por lo tanto, el proveedor es el responsable de ofertar los servicios de su nube con todos los mecanismos, políticas, certificados, etc., para que el usuario simplemente haga uso de lo contratado sin necesidad de preocuparse por la seguridad de su servicio o aplicación.

En definitiva, *Cloud Computing* ha sido y seguirá siendo una tecnología nueva para las empresas y usuarios pequeños que necesitan servicios y aplicaciones de una manera más versátil y escalable; pero antes de que las empresas puedan usar nubes de manera más innovadora, se deben mejorar las

tecnologías de seguridad, los estándares y la interoperabilidad entre los proveedores Cloud y los clientes.

Por lo que la seguridad en la nube sigue siendo un reto tanto para las empresas como para los clientes de *Cloud Computing*. En donde se debe considerar el rendimiento, buen manejo y control de los datos para tener una administración segura de la nube y evitar que sea atacada por riesgos inminentes.

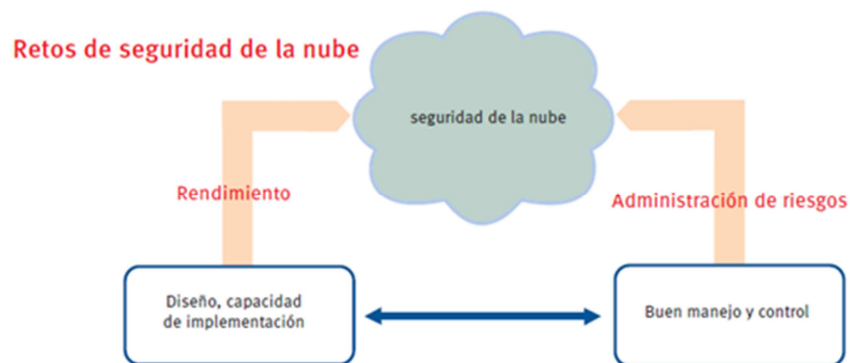


Figura 2. 10 Retos de seguridad en la nube [7]

2.4 PRINCIPIOS PARA LA PROTECCION DE LA NUBE

Debido a que todos los datos terminaran en la nube, es necesario contar con distintos niveles de protección de los mismos, adicionalmente a la protección brindada por el proveedor y la implementada por los clientes. Es decir, tener niveles de seguridad para que se ajusten a la confidencialidad de los diferentes tipos de datos.



Figura 2. 11 Elementos principales para proteger la nube [32]

2.4.1 Seguridad de la Identidad

La seguridad de la identidad preserva la integridad y la confidencialidad de los datos y aplicaciones, además de ofrecer disponibilidad inmediata a los usuarios.

Como solución de seguridad se puede considerar el mecanismo de autenticación sólida de nombres de usuario y contraseñas, con la adopción de técnicas y tecnologías estandarizadas, como ya se mencionaron.

Además de un control exhaustivo por parte de la empresa en la creación y asignación de nuevos usuarios, los cuales a su vez deberían ser llevados en un control cada vez que accedan a la información.

2.4.2 Seguridad de la Infraestructura

La nube debe ser diseñada para ser segura, con componentes seguros, como interfaces sólidas y con sistemas de evaluación de vulnerabilidades y

administración de cambios con niveles de servicio que creen confianza en la empresa o usuario que desee hacer uso de la nube.

Además de la seguridad de sus componentes, debe ser segura en la interfaz de administración como por ejemplo, mediante mecanismos y dispositivos lectores de huellas digitales para acceder a la administración de la nube y de sus componentes. Por lo que las empresas proveedoras deben especificar estas políticas de seguridad para garantizar al usuario que los datos, información y aplicaciones a utilizar estarán seguros y serán administrados únicamente por la empresa proveedora sin correr el riesgo de cyber criminales.

En cuanto a la administración, es importante considerar el ciclo de vida de los recursos de la nube, ya las necesidades y los requerimientos de los clientes se modifican, el proveedor de servicios debe ofrecer nuevos recursos y eliminar los recursos obsoletos, tomando en cuenta que esto brindara niveles de confianza hacia los clientes.

2.4.3 Seguridad de la Información

Para dar seguridad a la información es necesario tener una barrera de protección que garantice la seguridad de la infraestructura a utilizar. Por lo que es necesario:

- Aislamiento de los datos en situaciones de tenencia múltiple ya que al tener varios usuarios que hagan uso de recursos compartidos, estos se ven vulnerables a ataques y robo. Por tanto, la virtualización, la encriptación y el control de acceso son herramientas que permitirán distintos grados de separación entre las organizaciones, pequeños usuarios y usuarios independientes.

- Clasificación de los datos, es decir según su importancia; para lo cual se podrá implementar políticas de seguridad en las cuales dependiendo del grado de confidencialidad los datos podrán ser almacenados dentro de la misma empresa en un servidor exclusivo, o bajo medidas de encriptación de datos.
- Buen manejo y control de cumplimiento de normas de seguridad, con la creación de información de administración y validación realizada a manera de monitoreo y auditoria del estado del manejo de la información. Brindando seguridad al documentar el acceso y denegación de acceso a los datos, y verificando que no se haya cambiado el contenido de la información.

La expansión de las políticas de retención para el cumplimiento de normas y políticas de datos también se convertirá en una capacidad esencial de la nube. Básicamente, las infraestructuras de *Cloud Computing* deben tener la capacidad de verificar que se administren los datos según las reglamentaciones locales e internacionales correspondientes con controles adecuados, recopilación de logs y creación de informes.

En el siguiente cuadro, se resumen los distintos niveles de seguridad que deben correr por parte del proveedor como del cliente en un entorno *Cloud Computing*, ya que dependiendo del modelo de servicio implementado, es necesario implementar políticas y mecanismos de seguridad en la nube para proteger los datos, aplicaciones e información, de amenazas y riesgos que puedan correr al ser manipulados por varios usuarios.

Tabla 2. 1 Mecanismos de Seguridad: Proveedor vs. Cliente

MODELOS DE SERVICIO	MECANISMOS DE SEGURIDAD POR PARTE DE:	
	PROVEEDOR	CLIENTE
INFRAESTRUCTURA COMO SERVICIO (IAAS)	Debe brindar seguridad a los equipos y por ende a la localidad donde se encuentre.	El cliente es responsable de mantener el sistema operativo actualizado e instalar los parches de seguridad que aparezcan.
	Adoptar las medidas técnicas de seguridad necesarias para garantizar la seguridad del datacenter, equipos y programas, y garantizar la disponibilidad de la información.	Mantener políticas de seguridad tradicionales como el control de usuarios, el borrado de cuentas de usuario que ya no se utilizan, o la revisión del software para comprobar que no tiene vulnerabilidades, entre otras.
	Garantizar que la información no se pierda o que sea accedida o tratada por personal no autorizado. Además de tener copias de seguridad.	Instalación y configuración de un firewall, para monitorizar todas las comunicaciones que se realizan desde o hacia el equipo o la red y dar los permisos necesarios.
	Especificar en el contrato de prestación de servicios los riesgos y la responsabilidad que recae en el cliente si hace uso ilícito de la nube.	Autenticación, autorización, administración y configuración de usuarios para brindar los permisos necesarios para que puedan acceder a los beneficios de la nube.
	Deberá mantener sus equipos actualizados tanto a nivel hardware como software para hacer frente a las amenazas existentes en Internet.	Realizar copias de seguridad de los datos para garantizar que no haya ninguna pérdida de información en el caso de producirse un fallo en la red.

PLATAFORMA COMO SERVICIO (PAAS)	El proveedor controla sistemas operativos, hardware, infraestructura de red y gestión de recursos	El cliente crea, despliega y ejecuta, una aplicación, administra los upgrades y parches para todas las funcionalidades de la misma.
	Protección de los datos, además de la administración del acceso a las aplicaciones. La protección de datos incluye la mitigación de riesgo de uso de la PaaS como centros comando y control que dirigen las operaciones de un botnet para uso en la instalación de aplicaciones de malware.	
	Mecanismos de control y eliminación del software malintencionado que pretenda burlar las protecciones del hipervisor para tener acceso a otras máquinas virtuales o incluso al sistema anfitrión.	
SOFTWARE COMO SERVICIO (SAAS)	Administración del acceso a aplicaciones específicas que se ofertan en la nube	El único control que un usuario final tiene es acceder a la aplicación del usuario final desde un desktop, laptop o teléfono móvil.
	El proveedor controla los sistemas operativos, hardware, infraestructura de red, upgrades de aplicaciones y parches.	
	El proveedor define los niveles de umbral de los usuarios.	

CAPÍTULO III

ANÁLISIS DE LA NUBE EN XEN CLOUD PLATFORM

El proyecto implementado en los Laboratorios de Electrónica, está diseñado para brindar infraestructura como servicio (IAAS), es decir capacidad de almacenamiento y procesamiento, además de software como servicio (SAAS), con servicios como *web hosting*, servidor web, correo electrónico, cortafuegos, *DHCP*, *DNS* y almacenamiento en nube.

3.1 INFRAESTRUCTURA COMO SERVICIO

Tal como se especificó en el capítulo 1, IAAS permite a los usuarios Tener un modelo de servicios accesibles, es decir, disponer de procesamiento, almacenamiento, redes y recursos informáticos, así como implementar y ejecutar sistemas operativos y aplicaciones según las necesidades del consumidor.

El tipo de infraestructura Cloud implementada en los laboratorios del DEEE, abarca un modelo de despliegue con una nube privada, que a su vez tiene un modelo de servicio IAAS y SAAS.

Por lo tanto, el modelo de servicio de IAAS implementado, al ser la parte hardware de la infraestructura Cloud, está compuesto por los siguientes elementos:

1. Máquina *front-end*³⁰: Esta máquina tiene instalada la plataforma de *Cloud Computing* denominada *Xen Cloud Platform (XCP)* de virtualización de servidores. Esta plataforma tiene la ventaja de ser gratuita y abierta a cualquier usuario que desee hacer uso de la misma.
2. Nodo: Máquina que permite el almacenamiento en red (NFS), con sistema operativo Linux, distribución FreeNAS que permite dar soporte de almacenamiento accesible desde red, como almacenamiento masivo de información, música, backups, etc.

3.1.1 Características de los elementos Hardware de IAAS

Como características de estos dos elementos que componen la parte hardware de IAAS podemos definir las siguientes:

³⁰ **Front - End:** Es el software con el que se relacionan los usuarios.

Tabla 3. 1 Características de los equipos hardware

CARACTERÍSTICAS HARDWARE Y BIOS					
Equipo	Modelo de la máquina	Detalles del procesador			
MÁQUINA FRONT-END (SERVIDOR)	Servidor HP ProLiant ML350 G6	CPU's Lógicas	RAM	Red	Capacidad de disco
		15 x 64 bit (Intel Xeon) CPU's. 2,4 GHz	12 GB	2 NIC's 100Mbit/s	320 GB SATA
NODO (FREENAS)	Intel Pentium 4	CPU's Lógicas	RAM	Red	Capacidad de disco
		1 x X86 CPU's 2,8 GHz	512 GB	1 NIC's 100Mbit/s	120 GB SATA

3.1.2 Topología IAAS

El diseño del modelo de servicio IAAS (Infraestructura como servicio) se divide en dos topologías; una en la cual se detalla el modelo hardware, y otra en la cual se detalla el modelo virtual IAAS que contiene la nube.

A. TOPOLOGIA EN HARDWARE

En este gráfico se pueden observar los equipos y como se encuentran conectados.

Tal como se muestra en el grafico 3.1, la nube privada está formada por un servidor (máquina Front-end), en el cual se encuentra instalado el software de virtualización Xen Cloud Platform. Este servidor a su vez alberga todas las máquinas virtuales instaladas con los diferentes servidores que ofrece la nube.

Este servidor posee tres interfaces, dos interfaces Ethernet, y una virtual:

- ETH0: Conectada a la red de internet de los laboratorios del DEEE.
- ETH1: Conectada a la LAN para conexión de los usuarios.
- ETH Virtual: Conectada a un switch virtual al cual se conectan las máquinas virtuales.

En la topología se muestra un segundo servidor conectado a la red de internet. Este servidor es el de almacenamiento; cuenta con un software de distribución libre llamado FreeNAS (Nodo), el cual permite almacenar todos los datos de los usuarios fuera de la nube a manera de seguridad para precautelar que los datos no se pierdan en caso de que falle algún servidor dentro de la nube.

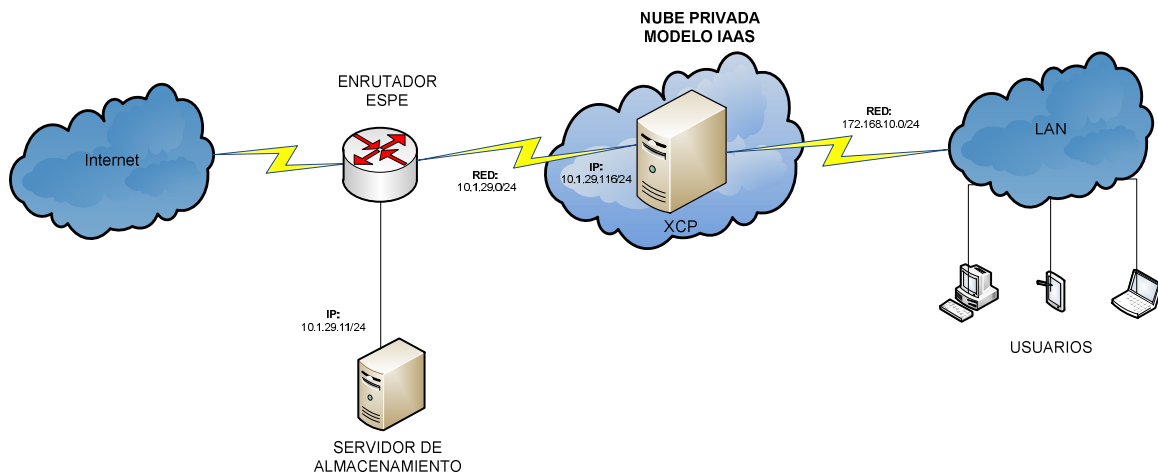


Figura 3. 1 Topología IAAS. Hardware

En la figura 3.1 también se puede observar las direcciones IP de la red; como por ejemplo, las direcciones IP privadas entregadas al servidor XCP y al servidor de almacenamiento FreeNAS, conectados en la red de los laboratorios del DEEE; además de la dirección de red que entrega el servidor XCP a los clientes que se conecten a la nube, mediante DHCP.

B. TOPOLOGIA HARDWARE VIRTUAL

En el gráfico 3.2 se puede observar cómo se encuentra conectado el servidor XCP físicamente como virtualmente; es decir, la conexión de los servidores virtuales instalados en la máquina front-end, y su distribución dentro de la nube.

En la tabla 3.2, se detalla las diferentes direcciones IP y de red de la topología de la nube.

Tabla 3. 2 Direccionamiento IP de la Topología IAAS

DIRECCIONAMIENTO IP DE LA NUBE IAAS			
EQUIPO	DIRECCIÓN IP DE INTERFACES		
	Interfaz Física ETH0	Interfaz Física ETH1	Interfaz Virtual
	RED WAN	RED LAN	RED DMZ
Máquina Front - End (XCP)	10.1.29.116dd	172.168.10.1	NO
Máquina NAS	10.1.29.122	NO	NO
Máquina Virtual 1: Firewall - DHCP	Conexión DHCP a red 10.1.29.0/24	172.168.10.1	10.0.0.1
Máquina Virtual 2	NO	NO	10.0.0.2
Máquina Virtual 3	NO	NO	10.0.0.3

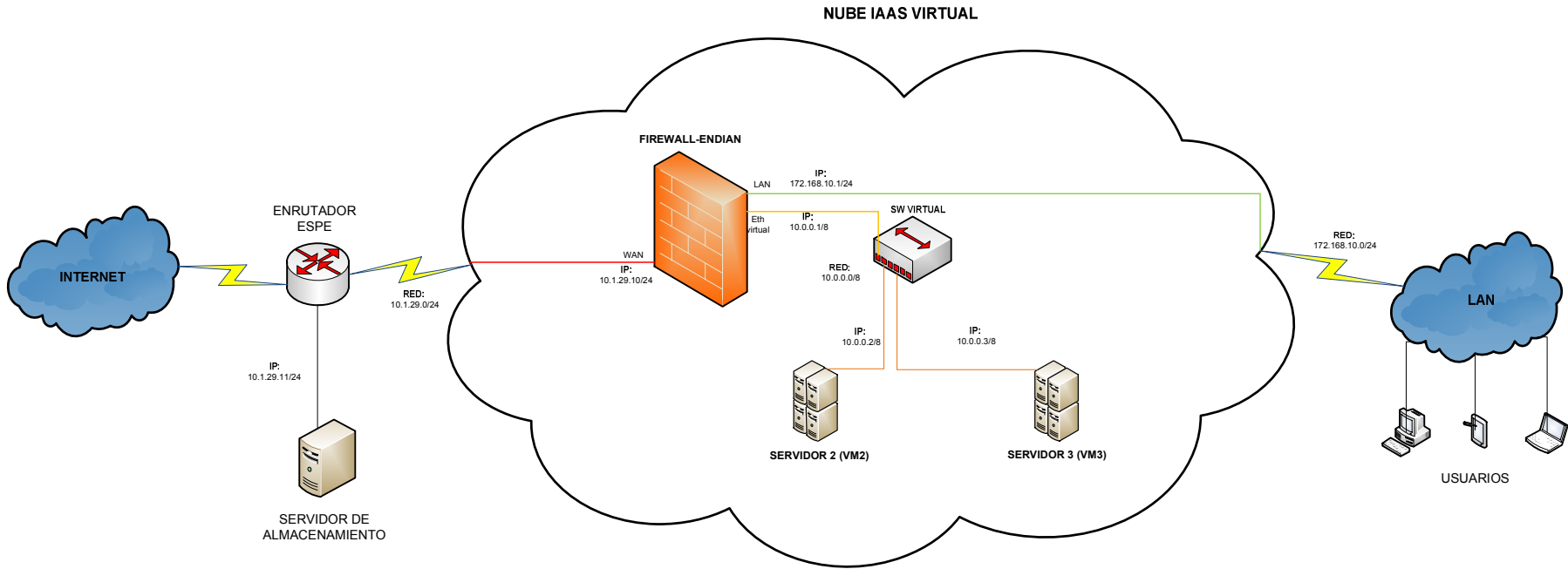


Figura 3. 2 Topología IAAS. Virtualizado

La máquina front - end, está compuesta por tres máquinas virtuales:

- **Máquina Virtual 1 (Firewall – Endian):** Esta máquina virtual tiene como software un firewall de virtualización llamado Endian. Conocido por ser una distribución GNU/Linux libre especializada en Firewall, ruteo y gestión unificada de amenazas.

Endian se encuentra configurado de tal manera que la red se encuentra distribuida en zonas: WAN (roja), LAN (verde), DMZ (naranja - zona de servidores virtuales).

Además de hacer las funciones de firewall, Endian se encuentra configurado para dar servicio de DHCP a todos los usuarios que se conecten a la nube.

- **Máquina Virtual 2 (Servidores):** Esta máquina virtual consta del sistema operativo Ubuntu versión 10.04 LTS, en el cual se han instalado los servidores de correo electrónico, web, DNS.

Estos servicios se los puede administrar mediante webmin³¹, únicamente por medio de un navegador.

Por el contrario, el servidor de correo electrónico se encuentra configurado en un software de correo electrónico y calendario de código abierto llamado Zimbra. Este software ofrece algunas ventajas y servicios adicionales que otros servidores de correo no.

- **Máquina Virtual 3 (Cloud Storage):** Esta máquina virtual consta de un sistema operativo Ubuntu, en el cual se gestiona un servidor de almacenamiento bajo una aplicación llamada OwnCloud.

OwnCloud es una suite de software libre que permite crear un servidor en la nube para obtener un almacenamiento independiente, de manera que

³¹ **Webmin:** Interfaz basada en web para la administración del sistema Unix, como configuración de cuentas de usuario, servidores web, apache, correo, dns, dhcp, etc.

el administrador pueda gestionarlo según las necesidades de los usuarios. Este software no da como ventaja principal eliminar las limitaciones en cuanto a capacidad ya que dispondremos de todo el espacio libre que tengamos en el disco duro, además de administrarlos según las necesidades de almacenamiento.

Además, en la figura 3.2 se puede observar que la distribución del servidor de almacenamiento externo NAS dentro de la topología de la red, no se encuentra en un área segura, debido a que este servidor físico tiene almacenadas un backup de todas las máquinas virtuales que forman parte de la nube. Por esta razón es de suma importancia realizar un rediseño de la topología de la red para brindar seguridad a este servidor ya que debido a su conexión directa con el switch a Internet, se corre el riesgo de que pueda haber algún tipo de ataque o infiltración al mismo y por ende a una parte de la nube.

3.2 SOFTWARE COMO SERVICIO

Al igual que IAAS, SAAS es un modelo de servicio que brinda al usuario la capacidad de tener un despliegue de software como aplicación a través del internet, de modo que el cliente puede usar diferentes tipos de aplicaciones únicamente con mediante una conexión a internet.

El modelo de servicio SAAS implementado en los laboratorios del DEEE, brinda las siguientes aplicaciones:

3.2.1 Servicio de Firewall

Este servicio está implementado mediante un software de distribución libre llamado Endian.

Comunidad Endian Firewall (EFW) es un software abierto en distribución Linux que sirve para convertir a un sistema en un dispositivo de seguridad con todas las funciones de gestión unificada de amenazas (UTM). [17]

Este software se encuentra instalado en la primera máquina virtual de XCP; y permite mejorar la distribución de la red implementada en la nube, de tal manera que se pueden especificar las zonas LAN, WAN y DMZ para definir la distribución de la topología virtual en la nube.

Al ser un software Open Source de servicio de firewall para la red, la ventaja más importante que ofrece al usuario es el nivel de seguridad para la nube que se puede configurar dependiendo de las políticas y reglas necesarias para bloquear el acceso no autorizado, y a su vez permitiendo comunicaciones autorizadas, para dar protección a los recursos y servicios que brinda la nube.

La versión pagada de este software ofrece servicios adicionales en comparación con la versión libre; entre los cuales se encuentran herramientas configurables de, detección de intrusos, escaneo de puertos, antivirus y filtrado de spam para el tráfico de correo electrónico, filtrado del contenido del tráfico web, distribución de carga de datos, manejo proxy, enrutamiento y alta disponibilidad, y solución de VPN's basado en OpenVPN.

Los mensajes que ingresen o salgan de la nube pasan a través del firewall, éste examina cada mensaje, y dependiendo de las reglas configuradas, bloquea aquellos que no cumplan los criterios de seguridad especificados en cada regla.

Análisis:

Al investigar las características que tiene la versión libre de Endian, misma que se encuentra instalada en el servidor, se puede notar que no contiene las características de Alta disponibilidad, detección de intrusos, antivirus, necesarios para cumplir con los parámetros de seguridad necesarios para dar protección a la nube.

La topología del firewall se muestra en la figura 3.3:

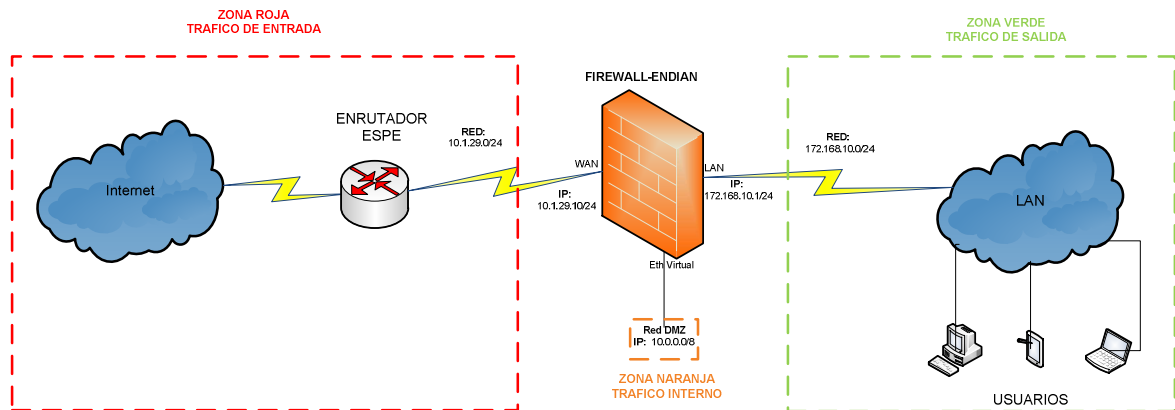


Figura 3. 3 Topología Firewall-Endian

Tal como se ha mencionado, el firewall se encuentra conectado a tres redes, RED WAN (ZONA ROJA), RED LAN (ZONA VERDE), y RED DMZ (ZONA NARANJA). Cada una de estas zonas genera tráfico de datos que necesariamente debe pasar por el firewall; por lo que para proteger la nube, las reglas de filtrado de datos deberían estar configuradas para prevenir riesgos en cada una de las zonas; sin embargo, las reglas que se encuentran configuradas en este servicio son:

- **Tráfico de Entrada (ZONA ROJA):**

En la figura 3.4 se muestra la configuración realizada para la regla de tráfico entrante hacia la red, en donde se permite cualquier tipo de tráfico de datos que venga desde la Zona Roja.

Análisis:

Como se puede observar, aquí se detecta que no existe ninguna seguridad para el tráfico que ingresa a la nube desde el internet; necesariamente deberían estar

configuradas reglas en las cuales se limite dicho tráfico. Por lo tanto, este riesgo detectado debe ser corregido en la configuración del firewall.

Incoming Routed Traffic Firewall Rule Editor

Source
Type * <RED>

Destination
Type * <ANY>

This rule will match the entire RED This rule will match any destination

Service/Port
Service * <ANY> Protocol * <ANY> Destination port (one per line)

Policy *
Action ALLOW Remark Position * First

Enabled Log all accepted packets

[Update rule](#) or [Cancel](#) * This Field is required.

#	Source	Destination	Service	Policy	Remark	Actions
1	<ANY>	RED	<ANY>	→		<input checked="" type="checkbox"/> <input type="checkbox"/>

Legend Enabled (click to disable) Disabled (click to enable) Edit Remove

Show system rules [>>](#)

#	Source	Destination	Service	Policy	Remark
---	--------	-------------	---------	--------	--------

Legend Enabled (click to disable) Disabled (click to enable) Edit Remove

Figura 3. 4 Tráfico de entrada Firewall-Endian

- **Tráfico de Salida (ZONA VERDE):**

En la figura 3.5 se muestra las diferentes reglas configuradas para el tráfico de salida de la red, en donde se permite cualquier tipo de tráfico de datos que venga desde la Zona Roja, es decir la conexión a internet.

Outgoing firewall configuration

>> Current rules

[Add a new firewall rule](#)

#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN ORANGE	RED	TCP/80	→	allow HTTP	↓ ✓ ✎ 🗑
2	GREEN ORANGE	RED	TCP/443	→	allow HTTPS	↑ ↓ ✓ ✎ 🗑
3	GREEN	RED	TCP/21	→	allow FTP	↑ ↓ ✓ ✎ 🗑
4	GREEN	RED	TCP/25	→	allow SMTP	↑ ↓ ✓ ✎ 🗑
5	GREEN	RED	TCP/110	→	allow POP	↑ ↓ ✓ ✎ 🗑
6	GREEN	RED	TCP/143	→	allow IMAP	↑ ↓ ✓ ✎ 🗑
7	GREEN	RED	TCP/995	→	allow POP3s	↑ ↓ ✓ ✎ 🗑
8	GREEN	RED	TCP/993	→	allow IMAPs	↑ ↓ ✓ ✎ 🗑
9	GREEN ORANGE BLUE	RED	TCP+UDP/53	→	allow DNS	↑ ↓ ✓ ✎ 🗑
10	GREEN ORANGE BLUE	RED	ICMP/8 ICMP/30	→	allow PING	↑ ✓ ✎ 🗑

Legend Enabled (click to disable) Disabled (click to enable) ✎ Edit 🗑 Remove

Show system rules >>

#	Source	Destination	Service	Policy	Remark
1	<ANY>	RED	ICMP/8 ICMP/30	→	allow Ping/Traceroute

Legend Enabled (click to disable) Disabled (click to enable) ✎ Edit 🗑 Remove

>> Outgoing Firewall Settings

Enable Outgoing firewall >>

Figura 3. 5 Tráfico de salida Firewall-Endian

La primera y segunda regla, se encuentran configuradas para que todo el tráfico HTTP³² y HTTPS³³ que vaya desde la Zona Verde y Zona Naranja, hacia la Zona Roja, se encuentre permitido mediante el protocolo de transporte TCP con sus respectivos puertos.

Desde la regla 3 hasta la 8, se encuentra permitido todo el tráfico FTP, SMTP, POP, IMAP, POP3s, IMAPs, que vaya desde la Zona Verde hacia la Zona Roja, mediante el protocolo de transporte TCP con sus respectivos puertos.

³² **HTTP:** Protocolo de transferencia de hipertexto. Permite la transferencia de archivos entre navegador y servidor web.

³³ **HTTPS:** Protocolo de transferencia de hipertexto de forma segura. Utiliza un cifrado basado en SSL (**Secure Socket Layers**), creando un canal de transferencia cifrado para aumentar la seguridad en la transferencia de datos.

La regla 9 y 10, se encuentran configuradas de tal manera que desde las Zonas Verde, Naranja y Azul (Red Inalámbrica WIFI), se permite el tráfico DNS mediante los protocolos de transporte TCP y UDP, además del rastreador de paquetes PING³⁴ mediante el protocolo ICMP.

Además de estas reglas, se encuentra habilitada la opción de firewall para el tráfico de salida y los permisos correspondientes para usar las herramientas de PING y TRACEROUTE³⁵ desde cualquier lugar de la red hacia la Zona Roja.

Análisis:

Según esta configuración, se ha determinado que no debe estar permitido todo tipo de tráfico desde la LAN hacia el Internet y viceversa, ya que se puede considerar como vulnerabilidad que no exista una regla de configuración para filtrar el tráfico hacia y desde la red LAN.

- **Tráfico Interno entre zonas:**

Para el tráfico entre zonas se encuentran configuradas reglas tanto para la Zona Verde, Naranja y Azul, en las cuales se admite el tráfico de datos sin restricción alguna.

Análisis:

A esta configuración se la puede ver como un riesgo ya que es necesario crear reglas específicas que permitan el tráfico desde el internet hacia la DMZ, y desde la LAN hacia la DMZ, ya que para el caso de que un usuario requiera software como servicio (SAAS), este no debe tener acceso a la DMZ desde la LAN.

³⁴ **PING:** Rastreador de paquetes. Herramienta que comprueba el estado de la conexión por medio del envío de paquetes ICMP de solicitud y de respuesta.

³⁵ **TRACEROUTE:** Es una herramienta de consola de diagnóstico que permite seguir la pista de los paquetes.

Inter-Zone firewall configuration

>> Current rules

[Add a new inter-zone firewall rule](#)

#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN	GREEN	<ANY>	→		↓ ✓ ✎ 🗑
2	GREEN	BLUE	<ANY>	→		↑ ↓ ✓ ✎ 🗑
3	GREEN	ORANGE	<ANY>	→		↑ ↓ ✓ ✎ 🗑
4	BLUE	BLUE	<ANY>	→		↑ ↓ ✓ ✎ 🗑
5	ORANGE	ORANGE	<ANY>	→		↑ ✓ ✎ 🗑

Legend: Enabled (click to disable) Disabled (click to enable) ✎ Edit 🗑 Remove

Show rules of system services >>

#	Source	Destination	Service	Policy	Remark
---	--------	-------------	---------	--------	--------

Legend: Enabled (click to disable) Disabled (click to enable) ✎ Edit 🗑 Remove

>> Inter-Zone Firewall Settings

Enable Inter-Zone firewall

Log accepted Inter-Zone connections

Figura 3. 6 Trafico de Interno entre zonas. Firewall-Endian

Las características y servicios configurados en el Endian son los siguientes:

- **Network Configuration:**

Tal como se indicó en la figura 3.2, Endian posee 3 interfaces, WAN (interfaz roja), LAN (interfaz verde), y DMZ (Interfaz virtual naranja):

- Interfaz WAN, que se encuentra relacionada directamente con la interfaz física ETH0 del servidor; es decir la conexión y el tráfico hacia el internet, por medio de la IP: 10.1.29.10/24.
- Interfaz LAN, que se encuentra relacionada con la interfaz física Eth1 del servidor; es decir la conexión hacia la LAN para dar servicio a todos los usuarios que quieran conectarse a la nube, por medio de la red 172.168.10.0/24.
- Interfaz Eth Virtual a la que se encuentran conectadas las máquinas virtuales con los servidores, por medio de la red 10.0.0.0/8.

- **Servicio DHCP:**

Este servicio se encuentra configurado en la interfaz LAN, relacionada a la interfaz física ETH1 LAN (zona verde); para proporcionar una dirección IP a los usuarios que se conecten a la nube, proporcionando 98 direcciones disponibles.

Además, está configurado para la zona roja para que el momento en que se conecte a la red WAN, obtenga una dirección IP mediante DHCP.

Para la LAN, la dirección IP de red es 172.168.10.0/24, con direcciones IP disponibles para los usuarios desde la 172.168.10.100/24 a la 172.168.10.200/24. Mientras que para la WAN, la dirección IP de red es la 10.1.29.0/24.

Endian brinda la posibilidad de configurar este servicio de manera sencilla y optima, evitando al proveedor la creación de un servidor DHCP bajo un software independiente, lo que implicaría la creación de una nueva máquina virtual con un software especial para la creación y configuración de este servidor.

Además de estos servicios que se encuentran configurados en Endian, están otros que por default se habilitan para que pueda funcionar correctamente el firewall. Estos servicios son:

- **CRON Server:** Cron es un planificador de tareas de Unix para sistemas operativos. Cron permite a los usuarios programar tareas bajo comandos o scripts³⁶, para ejecutar periódicamente en determinados momentos o fechas. Se utiliza comúnmente para automatizar el mantenimiento o administración del sistema.
- **DNS proxy Server:** Este servicio está configurado de manera automática para la zona WAN (roja); utiliza una base de datos distribuida jerárquicamente que almacena información asociada a nombres de

³⁶ **SCRIPT:** Es un guion, archivo de órdenes o archivo de procesamiento por lotes, es un programa usualmente simple, que por lo regular se almacena en un archivo de texto plano.

dominio a direcciones IP, en redes como Internet, pero el sistema puede dejar las direcciones vulnerables a ataques. Pero al ser un servidor DNS proxy protege las direcciones de espías y ataques a manera de antispyware.

- **Logging Server:** Es un servidor de registro de archivos automáticamente creado y mantenido por el servidor o software en el cual se encuentra corriendo. Es decir, Endian posee como servicio adicional este servidor para llevar un registro de los usuarios que ingresen al sistema.
- **NTP Server:** Network Time Protocol, es un protocolo que permite sincronizar el tiempo de los sistemas informáticos, por medio del enrutamiento de paquetes. Utiliza como medio de transporte el protocolo UDP³⁷.

Endian Firewall mantiene la hora del sistema sincronizado con los hosts de servidor de hora de Internet utilizando el protocolo de tiempo de red (NTP). [17]

- **Web Server:** Este servidor permite el procesamiento de la aplicación Endian en un servidor de internet, para permitir las conexiones con el cliente o clientes de la nube.

3.2.2 Servidor DNS

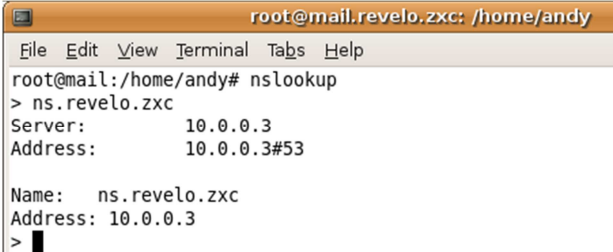
El servidor DNS se encuentra configurado en la tercera máquina virtual bajo el sistema operativo Ubuntu 8.04.

Y, es aquel que se utiliza para proveer a los usuarios o clientes de un nombre equivalente a las direcciones IP, siendo este de uso transparente para los usuarios si se encuentra bien configurado.

³⁷ **UDP:** Es un protocolo del nivel de transporte basado en el intercambio de datagramas.

Ubuntu da la posibilidad de montar un servidor DNS mediante comandos de configuración de archivos, o bajo un software llamado WEBMIN³⁸ que mediante una interfaz web permite al administrador configurar cuentas de usuario, Servidor Apache, Servidor DNS, compartir archivos, etc.

El Servidor DNS para la nube se encuentra configurado en WEBMIN, el dominio es **ns.revelo.zxc** asociado a la **IP: 10.0.0.3/8** que corresponde a la máquina virtual 3, tal como se indica en la figura 3.7.



```

root@mail.revelo.zxc: /home/andy
File Edit View Terminal Tabs Help
root@mail:/home/andy# nslookup
> ns.revelo.zxc
Server:      10.0.0.3
Address:     10.0.0.3#53

Name:   ns.revelo.zxc
Address: 10.0.0.3
>

```

Figura 3. 7 Prueba del Servidor DNS

Además, se encuentran configurados otros registros para el servidor de correo electrónico, OwnCloud, y el servidor de almacenamiento, tal como se ve en la figura 3.8.

Name	TTL	Address	Name	TTL	Address
<input type="checkbox"/> ns.revelo.zxc.	Default	10.0.0.3	<input type="checkbox"/> storage.revelo.zxc.	Default	10.0.0.2
<input type="checkbox"/> box.revelo.zxc.	Default	10.0.0.3	<input type="checkbox"/> cloud.revelo.zxc.	Default	172.168.10.1
<input type="checkbox"/> mail.revelo.zxc.	Default	10.0.0.3			

Figura 3. 8 Registros Configurados en el servidor DNS

³⁸ **WEBMIN:** Interfaz basada en web para la administración del sistema de Unix, en el cual se puede configurar cuentas de usuario, Apache, DNS, compartir archivos y mucho más desde la consola o remotamente.

3.2.3 Servidor de Correo Electrónico

El Servidor de correo se encuentra implementado en un software libre llamado Zimbra.

Zimbra es una solución empresarial constituida en la nube, que ofrece servicio de mensajería instantánea, correo electrónico y calendario.

Al igual que el servidor DNS, Zimbra se encuentra instalado en la misma máquina virtual 3, con un registro MX en el servidor DNS como **mail.revelo.zxc**.

La ventaja de Zimbra es que trabaja bajo una consola de administración sencilla, misma que nos permite usar el servicio de manera óptima y rápida. En la figura 3.9 se muestra la consola de Administración usada y los diferentes correos electrónicos enviados a manera de prueba.

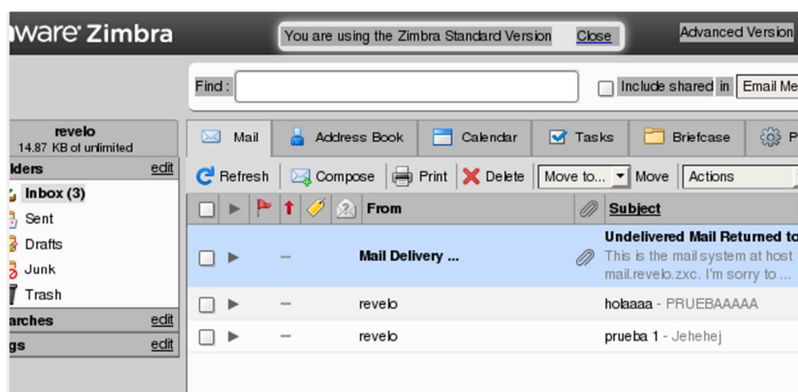


Figura 3. 9 Servidor de Correo Zimbra

Para que el usuario pueda ingresar a este servicio montado en la nube, debe acceder hacia cualquier navegador web, y en el browser digitar la dirección **mail.revelo.zxc**.

3.2.4 Servidor Almacenamiento (OWNCLOUD) y Servidor Web

El servidor Apache se encuentra instalado en la segunda máquina virtual bajo el sistema operativo Ubuntu 10.04. De igual manera esta máquina se encuentra atada al dominio revelo.zxc con la dirección IP **10.0.0.2/8**

El servidor Web instalado y configurado es un servidor Apache, el mismo que procesa una aplicación del lado del servidor realizando conexiones bidireccionales o unidireccionales con el cliente. Este servidor es una aplicación libre que corre tanto en Linux como Windows.

El servidor de almacenamiento corre bajo una aplicación llamada OWNCLOUD de distribución libre. Esta aplicación brinda al usuario la posibilidad de acceder a sus archivos desde cualquier parte del mundo por medio de un navegador web. Además de ofrecer servicios como sincronización de contactos, calendario y notas.

3.2.5 Servidor FREENAS

Este servidor se encuentra implementado fuera de la nube, a manera de un nodo externo, tal como se observa en la figura 3.2. Configurado la dirección IP **10.1.29.11/24**

FreeNAS es una plataforma de almacenamiento de código abierto basado en FreeBSD³⁹ que soporta el uso compartido de información, archivos, ficheros, etc., a través de Windows, Apple y sistemas de tipo UNIX. Además consta con una interfaz gráfica sencilla para la administración del sistema, permitiendo la gestión de las diferentes capacidades de almacenamiento, integración de sistemas de archivos, y gestión de volúmenes.

³⁹ **FreeBSD:** Es un avanzado sistema operativo para arquitecturas x86 compatibles con diferentes tipos de procesadores como Pentium, amd, etc.

Este servidor tiene configurado un disco de almacenamiento en el cual se encuentran almacenadas copias de seguridad de las máquinas virtuales.

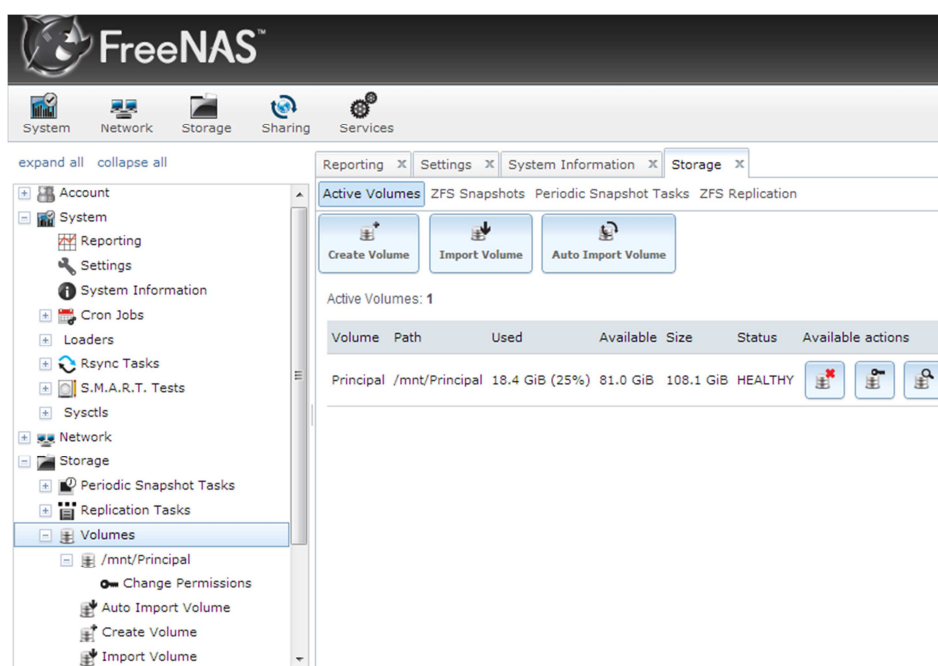


Figura 3. 10 Servidor FreeNAS

Como servicios se encuentran habilitados CIFS⁴⁰ y NFS⁴¹ para permitir la compartición de archivos tanto en Linux como en Windows.

3.3 ANÁLISIS DE LA SEGURIDAD DE LA NUBE

En base al análisis realizado de cada una de las partes que conforman la nube, tanto hardware como software, es importante y necesario una protección

⁴⁰ **CIFS**: Common Internet File System, es un protocolo de red que permite compartir archivos e impresoras entre nodos de una red, además incluye soportes para enlaces simbólicos, enlaces duros y archivos de mayor tamaño.

⁴¹ **NFS**: Network File System, es un protocolo de nivel de aplicación utilizado para sistemas de archivos distribuidos en un entorno de red local.

adicional en todo el sistema, para dar mayor seguridad tanto al administrador de la nube como a los usuarios que harán uso de la misma.

En el Capítulo 2, se mencionó los riesgos y vulnerabilidades que puede presentar un entorno *Cloud Computing* que no se encuentre con la seguridad suficiente tanto en hardware como en software, ya que el sistema se expone y es tiende a ser más vulnerable a ataques; por esta razón, es necesario considerar todos y cada uno de los aspectos que conforman la nube para precautelar los datos y la información de la misma y que a su vez el usuario tenga plena confianza al momento de usar los servicios y aplicaciones que la conforman.

Al ser una nube privada que se encuentra implementada en el Edificio de los Laboratorios del DEEE, todos los servicios y aplicaciones pueden ser usados por los alumnos y docentes del Departamento; la importancia de esto, es que debe brindar toda la seguridad a los usuarios por lo que debe haber una sola persona que administre la nube, o a su vez un equipo de trabajo que pueda administrar o gestionar la nube implementada según los requerimientos de los usuarios del Departamento.

En base al análisis realizado de la nube implementada, se han determinado las vulnerabilidades de la misma, y se propondrán soluciones como proveedores de un servicio completo de Cloud Computing, de tal manera que se proporcione políticas y mecanismos de seguridad para los diferentes modelos de servicio que puede ofertar el entorno Cloud.

3.3.1 Vulnerabilidades en IAAS

Tal como se habló en 3.1, IAAS se encuentra conformado por dos partes, infraestructura física (hardware), e infraestructura virtual; y cada una de estas partes se encuentra expuesta a riesgos y amenazas que pueden provocar la

pérdida del sistema e información, y daños materiales como averías en el servidor físico, etc.

Por lo tanto, es importante destacar que todo sistema informático requiere de mecanismos y políticas de seguridad para precautelar la integridad de los datos, administradores y usuarios del sistema; de manera que se encuentre libre de todo peligro, daño o riesgo a fin de mantener el sistema bajo tres aspectos fundamentales de funcionamiento: confidencialidad, integridad y disponibilidad.

La nube implementada en los Laboratorios del DEEE debe cumplir con estos requisitos para que sea un sistema seguro y óptimo que garantice de manera confiable y segura el uso de sus recursos a todos los usuarios de la nube. Por esta razón, es necesario determinar las vulnerabilidades de todos y cada uno de los aspectos que conforman la nube y dar soluciones de mecanismos de seguridad para la misma.

Las vulnerabilidades que se detectaron, tanto físicas como lógicas en IAAS son:

Tabla 3. 3 Vulnerabilidades en IAAS

MODELO DE SERVICIO	VULNERABILIDADES DETECTADAS	
	INFRAESTRUCTURA FISICA	INFRAESTRUCTURA LOGICA
IAAS	Condiciones de la localidad inadecuadas, falta de seguridad en la ubicación de los equipos	Implementar un sistemas de alta disponibilidad para el servidor físico; tanto en hardware como en software
	El lugar donde se encuentra el servidor no consta con un sistema de autenticación de usuarios permitidos para el acceso.	Realizar una redistribución de la topología física de la nube para garantizar la seguridad, tanto en el servidor XCP como en el servidor de almacenamiento externo.
	Localidad de los equipos sin condiciones adecuadas para la prevención de un desastre natural	Cuando un usuario requiera el uso de un servicio de la nube, se debe especificar las políticas de prestación de dicho servicio, para evitar problemas entre proveedor y cliente
	Se requiere de una redistribución de los medios físicos empleados para mejorar la distribución de la información	Cumplir con un plan de mantenimiento (actualizaciones) de los servidores, a nivel de hardware como de software.
	Dotar de toda la seguridad física para evitar el ingreso de personal no autorizado que pueda plagiar los equipos	Administrar usuarios autorizados para la gestión de la nube.
	Protección de los equipos ante fallas eléctricas	

3.3.2 Vulnerabilidades en PAAS

En el capítulo 1, la figura 1.6 muestra los diferentes niveles de servicios que ofrece una nube de Cloud Computing, por lo tanto, la nube implementada en los

Laboratorios del DEEE, al brindar los servicios de IAAS y SAAS; también puede ofrecer el servicio de plataforma PAAS si el usuario lo requiera.

Al analizar las condiciones de la nube, y en base a los mecanismos de seguridad que debe dotar el proveedor se determinaron las posibles vulnerabilidades que pudieran afectar a PAAS en el caso de implementar este servicio.

Tabla 3. 4 Vulnerabilidades en PAAS

MODELO DE SERVICIO	VULNERABILIDADES DETECTADAS
PAAS	No existe ningún método o control independiente de los sistemas operativos o máquinas virtuales, en el caso de que un usuario requiera tener acceso a una de ellas, mas no a la plataforma.
	No se encuentra implementado ningún sistema de administración de acceso a los usuarios según requerimientos específicos para acceder a las plataformas requeridas
	Faltan medidas de seguridad para garantizar un acceso seguro a los clientes hacia la plataforma requerida
	No existe ninguna protección de la plataforma mediante mecanismos como firewall, IDS y antivirus

3.3.3 Vulnerabilidades en SAAS

Tal como se mencionó en el apartado 3.2, la nube en Xen Cloud Platform oferta Software como Servicio, por lo tanto es importante analizar las vulnerabilidades a las cuales se encuentran expuestos los diferentes servicios y aplicaciones que conforman la nube.

Los servicios a los cuales pueden acceder los usuarios de la nube, básicamente son, el servidor de correo Zimbra, y la plataforma de almacenamiento OwnCloud.

Debido a que los usuarios harán uso de la nube para tener acceso a estos dos servicios, es necesario implementar políticas de seguridad adicionales en cada uno, como por ejemplo, autenticación de usuarios, protección de los datos (correo electrónico, información, fotos, etc.), administración de los recursos, etc. Por lo que se propone como solución de seguridad lo siguiente:

Además de estos servicios ofrecidos a los usuarios, la nube tiene configurado un servidor de firewall llamado Endian, mismo que es transparente para los usuarios. Este firewall proporciona un servidor de DHCP para la red LAN, además de cumplir con las funciones de firewall según las reglas que tiene configuradas.

Al analizar las características y funcionalidades que tiene Endian, se encontró con que la versión Open Source instalada no brinda todas las herramientas que poseen las diferentes versiones pagadas del mismo; como por ejemplo, la versión Endian UTM 2.5, que tiene funciones como IPS, antivirus, alta disponibilidad, calidad de servicio, entre otras.

Por esta razón es que se considera como vulnerable a esta máquina virtual y como solución se propone la instalación y configuración de otro servidor de firewall que proporcione características de configuración como alta disponibilidad, distribución de antivirus, detector de vulnerabilidades y configuración de calidad de servicio.

CAPÍTULO IV

DISEÑO DE LA SOLUCIÓN

La norma ISO/IEC 27001, en el Anexo B (Informativo); tabla B.1 – Principios OECD⁴² y Modelo PDCA⁴³; indica que para cumplir el diseño e implementación de la seguridad, se debe considerar a la seguridad de los sistemas y redes de información como un elemento esencial para el cumplimiento de buenas prácticas de seguridad en donde una vez se haya cumplido el proceso de evaluación y análisis del sistema, se seleccionan los controles para el tratamiento de riesgos y vulnerabilidades por las cuales atraviesa el sistema y se cumplen las fases de “**Planear**” métodos de seguridad para atacar estos riesgos, y posteriormente, la fase de “**Hacer**”, es decir la implementación y uso operacional de todos los recursos necesarios para **dotar** de seguridad a la nube. (Anexo A: Norma ISO/IEC 27001)

4.1 DISEÑO DE LAS SOLUCIONES DE SEGURIDAD EN IAAS

Tal como se plantea en el Capítulo 3 apartado 3.3.1, las soluciones a implementar para dar seguridad a IAAS, comprenden tanto la parte física como la lógica:

⁴² **OECD**: Organisation for Economic Co-operation and Development

⁴³ **PDCA**: Planificar, Hacer, Verificar, Actuar. Estrategia de mejora continua de la calidad en cuatro pasos.

4.1.1 Seguridad Física

“La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial”⁴⁴ [20].

Para implementar mecanismos y técnicas de seguridad física a un datacenter⁴⁵ se deben considerar los tipos de amenazas a las cuales puede ser vulnerable el Centro de Datos. Estas amenazas dan la pauta para proponer diferentes soluciones de seguridad dependiendo de la ubicación de los equipos y el cuarto donde estos se encuentran:

1. Desastres naturales, incendios accidentales, fenómenos naturales como tormentas, inundaciones, etc.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos o externos, robo, fraude, etc.

En base a estas amenazas se deben considerar los aspectos e inmediaciones vulnerables a las mismas:

1. Edificios, instalaciones, locales.
4. Autenticación y control de acceso físico.
5. Medios empleados para la transmisión de la información.
6. Conductos y gabinetes de comunicaciones.
7. Medios físicos empleados para el almacenamiento y procesamiento de la información.
8. Documentación, listados, plantillas, planos, etc.

En el mes de octubre del año 2005, la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) publicaron

⁴⁴ HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital. Página 21. 2 de Octubre de 2000.

⁴⁵ **DATA CENTER:** Centro de procesamiento de datos (CPD) es aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

la norma ISO/IEC 270001 que es un estándar para la seguridad de la información; en la cual se especifica los requisitos necesarios para establecer, implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la información (SGSI).

En esta norma se destacan los mecanismos, objetivos y controles que son necesarios para proteger los equipos y la información de un Centro de Datos o datacenter.

En el Anexo A (Normativo) de la norma ISO/IEC 27001, se describen los objetivos de control y controles que una empresa debe implementar como mecanismo de seguridad de la información.

En la tabla A.1 – Objetivos de control y controles, apartado A.9 Seguridad física y ambiental se describen parámetros para evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.

En base a este anexo de la norma, se proponen soluciones de seguridad para tener áreas seguras en un datacenter, en este caso en los Laboratorios del DEEE donde se encuentran los servidores de la nube:

A.9.1.1 Perímetro de seguridad física: Se debe utilizar perímetros de seguridad como mecanismos de control, barreras físicas, alarmas, barras metálicas, puertas de seguridad de ingreso controlado, etc.

A.9.1.2 Controles de entrada físicos: Se debe proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita el acceso al personal autorizado.

A.9.1.3 Seguridad de oficinas, habitaciones y medios: Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.

SOLUCIÓN:

El datacenter de los Laboratorios DEEE debe estar ubicado en un cuarto con todos los acondicionamientos necesarios para el correcto funcionamiento de los equipos y gestión de los mismos. Para el ingreso a esta área se debe colocar un lector biométrico de huellas dactilares que permita que la puerta de ingreso se abra cuando reconozca una huella dactilar registrada en el sistema; y a su vez se desactive una alarma con sensores en la puerta que detecte el ingreso del personal. Cabe recalcar que el lector biométrico debe estar configurado únicamente con las huellas del personal autorizado como por ejemplo los administradores de la red.

Para dar mayor seguridad para el acceso al datacenter, se sugiere la colocación de cámaras de video como sistema de vigilancia que transmita la información vía TCP/IP usando cualquier tipo de compresión, como MPEG4; y que permita visualizar varias cámaras en tiempo real y simultáneamente, con grabación en PC remota y entrada de audio incorporado, además de detección de movimiento inteligente.

A.9.1.4 Protección contra amenazas externas y ambientales: Se debe diseñar y aplicar protección física, contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.

SOLUCIÓN:

Para reducir los riesgos de amenazas ante estos factores se debe considerar lo siguiente:

- Incendios: Las paredes del datacenter deben ser de un material aislante que no sea inflamable ni con combustible, y deben extenderse desde el suelo hacia el techo. Además, el cuarto debe tener un piso falso instalado sobre el piso real con materiales incombustibles y resistentes al fuego. Además de alarmas contra incendios y detectores de humo que emitan informes indicando las condiciones de temperatura del cuarto de equipos.

El datacenter debe estar provisionado de extintores de incendios tanto manuales como automáticos; debidamente probados y con capacidad de detener el fuego generado por un recalentamiento de equipo eléctrico, papel o químicos especiales.

- Inundaciones: El techo del cuarto de equipos debe ser impermeabilizado para evitar el paso de agua desde un nivel superior y se debe acondicionar las puertas para contener el paso de agua en el caso de que el nivel de agua sobrepase el del suelo. Además, las cañerías de desagüe del cuarto de equipos deben estar ubicadas en el piso, con válvulas de retención de líquidos en flujo inverso a fin de que no sirvan como bocas de inundación ante sobre-flujos o Interferencia Eléctrica y/o Radiación electromagnética.

- Ambiente Climático: Este punto es sumamente importante y se deben considerar las condiciones ideales para el buen funcionamiento de los equipos en el datacenter. La temperatura debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe ser entre el 45% y el 65%. Por lo que es necesario la colocación de sistemas de aire acondicionado que renueven el aire periódicamente y mantengan el nivel de temperatura requerido.

A.9.2: Seguridad del Equipo:

En este apartado se pretende evitar la pérdida, daño, robo de los equipos que se encuentran en el datacenter.

A.9.2.1 Ubicación y protección del equipo: El equipo debe estar ubicado o protegido para reducir los riesgos y amenazas por el acceso no autorizado.

A.9.2.2 Servicios Públicos: El equipo debe estar protegido ante fallas energéticas y fallas de los servicios públicos.

A.9.2.3 Seguridad en el cableado: El cableado de la energía y de las telecomunicaciones que permiten el intercambio de información y datos deben ser protegidos de la interceptación o daños.

A.9.2.4 Mantenimiento del equipo: El equipo debe estar en mantenimiento continuo para no perder la disponibilidad del mismo y la integridad de los datos y la comunicación.

SOLUCIÓN:

En cuanto a ubicación y protección del equipo, en el apartado A.9.1 se han mencionado las condiciones y equipamiento de seguridad necesario que deben tener las instalaciones en donde se encontrarán los equipos, además del debido control de acceso para el personal autorizado.

Los equipos deben ser protegidos de fallas de suministro eléctrico y otro tipo de anomalías; por lo que los sistemas de abastecimiento de potencia deben cumplir con las especificaciones de los fabricantes de los equipos, como:

- Uso de UPS⁴⁶: Estos equipos se deben probar según las recomendaciones del fabricante, de tal forma que garanticen el suficiente tiempo para realizar las funciones de respaldo en servidores y aplicaciones.
- Generador de energía: En caso de exista corte de energía eléctrica, debe encenderse un generador de energía para que los equipos permanezcan encendidos y no exista pérdida de comunicación y por ende de la información transmitida.
- Interruptores eléctricos adicionales: Deben estar localizados cerca de las salidas de emergencia, para lograr un rápido apagado de los sistemas en

⁴⁶ **UPS:** Sistema de alimentación ininterrumpida. Es un dispositivo que tiene baterías y otros elementos almacenadores de energía, que proporcionan energía eléctrica por un tiempo limitado y durante un apagón a todos los dispositivos que tenga conectados.

caso de una falla o contingencia. Las luces de emergencia deben funcionar en caso de fallas en la potencia eléctrica.

En cuanto a seguridad en el cableado, la red debe estar protegida de interferencias electromagnéticas o del ruido, por lo que se puede usar canaletas que lo protejan los cables de cualquier daño físico. Además, los cables de potencia deben estar separados de los cables de comunicaciones, siguiendo las normas técnicas, y con su respectivo polo a tierra.

Finalmente, se deberán realizar mantenimientos sobre los equipos de acuerdo a las recomendaciones del fabricante y esto se lo debe hacer únicamente por personal autorizado, para precautelar la información y configuración de la red.

4.1.2 Seguridad Lógica (Infraestructura Virtual)

“La seguridad Lógica es toda aquella relacionada con la protección del software y de los sistemas operativos, que en definitiva es la protección de los datos y la información”⁴⁷ [21]

Por otro lado, IAAS proporciona un conjunto de API's que permiten la gestión y otras formas de interacción de la infraestructura por parte del consumidor del servicio; por esta razón, es de suma importancia implementar políticas de seguridad lógica, en el software de administración de la nube IAAS. Además, se deben tomar en cuenta todos y cada uno de los puntos vulnerables a amenazas que conforman la infraestructura de la nube.

La nube se encuentra estructurada de tal manera que se considera como seguridad lógica a la parte de administración y acceso a las aplicaciones y recursos de la nube, tanto por parte del cliente como por parte del administrador.

⁴⁷ Aguilera López, Purificación. "Seguridad Informática". Capítulo 2. Página 30. Edición 2010.

Según el artículo “**Cree una política de seguridad para servicios en la nube**” [22], en los tres modelos de servicio que ofrece *Cloud Computing*, es necesario crear políticas de seguridad para cada uno, esto incluye en la administración de usuarios, protección de datos y seguridad para las máquinas virtuales.

En IAAS, la política de seguridad lógica se basa en la administración de las máquinas virtuales, protección de los datos y la correcta administración del acceso a los usuarios a la infraestructura de los recursos de la nube.

La infraestructura montada en el hipervisor Open Source Xen cloud Platform, debe tener mecanismos de seguridad tanto físicos como lógicos; por lo que es necesario implementar medidas de protección que garanticen la seguridad de la infraestructura tanto para el proveedor como para los clientes que hagan uso de la nube.

Como soluciones de seguridad lógica para IAAS, se propone:

SOLUCIÓN A:

Diseño e Implementación de un sistema de alta disponibilidad de servidores para garantizar la conexión de los usuarios hacia los servicios de la nube.

SOLUCIÓN B:

Diseño e implementación de firewalls de alta disponibilidad para dar mayor protección a la infraestructura de la nube.

SOLUCIÓN C:

Rediseño de la distribución de los recursos de la nube, para proteger el servidor de almacenamiento NAS.

SOLUCIÓN A: ALTA DISPONIBILIDAD DE SERVIDORES FÍSICOS

El servicio de Alta disponibilidad permite a la plataforma de virtualización controlar el arranque de los servidores virtuales ante la falla del servidor master que alberga al hipervisor.

El hipervisor Xen Cloud Platform se encuentra instalado en un servidor con las características mencionadas en 3.1.1; tal como establece la norma ISO/IEC 270001, Anexo A, punto A.9.2.4; el equipo debe llevar un mantenimiento adecuado para garantizar siempre su disponibilidad e integridad.

Al analizar los riesgos que presenta IAAS en la parte física, se decidió proponer e implementar como solución ante posibles inconvenientes de disponibilidad del servidor (fallas eléctricas, fallas de hardware, etc.), la instalación y configuración de un servidor XCP adicional en modo Slave para garantizar que los usuarios no pierdan conectividad y acceso a los servicios y a las aplicaciones de la nube. Por lo tanto, el diseño de la solución se muestra en la figura 4.1

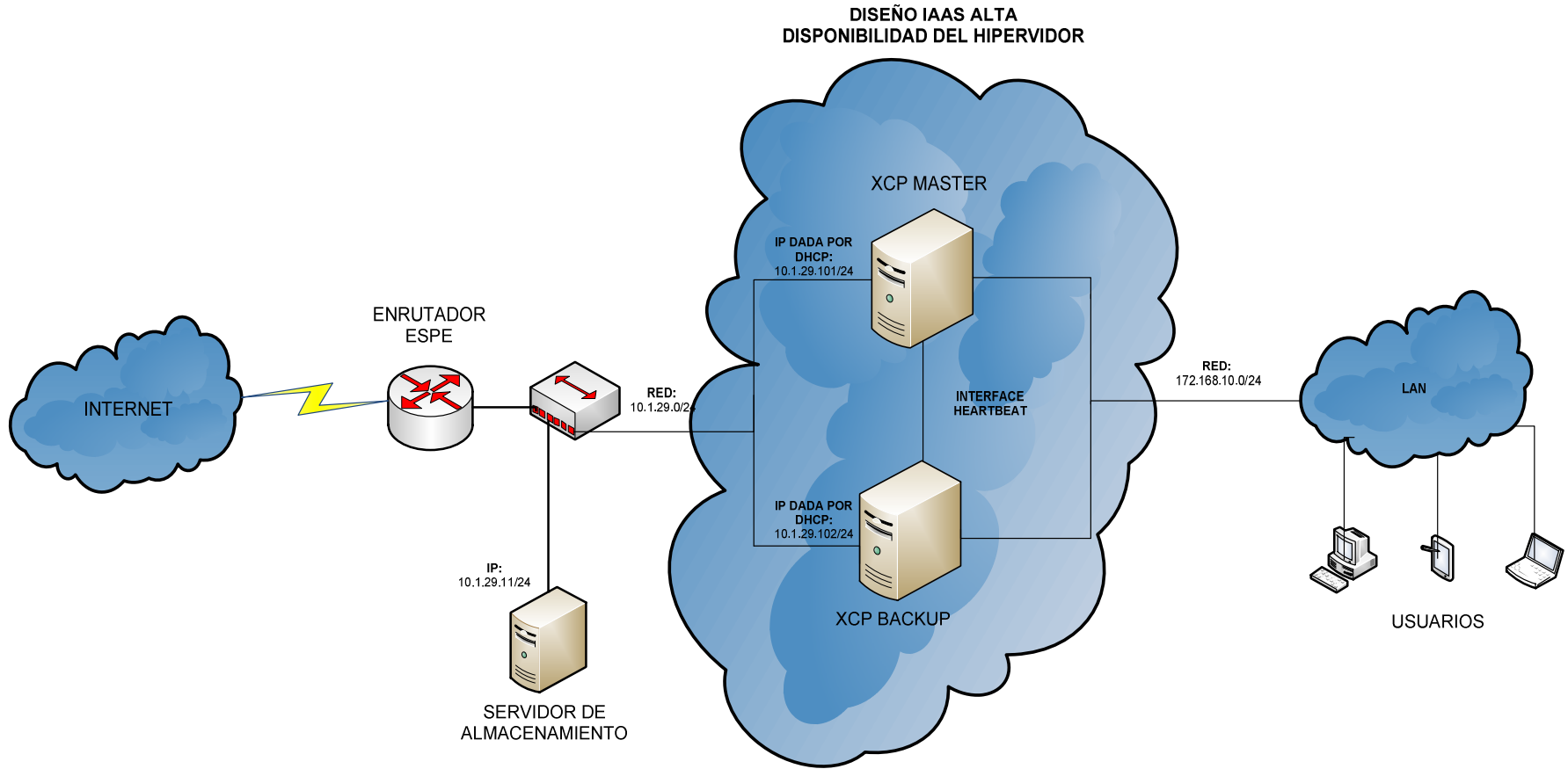


Figura 4. 1 Diseño de Alta Disponibilidad de Servidores XCP

Tal como se muestra en la figura 4.1, la distribución de los servidores en un esquema de alta disponibilidad viene dado por las siguientes características:

- Redundancia en conexiones eléctricas.
- Redundancia en conexiones de red.
- Redundancia en configuraciones del hipervisor.
- Redundancia en máquinas virtuales (redundancia de software).

Es decir, que si el servidor principal llegase a tener algún daño o falla, automáticamente el servidor de backup cubrirá las operaciones físicas y lógicas sin dejar a los usuarios sin servicio.

SOLUCIÓN B: FIREWALLS DE ALTA DISPONIBILIDAD

Tal como se indicó en 3.3.2, el Firewall Endian que se encontraba implementado en una de las máquinas virtuales de la nube, al ser una versión gratuita, no brindaba todas las características y funcionalidades que se requería para poder implementar métodos y políticas de seguridad como la Alta disponibilidad, ya que únicamente la versión pagada de este software proporciona dichas funcionalidades y características extras de configuración.

Por esta razón, se buscó un firewall Open Source que permita tener estas funcionalidades extras y de manera gratuita. PFSense fue el más indicado para implementarlo en la nube, no solo como firewall sino también como gestor, y visor de vulnerabilidades, gracias a los paquetes que trae consigo que brindan estas funciones.

PFSENSE es una herramienta Open Source que pertenece a una distribución personalizada de FreeBSD⁴⁸ para usarlo en redes LAN, WAN y que permite la implementación de servicios como firewalls, enrutador, balanceo de

⁴⁸ **FreeBSD**: Avanzado sistema operativo para arquitecturas x86 compatibles, amd64, UltraSPARC®.

carga, entre otras. Funciona bajo el sistema operativo m0n0wall⁴⁹. Es fácil de instalar en equipos comunes como cualquier ordenador o servidor independientemente de su arquitectura, pero que cuente con un mínimo de dos tarjetas de red.

En el presente proyecto, al ver que el Firewall Endian implementado en la nube no contaba con todas las funcionalidades como permitir alta disponibilidad, y la instalación de pluggins como Snort, Nmap, ClamAV, etc., se decidió cambiarlo por PFSense. De tal manera que la topología de la nube cambia, tal como se observa en la figura 4.3; en donde se observa la redundancia de los firewalls, dando mayor seguridad lógica a la infraestructura y plataforma de la nube.

⁴⁹ **mOnOwall**: Distribución FreeBSD dedicada, orientada a sistemas embebidos y diseñados para usar almacenamiento tipo flash.

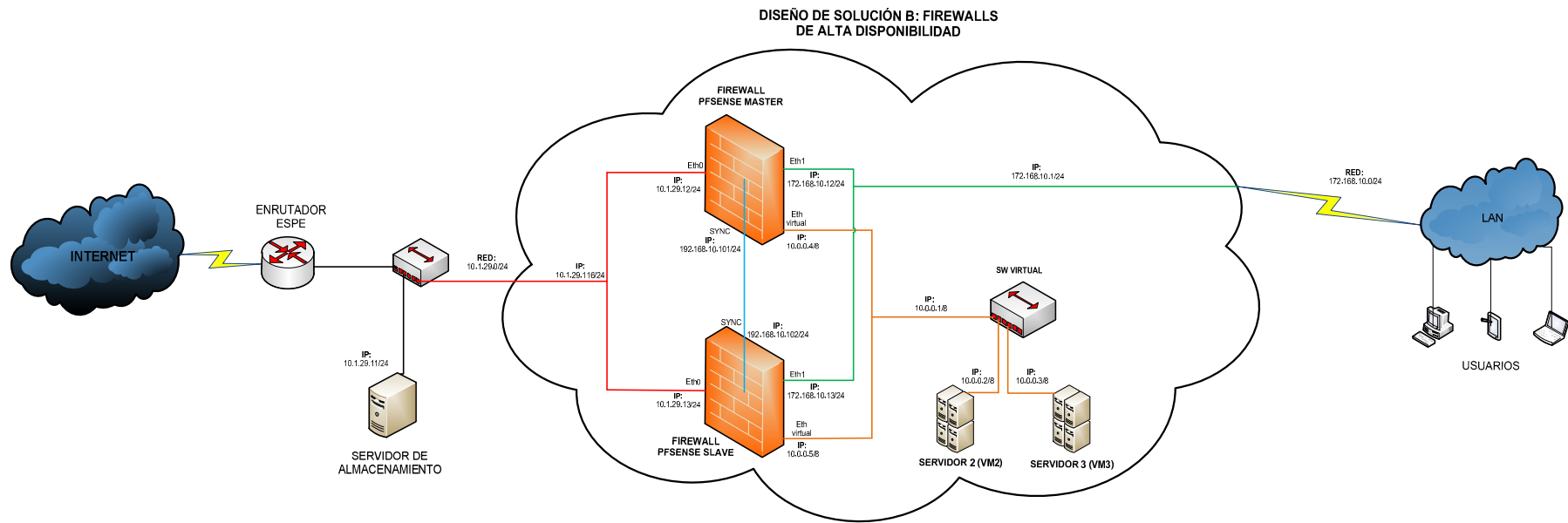


Figura 4. 2 Alta Disponibilidad de Firewall PFSENSE

SOLUCIÓN C: REDISTRIBUCIÓN DE RECURSOS DE LA NUBE

En el capítulo 3 se analizó la infraestructura de la nube y los diferentes elementos que la componen y que hacen parte del funcionamiento de la misma. En el apartado 3.1.2 se determinó que la ubicación del servidor de almacenamiento externo, no era la más indicada por parámetros de seguridad, debido a que se encontraba conectado directamente al switch proveedor de internet.

Por esta razón, se propone la reubicación del servidor FreeNAS y todos los parámetros de configuración que lo contemplan; de tal manera que se encuentre protegido y dentro de la nube para evitar que existan riesgos que puedan afectar a su funcionamiento o la información almacenada en el mismo. Tal como se muestra en la figura 4.3.

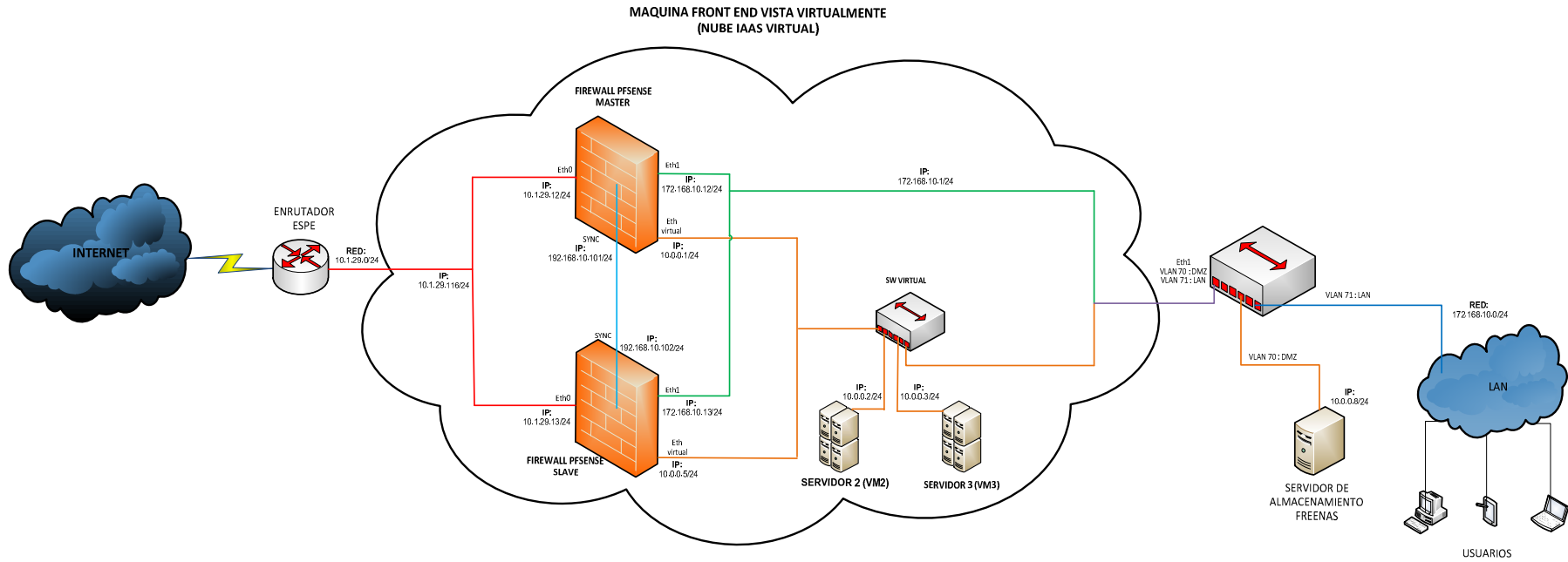


Figura 4. 3 Diseño de Redistribución de la nube. Servidor FreeNAS

Como se puede observar, el diseño planteado integra el servidor FreeNAS a la zona DMZ, para dotarlo de toda la seguridad que provee la nube, en especial del firewall a instalar.

4.2 SOLUCIONES DE SEGURIDAD EN PAAS

Al analizar el tipo de nube implementada en los Laboratorios del DEEE, se determinó que además de los servicios de Infraestructura y Software que ofrece, también puede ofertar el servicio de Plataforma si así lo llegara a requerir algún cliente y usuario.

Por lo tanto, como diseño de la seguridad en PAAS, se propone lo siguiente:

SOLUCIÓN A:

Debido a que el firewall escogido para la seguridad permite la instalación de paquetes adicionales, se instaló un IDS (Intrusion Detection System), para que monitoree y detecte intrusiones en la red, de tal manera que el administrador de la misma, siempre se encuentre alerta e identifique dicha intrusión en caso de que exista.

Por lo tanto, se selecciona el paquete SNORT en PFSense, mismo que es un Sistema de Detección de Intrusos de código abierto, y que a su vez funcionará como un IPS (Intrusion Prevention System) para analizar el tráfico de la red en tiempo real.

SOLUCIÓN B:

Otro paquete con el que cuenta PFSense es un antivirus llamado HAVP (HTTP Proxy Antivirus), que es una solución proxy con un filtro anti virus llamado

ClamAV, que escanea el tráfico de la red, detectando código malicioso en navegación HTTP.

Su funcionamiento se basa en las peticiones HTTP que los usuarios SAAS de la nube realicen hacia la red, dichas peticiones pasan por HAVP y en caso de que la navegación HTTP apunte a una muestra malware que ClamAV reconozca, HAVP mostrará una pantalla en el navegador del usuario informando la existencia de un virus.

SOLUCIÓN C:

Debido a que el servicio de Plataforma en la nube quiere decir que se le provee al usuario la capacidad de tener tanto hardware como software dentro de la nube, es decir máquinas virtuales a su disposición según sean sus necesidades. Se ha diseñado un plan para que el usuario pueda realizar peticiones de este tipo y que a su vez pueda gestionar y tener acceso a las máquinas virtuales requeridas según su necesidad.

Gracias a que Citrix proporciona las herramientas necesarias para la gestión y manejo del hipervisor XCP, se implementará un appliance de XenCenter, llamado Web Self Service, que es una consola de gestión para poder gestionar el servicio de plataforma de la nube.

Adicionalmente, Citrix XenCenter cuenta con la posibilidad de manejar diferentes tipos de usuarios para la gestión, administración y uso de la nube. Por lo tanto, como plan de gestión de usuarios se realizará lo siguiente:

- Instalación de un servidor Windows Server 2008 con los servicios de DNS y Active Directory.
- Manejo de usuarios desde Active Directory para establecer políticas de administración de los servicios de la nube desde XenCenter.

- Instalación de una máquina virtual en XCP con el software de gestión Web Self Services para el manejo de las máquinas virtuales en caso de requerimiento de Plataforma como Servicio (PAAS).
- Pruebas de gestión de máquinas virtuales con los usuarios registrados en el Active Directory de Windows Server 2008.

Por lo tanto, una vez establecidos los requerimientos, la topología de diseño de la solución será la de la figura 4.4.

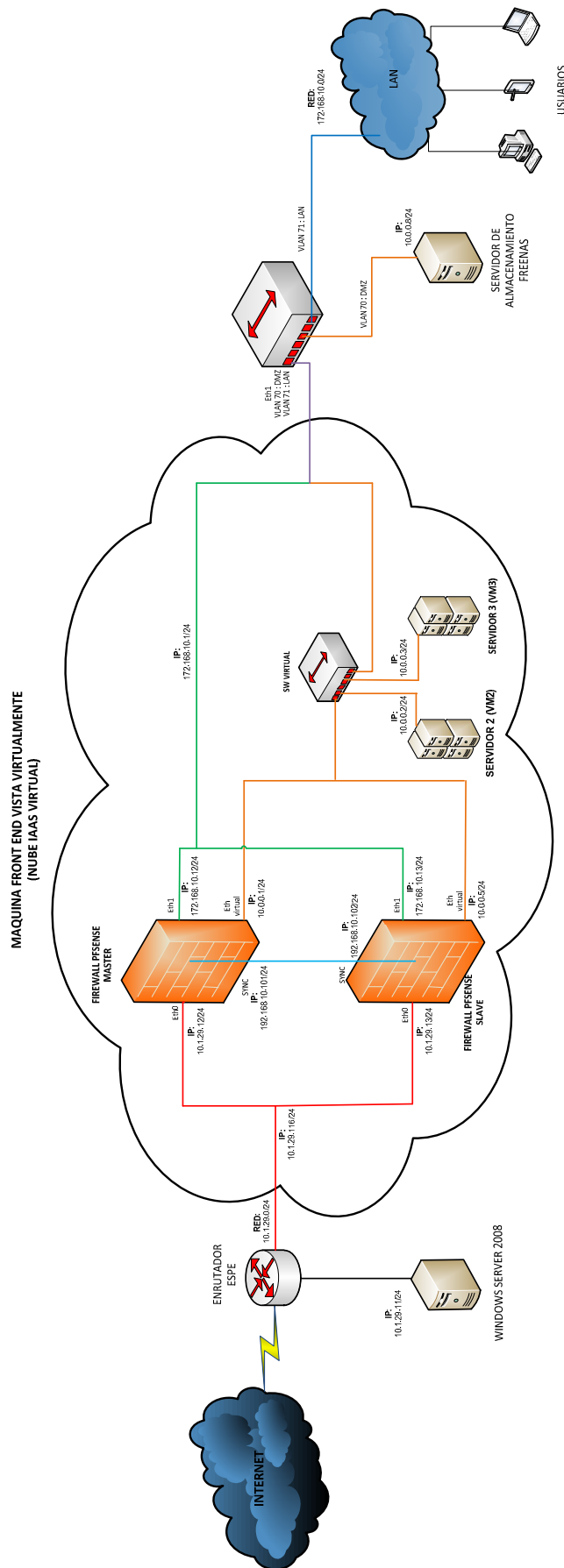


Figura 4. 4 Diseño de la solución PAAS

4.3 SOLUCIONES DE SEGURIDAD EN SAAS

La Seguridad en SAAS quiere decir, implementar todos los mecanismos y políticas de seguridad para brindar mayor protección y seguridad a los usuarios que hagan uso de los servicios de software que ofrece la nube.

En la figura 1.6 se especifican los diferentes niveles de servicio que puede ofrecer una nube de Cloud Computing, por lo tanto, al tener una nube cuyo principal objetivo fue ofertar Software como Servicio, necesariamente, la nube debe contar con los niveles de Infraestructura y Plataforma como Servicio.

En los puntos anteriores se propuso una solución de diseño de seguridad para estos niveles, por lo que además de dar seguridad a los mismos, también se brinda seguridad al Software que oferta la nube en lo que se refiere protección y administración de la Infraestructura y de la Plataformas que soportan Zimbra y OwnCloud.

De tal manera que al tener dos servicios como el de correo electrónico y almacenamiento en la nube, se consideraron las mejores alternativas para implementar Cloud Security en el modelo SAAS que oferta la nube implementada en los Laboratorios del DEEE.

4.3.1 Servicio de Correo Electrónico Zimbra

El servidor de correo Zimbra, tiene incorporado por defecto, filtros de seguridad como antispam y antivirus; pero además de esta protección para el servidor es necesario reforzar la seguridad para que los usuarios puedan acceder al servicio con la confianza de que su información será resguardada debidamente.

Por lo tanto, como soluciones de seguridad adicionales para Zimbra, se implementará lo siguiente:

- Actualizar la versión de Zimbra instalada.
- Actualización de reglas antispam.
- Validación de usuarios remitentes.

4.3.2 Servicio OwnCloud

El servidor OwnCloud permite tener una herramienta de almacenamiento en la nube, por lo tanto es importante brindar protección al servicio para precautelar la información de los usuarios que hagan uso de este servicio.

Como soluciones de seguridad, se implementará:

- Instalación de aplicaciones propias de Owncloud como antivirus.
- Manejo de cuentas de usuarios.

CAPÍTULO V

IMPLEMENTACIÓN DE CLOUD SECURITY

5.1 IMPLEMENTACIÓN DE CLOUD SECURITY EN IAAS

En el capítulo anterior se plantearon 3 soluciones para IAAS, las cuales una vez diseñadas las topologías respectivas, se inicia el proceso de implementación de las soluciones propuestas.

5.1.1 Implementación de la SOLUCIÓN A: Alta Disponibilidad de Servidores Físicos

La plataforma Xen Cloud Platform no contempla el servicio de alta disponibilidad, tal como lo especifica la página oficial de Citrix, cuya tabla de características se muestra en la figura 5.1. [24]

Por lo tanto, no fue posible realizar la configuración de alta disponibilidad entre dos hipervisores, uno master y otro en modo slave; ya que XCP no posee esta funcionalidad a diferencia del hipervisor Xen Server.

XCP/XenServer Feature Matrix

Features	Xen Cloud Platform	XenServer Free	XenServer Advanced	XenServer Enterprise	XenServer Platinum
Cost/Licensing	Free/Open Source (Multiple Licenses ¹)	Free/Citrix EULA ↗	Paid/Citrix EULA ↗		
XenServer hypervisor	X	X	X	X	X
IntelliCache	X	X	X	X	X
Resilient distributed management architecture	X	X	X	X	X
VM disk snapshot and revert	X	X	X	X	X
XenCenter management	X	X	X	X	X
Conversion tools	X	X	X	X	X
XenMotion® live Migration	X	X	X	X	X
Heterogeneous pools	X		X	X	X
Dynamic Memory Control	X		X	X	X
Performance alerting and reporting	X		X	X	X
Distributed virtual switching management tool			X	X	X
High availability			X	X	X
Automated VM protection and recovery	X		X ²	X ²	X
Host power management	X			X	X
Live memory snapshot and revert	X			X	X
Role-based administration	X			X	X
Dynamic workload balancing				X	X
Provisioning services (virtual)				X	X

Figura 5. 1 Características de XCP vs. Xen Server

Sin embargo, la pila de gestión y las consolas para administrar el hipervisor si contemplan realizar alta disponibilidad entre un pool de servidores. Este servicio está disponible en el producto comercial sobre el que está basada la plataforma open-source XCP, la solución de Citrix XenServer.

El software que permite gestionar la plataforma en un entorno amigable Windows, es XenCenter. Esta aplicación viene en varias versiones con diferentes funcionalidades cada una pero la versión implementada será la gratuita que también cuenta con la funcionalidad de realizar alta disponibilidad entre dos hipervisores Xen Cloud Platform.

La posibilidad de implementar alta disponibilidad en XenCenter permite la configuración de un clúster⁵⁰ entre un XCP Master y un XCP Slave mediante la configuración de pools de recursos; además de que es necesario contar con almacenamiento compartido, a través de iSCSI o mediante disco ofrecido por

⁵⁰ **CLÚSTER:** Es un conjunto de computadoras construidos mediante la utilización de hardware comunes y que se comportan como si fuesen una única computadora.

HBA, para que las máquinas virtuales se encuentren protegidas, ya que estarán creadas en un disco compartido por todos los nodos del Pool; tal como se observa en la figura 5.2

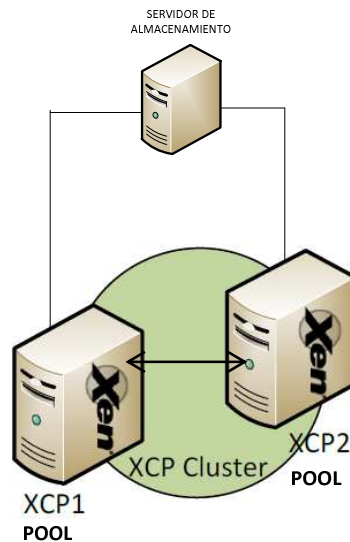


Figura 5. 2 Clúster de servidores XCP

Para poder escoger el tipo de configuración compartida, es necesario saber cuáles soporta Xen Cloud Platform:

1. NFS: Es un sistema de archivos en red, que permite que distintos sistemas conectados a una misma red puedan acceder a ficheros remotos.

El servidor XCP consta con un disco local que almacena ficheros; pero adicionalmente, para habilitar el servicio de alta disponibilidad se puede configurar NFS como recurso compartido del pool de servidores. Con esto, se garantiza que cualquier host pueda acceder a las máquinas virtuales del XCP que se almacenadas que usan el modelo de disco físico virtual VHD que permite optimizar la velocidad sobre los protocolos distribuidos en red.

2. iSCSI: Permite el uso del protocolo SCSI⁵¹ sobre redes TCP/IP para la transferencia de datos mediante una interfaz Ethernet. Lo cual permite una solución de almacenamiento centralizada.

Su uso en XenCenter permite la implementación de discos compartidos como Storage Repository en donde los volúmenes lógicos de las máquinas virtuales se asocian a un volumen lógico (LVM) del servidor de almacenamiento.

3. Hardware HBA: Es un controlador de host, llamado adaptador de bus de host que conecta los servidores físicos a una red y dispositivos de almacenamiento. Su funcionamiento es similar a iSCSI, pero difieren en que HBA permite acceder de forma compartida al almacenamiento a través de una red de fibra óptica de gran velocidad.

Para que HBA pueda funcionar en XenCenter, se debe disponer de HBA's compatibles con el mismo como por ejemplo Qlogic o Emulex.

Debido a que la topología de la nube ya cuenta con un servidor de almacenamiento para tener un respaldo de las máquinas virtuales creadas, no se implementó el servicio de alta disponibilidad entre dos servidores XCP.

Pero en el caso de haber realizado la implementación de este servicio, se hubiera realizado lo siguiente:

1. Una vez creado el Pool (XCP Clúster), se deberá crear una unidad de almacenamiento que sea compartida por todos los nodos.

La alta disponibilidad en XenCenter funciona con "Heartbeat SR" que será la conexión establecida entre los pools de servidores para tener disponibilidad de las máquinas virtuales a través de un Storage Repository.

2. Una vez creada el servidor de almacenamiento, desde la consola de gestión XenCenter escogemos el pool creado donde se encuentra el

⁵¹ **SCSI**, (Interfaz de Sistema para Pequeñas Computadoras), es una interfaz estándar para la transferencia de datos entre distintos dispositivos del bus de la computadora.

servidor XCP Master, y escogemos la opción de configuración de alta disponibilidad.

La ventana que se abrirá a continuación mostrará todos los repositorios de almacenamiento configurados en los pools previamente. Tal como se observa en la figura 5.3 [28]

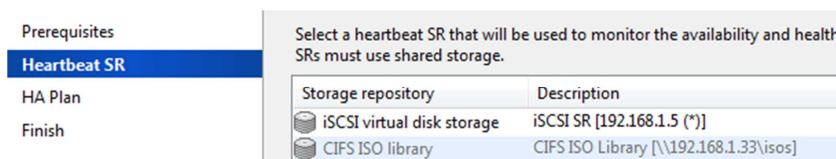
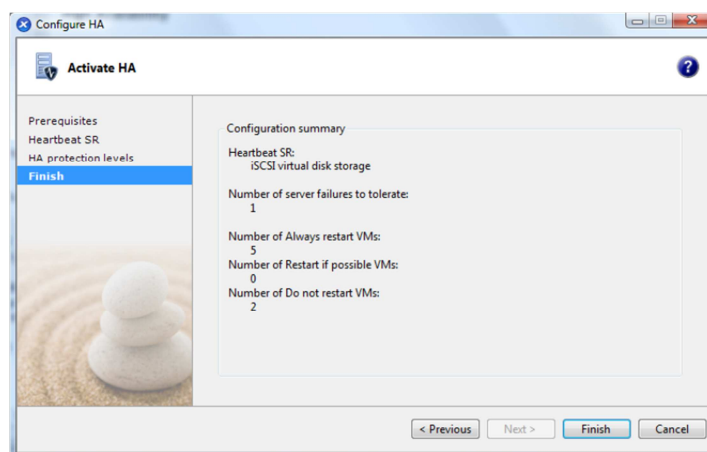


Figura 5. 3 Configuración de Alta Disponibilidad

3. Luego, se debe configurar el plan de Alta Disponibilidad. Para ello es muy importante definir cuantos Hosts pueden fallar; para lo cual, el propio asistente nos calcula el máximo en función de las máquinas virtuales que pongamos “**Restart**” en Restart Priority. Una vez finalizada la configuración debe aparecer un mensaje como se observa en la figura 5.4. [28]



✓ HA is guaranteed. The maximum number of server failures that HA can protect against is 2.

Figura 5. 4 Alta Disponibilidad configurada

4. Una vez que HA está activo, cada host escribe regularmente actualizaciones de almacenamiento en el disco virtual heartbeat, y el servicio que brinda la nube nunca deja de funcionar.

Cabe recalcar que a pesar de no tener la posibilidad de implementar Alta Disponibilidad de los Hiperviores, existe un servidor de almacenamiento externo que contiene un backup de todas las máquinas virtuales de XCP, de tal forma que si alguna de estas llegara a fallar o sufrir algún tipo de daño, automáticamente se habilitará el backup de dicha máquina pero desde el servidor de almacenamiento FreeNAS.

Gracias a esta solución, siempre existirá alta disponibilidad de las máquinas virtuales configuradas en el XCP.

5.1.2 Implementación de la SOLUCIÓN B: Firewalls de Alta Disponibilidad

Para implementar esta solución de diseño se buscó un firewall Open Source que cumpla con los requerimientos y funcionalidades necesarias para implementar las medidas de seguridad mencionadas, y tal como se indicó en la Solución, se escogió el firewall PFSense que es una solución de software libre de FreeBSD.

A. INSTALACIÓN DE PFSENSE:

1. Lo primero que se hizo fue apagar el Firewall Endian para que todos los servicios que brindaba a la nube se suspendan para poder implementar la nueva solución; y luego, se descargó PFSense de la siguiente ubicación <http://linux.softpedia.com/progDownload/pfSense-Download-5550.html>.
2. Una vez descargado el software, se adjunta el archivo .iso a la unidad cifs de los repositorios desde Citrix XenCenter, ya que FreeNAS da los permisos necesarios para que la máquina que contiene almacenado el

archivo .iso pueda acceder a los repositorios y adjuntar el software de instalación.

- Una vez realizado esto, se procede a la instalación de PFSense. Desde XenCenter, presionamos la pestaña de **VM**, y se selecciona la opción de **New VM**.

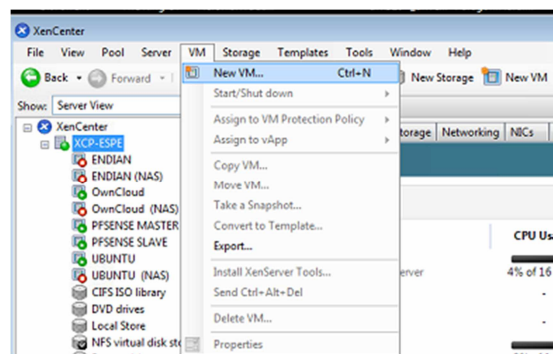


Figura 5. 5 Creación de nueva Máquina Virtual

- En la opción de Templates se selecciona **Other Install Media** para poder seleccionar la imagen iso guardada en el repositorio CIFS; y seleccionar el botón **Next**.

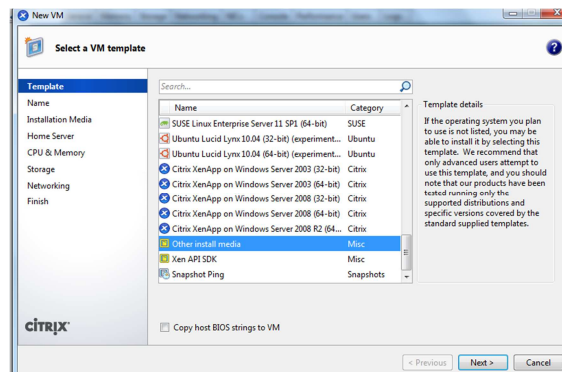


Figura 5. 6 Selección de tipo de VM

5. En la siguiente ventana se coloca el nombre que se desee poner a la máquina virtual y seleccionamos **Next**.

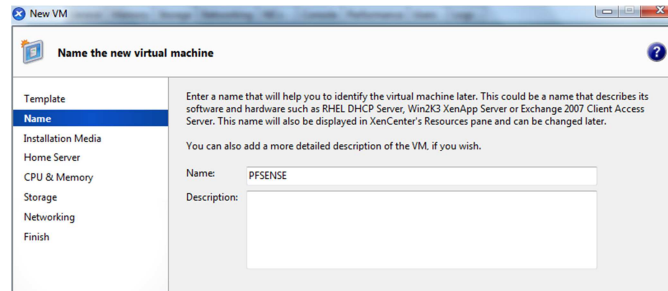


Figura 5. 7 Nombre de la VM

6. En la siguiente ventana se debe escoger la ubicación donde se encuentra la imagen iso a instalar, por lo tanto, ahí se coloca la opción de CIFS ISO Library, que es en donde se encuentra la imagen iso anteriormente.

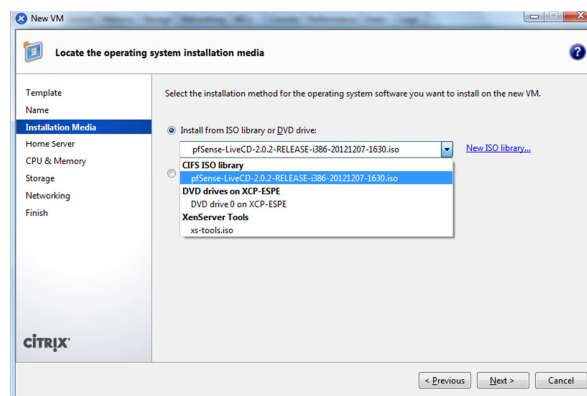


Figura 5. 8 Selección de ubicación de imagen iso

7. Luego se selecciona el servidor en el cual se desea instalar la máquina virtual y seleccionamos **Next**.

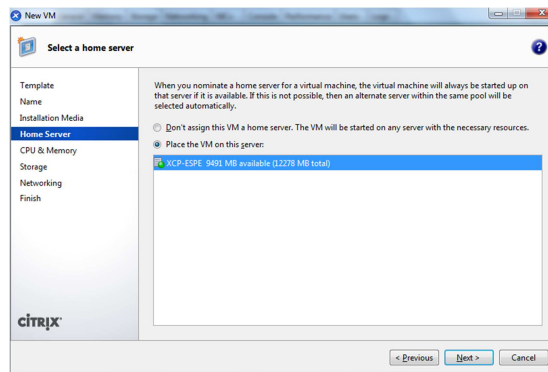


Figura 5. 9 Selección de Servidor en donde se instalará la MV

8. Posteriormente, se deben seleccionar las características de la máquina virtual como cantidad de CPU's y la cantidad de memoria.

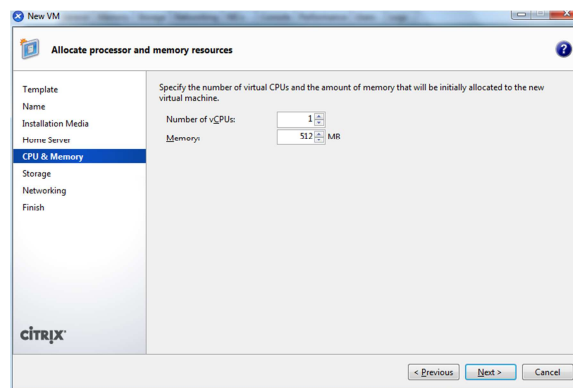


Figura 5. 10 Selección de cantidad de CPU's y memoria de la VM

9. Luego se selecciona la ubicación del disco virtual para la máquina y el tamaño. Como es una máquina virtual local, se debe seleccionar el disco local del servidor XCP y con un tamaño de 8 GB.

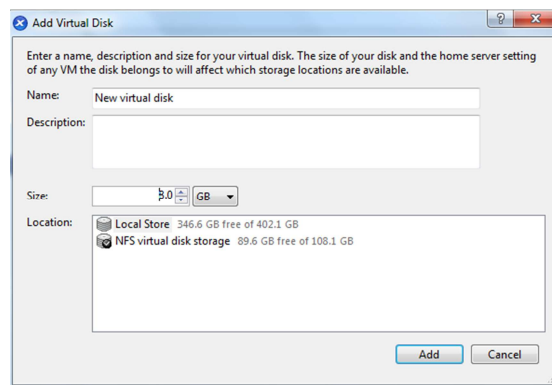


Figura 5. 11 Selección de Virtual Disk y tamaño del mismo

10. Finalmente, se escogen las interfaces que va tener la máquina virtual, en este caso seleccionamos las mismas que tenía Endian hasta realizar la configuración de PFSense; ya que posteriormente se deberá añadir una interfaz adicional que permitirá la sincronización entre los firewalls redundantes.

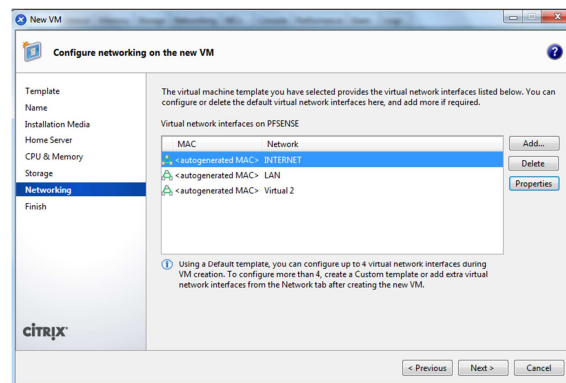


Figura 5. 12 Selección de interfaces virtuales de la VM

11. Por último nos aparecerá una ventana en donde se resume las características configuradas para la nueva máquina virtual; y procedemos a la creación de la misma.

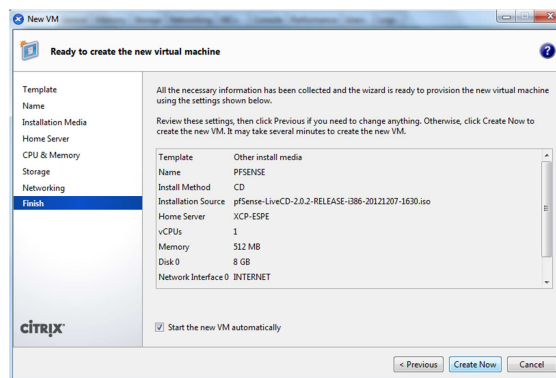


Figura 5. 13 Creación de la VM

Nota: Al igual que se creó esta máquina virtual, procedemos a crear una segunda máquina con las mismas características pero con nombre diferente para poder realizar la configuración de redundancia de firewalls para poder tener alta disponibilidad del servicio.

B. CONFIGURACIÓN DE MÁQUINAS PFSense:

Una vez instaladas las dos máquinas virtuales, una llamada PFSense Master y otra PFSense Slave; procedemos a la configuración de las mismas.

Tal como se indicó anteriormente, se instalan dos máquinas virtuales de PFSense para tener alta disponibilidad del servicio de Firewall, por lo que antes de configurar las máquinas es necesario crear una nueva interfaz en el servidor XEN que permita realizar las funciones de sincronización entre los firewalls.

CREACIÓN E IMPLEMENTACIÓN DE NUEVA INTERFAZ DE RED:

1. Para agregar las interfaces mencionadas, se debe seleccionar el servidor XCP-ESPE, en el lado derecho se pueden observar varias pestañas que

indican las características que tiene configuradas, una de ellas es la pestaña de Networking, en la cual se crea la nueva interfaz.

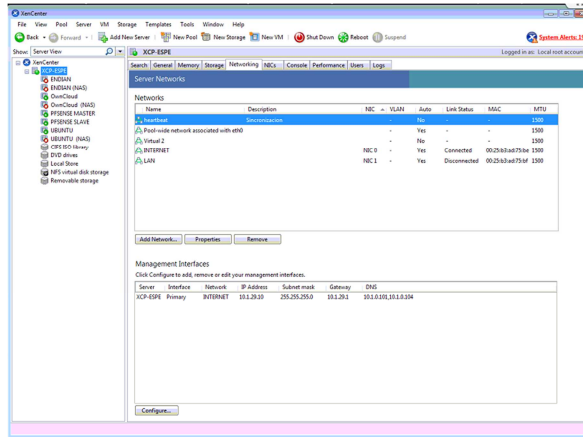


Figura 5. 14 Creación de nueva interfaz

2. Seleccionamos el botón inferior izquierdo para añadir una nueva interfaz de red, y en el cuadro que se abrirá a continuación seleccionamos la segunda opción: **Single Server Private Network**. Y posteriormente, se coloca el nombre de la interfaz y su descripción.
3. Y, finalmente se puede observar la interfaz creada en el servidor.

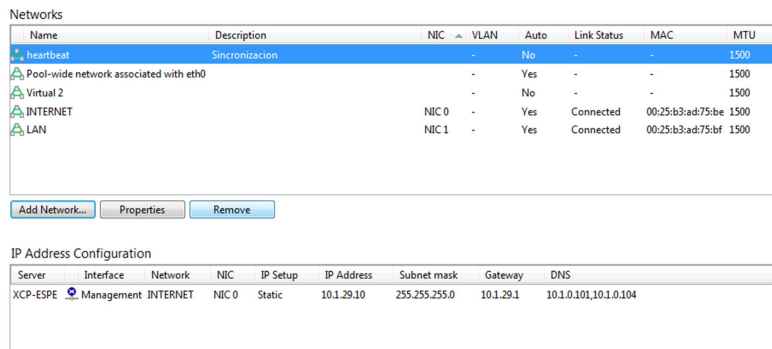


Figura 5. 15 Creación de la interfaz

4. Luego, tanto en la máquina virtual del PFSense Master, como del PFSense Slave, añadimos la interfaz creada.

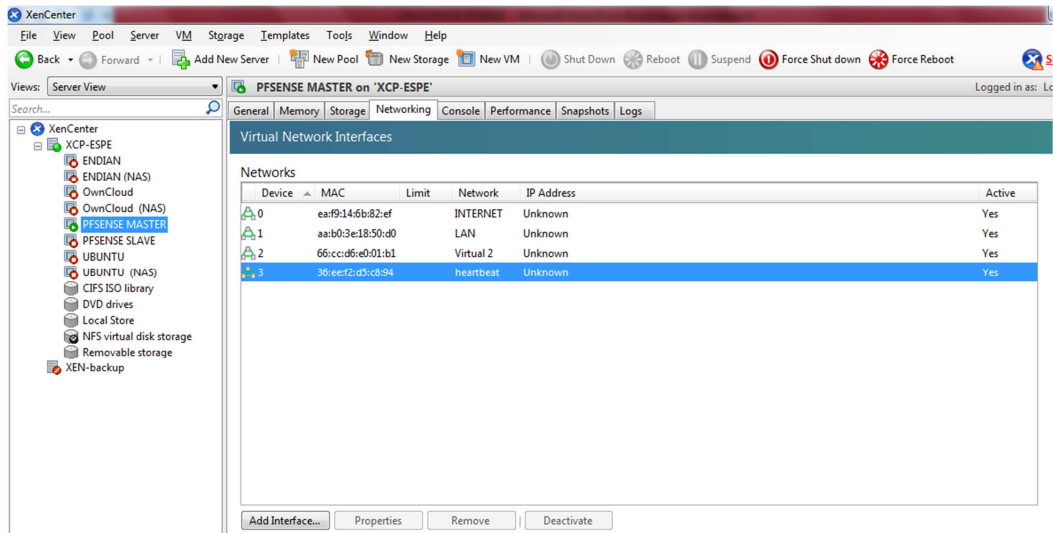


Figura 5. 16 Interfaz de Sincronización añadida en PFSense

CONFIGURACIÓN DE PFSense

Una vez instalado PFSense aparecerá una ventana de configuración de la siguiente manera:



Figura 5. 17 Interfaz de configuración de PFSense

1. En la siguiente ventana se debe escoger la opción 1 para poder asignar las tarjetas de red a cada una de las interfaces que tiene PFSense:

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): re1

Optional interface 1 description found: DMZ
Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished): re2

Enter the Optional 2 interface name or 'a' for auto-detection
(or nothing if finished): re3

Enter the Optional 3 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:
WAN -> re0
LAN -> re1
OPT1 -> re2
OPT2 -> re3

Do you want to proceed [y/n]?y
Writing configuration...
```

Figura 5. 18 Asignación de tarjetas de red a Interfaces de PFSense

2. Una vez asignadas las interfaces se debe configurar las direcciones de cada una. Esto se debe hacer tanto en el Firewall Master como en el Slave.

```
FreeBSD/i386 (pfsense.espefw) (tty0)
** Welcome to pfSense 2.0.2-RELEASE-pfSense (i386) on pfsense ***

WAN (wan)          -> re0          -> 10.1.29.12
LAN (lan)          -> re1          -> 172.168.10.12
DMZ (opt1)        -> re2          -> 10.0.0.1
SYNC (opt2)       -> re3          -> 192.168.10.101

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

Enter an option: █
```

Figura 5. 19 Configuración de Interfaces de red. PFSense Master

```

FreeBSD/i386 (pfSense.localdomain2) (tty00)

*** Welcome to pfSense 2.0.2-RELEASE-pfSense (i386) on pfSense ***

WAN (wan)          -> re0          -> 10.1.29.13
LAN (lan)          -> re1          -> 172.168.10.13
DMZ (opt1)         -> re2          -> 10.0.0.5
SYNC (opt2)        -> re3          -> 192.168.10.102

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 (ssh)
7) Ping host

Enter an option:

```

Figura 5. 20 Configuración de Interfaces de red. PFSense Slave

- Una vez realizadas estas configuraciones ya podemos acceder a la consola de gestión de PFSense mediante la interfaz gráfica a través del browser; únicamente ingresando la IP configurada en la interfaz LAN. En la consola que se abrirá a continuación se debe configurar los parámetros básicos de PFSense como el nombre de host, el dominio, y los servidores DNS Primario y Secundario, zona horaria y la configuración de las interfaces.

The screenshot shows the 'Basic' configuration page in the PFSense web interface. It includes the following sections:

- Hostname:** A text input field containing 'pfsense'. Below it, a note says: 'Name of the firewall host, without domain part e.g. firewall'.
- Domain:** A text input field containing 'localdomain'. Below it, a note says: 'Do not use 'local' as a domain name. It will cause local hosts running mDNS (avahi, bonjour, etc.) to be unable to resolve local hosts not running mDNS. e.g. mycorp.com, home, office, private, etc.'
- DNS servers:** A table with two columns: 'DNS Server' and 'Use gateway'.

DNS Server	Use gateway
10.0.0.3	LAN
8.8.8.8	None
	None
	None

 Below the table, there is explanatory text: 'Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS forwarder and for PPTP VPN clients. In addition, optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.'
- Checkboxes:**
 - Allow DNS server list to be overridden by DHCP/PPP on WAN. Below it, a note says: 'If this option is set, pfsense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). However, they will not be assigned to DHCP and PPTP VPN clients.'
 - Do not use the DNS Forwarder as a DNS server for the firewall. Below it, a note says: 'By default localhost (127.0.0.1) will be used as the first DNS server where the DNS forwarder is enabled, so system can use the DNS forwarder to perform lookups. Checking this box omits localhost from the list of DNS servers.'
- Time zone:** A dropdown menu set to 'America/Guayaquil'. Below it, a note says: 'Select the location closest to you'.

Figura 5. 21 Configuración básica de PFSense

- En las interfaces se debe revisar la configuración de la dirección IP, y se debe configurar la dirección de Gateway y los servidores DNS primario y

secundario. Estas configuraciones se deben realizar tanto en el PFSense Master como Slave.

Interfaces: LAN

General configuration	
Enable	<input checked="" type="checkbox"/> Enable Interface
Description	<input type="text" value="LAN"/> Enter a description (name) for the interface here.
Type	Static
MAC address	<input type="text"/> Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections) Enter a MAC address in the following format: xxxxxxxxxx or leave blank
MTU	<input type="text"/> If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.
MSS	<input type="text"/> If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and duplex	<input type="button" value="Advanced"/> - Show advanced option

Static IP configuration	
IP address	<input type="text" value="172.168.10.12"/> / <input type="text" value="24"/>
Gateway	<input type="text" value="None"/> -or- add a new one. If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above

Figura 5. 22 Configuración de Interface LAN. PFSense Master

Interfaces: DMZ

General configuration	
Enable	<input checked="" type="checkbox"/> Enable Interface
Description	<input type="text" value="DMZ"/> Enter a description (name) for the interface here.
Type	Static
MAC address	<input type="text"/> Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections) Enter a MAC address in the following format: xxxxxxxxxx or leave blank
MTU	<input type="text"/> If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.
MSS	<input type="text"/> If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and duplex	<input type="button" value="Advanced"/> - Show advanced option

Static IP configuration	
IP address	<input type="text" value="10.0.0.1"/> / <input type="text" value="24"/>
Gateway	<input type="text" value="DMZGW - 10.0.0.1"/> -or- add a new one. If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above

Figura 5. 23 Configuración de Interface DMZ. PFSense Master

Interfaces: WAN

General configuration	
Enable	<input checked="" type="checkbox"/> Enable Interface
Description	WAN Enter a description (name) for the interface here.
Type	Static
MAC address	<input type="text"/> Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections) Enter a MAC address in the following format: xxxxxxxxxx or leave blank
MTU	<input type="text"/> If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.
MSS	<input type="text"/> If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and duplex	Advanced - Show advanced option
Static IP configuration	
IP address	10.1.29.12 / 24
Gateway	WAN0 - 10.1.29.1 -or- add a new one. <small>If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above.</small>

Figura 5. 24 Configuración de Interface WAN. PFSense Master

Interfaces: SYNC

General configuration	
Enable	<input checked="" type="checkbox"/> Enable Interface
Description	SYNC Enter a description (name) for the interface here.
Type	Static
MAC address	<input type="text"/> Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections) Enter a MAC address in the following format: xxxxxxxxxx or leave blank
MTU	<input type="text"/> If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.
MSS	<input type="text"/> If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and duplex	Advanced - Show advanced option
Static IP configuration	
IP address	192.168.10.101 / 24
Gateway	None -or- add a new one. <small>If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above.</small>

Figura 5. 25 Configuración de Interface de sincronización. PFSense Master

5. Luego se configuran las reglas del NAT⁵² del firewall.

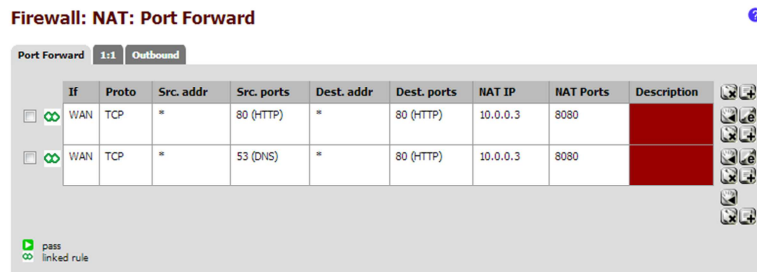



Figura 5. 26 Configuración de NAT: Port Forward

En esta regla se configura el acceso a los servidores desde la red WAN, que en este caso, solo se desea que se haga la traducción o re direccionamiento para el servidor DNS con la dirección IP 10.0.0.3.

Como se puede observar, se abre el puerto 8080 para la conexión con el servidor DNS; adicionalmente, el símbolo  (linked rule) indica que al activar la regla, automáticamente se crea una regla en el firewall dentro de la opción “Rules”.

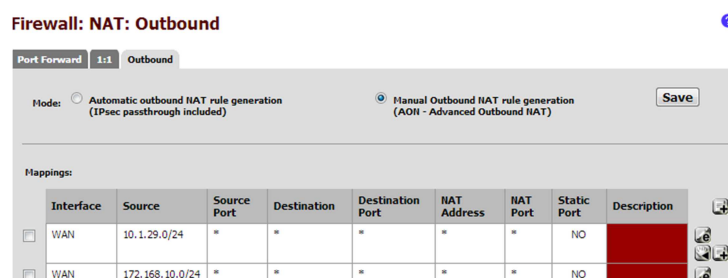


Figura 5. 27 Configuración de NAT: Outbound

⁵² **NAT: Network Address Translation.** Es un mecanismo para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.

La regla Outbound permite que el tráfico que salga de PFSENSE sea traducido a todas las redes que componen la topología.

Como primer paso, se debe seleccionar la opción de configuración Manual ya que aquí se activa el NAT de salida avanzado para que PFSENSE no genere automáticamente reglas NAT de salida.

Luego, se definió las combinaciones posibles entre la LAN y WAN, tal como se indica en la figura 5.27

6. Luego se configuran las reglas del firewall para cada una de las interfaces. Es necesario la configuración de estas reglas para permitir o denegar el tráfico en cada una de las interfaces.

Firewall: Rules S L ?

Floating WAN LAN DMZ SYNC

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	*	*	*	none		
	*	WAN address	*	LAN address	*	*	none		
	*	WAN address	*	DMZ address	*	*	none		

pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled)

Figura 5. 28 Configuración Reglas para la WAN

Las reglas configuradas para la WAN no permiten el tráfico hacia la LAN ni hacia la DMZ.

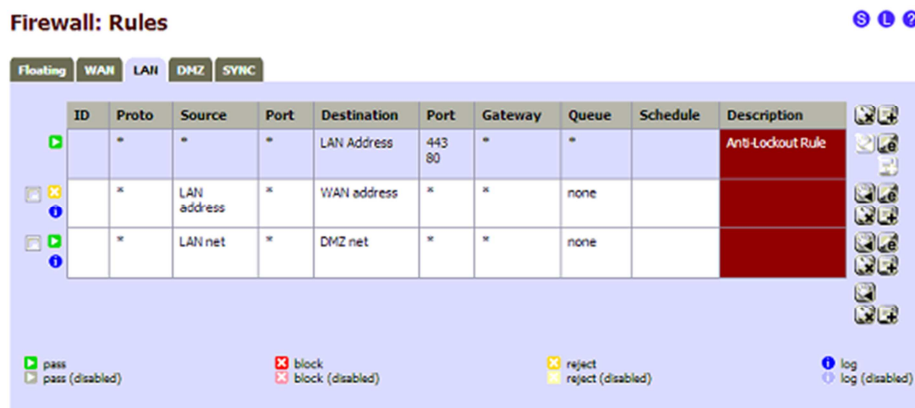


Figura 5. 29 Configuración Reglas para la LAN

Las reglas configuradas para la LAN permiten el tráfico desde la LAN hacia la DMZ y hacia la WAN por medio de cualquier protocolo.

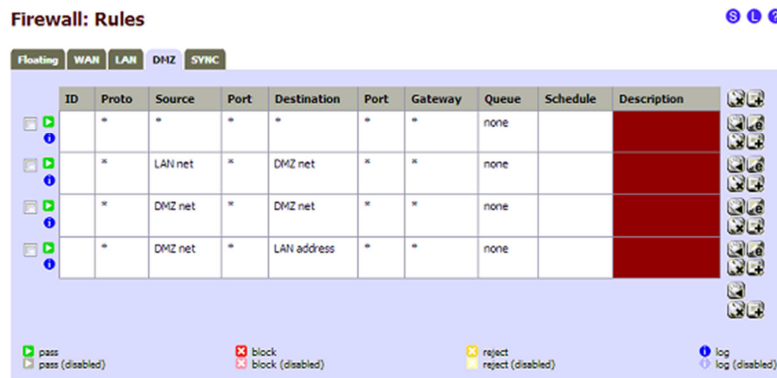


Figura 5. 30 Configuración Reglas para la DMZ

Las reglas configuradas para la zona DMZ permiten el tráfico desde la DMZ hacia la LAN y el tráfico interno de la zona, por medio del protocolo TCP.

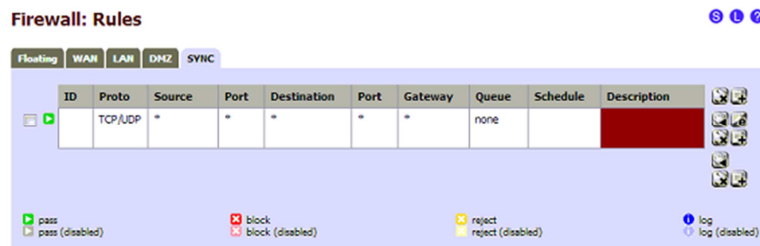


Figura 5. 31 Configuración Reglas para la interfaz de Sincronización

La primera regla que se ve configurada para la interfaz de sincronización se crea por defecto, para permitir el tráfico dentro de la misma interfaz.

- Una vez configuradas las reglas de firewall se debe configurar la alta disponibilidad tanto el PFSENSE MASTER como el PFSENSE SLAVE para tener ininterrumpidamente el servicio.

El sistema de funcionamiento de este firewall se basa en la utilización de los recursos CARP⁵³ (Common Address Redundancy Protocol) y PFSYNC⁵⁴ (packet filter state table synchronisation interface), que permiten el funcionamiento de dos servidores Firewall a manera de HA (High Ability) en modo activo-pasivo; es decir, ante la falta de disponibilidad del nodo MAESTRO, el nodo ESCLAVO asume las funciones del principal y mantiene todas sus conexiones activas.

Específicamente, el recurso CARP se basa en que todos los nodos Firewall compartan mediante técnicas de manipulación de las respuestas ARP, una dirección común para cada subred. Por lo tanto, todas las comunicaciones se deben enviar a la dirección CARP, de manera que cuando no responda el nodo MASTER, el nodo SLAVE responderá evitando así que se pierda el servicio y las conexiones.

⁵³ **CARP:** Es un protocolo que permite que varias máquinas en el mismo segmento de red compartan una dirección IP.

⁵⁴ **PFSYNC:** Es una interfaz de red de PFSENSE que permite el monitoreo del dispositivo mediante el protocolo TCPDUMP, con el cual se pueden observar en tiempo real los cambios de estado del dispositivo.

Tal como se indicó en el punto 4, en los dos servidores se configuraron las interfaces de Sincronización para permitir la comunicación entre los dos Firewalls, en la figura 4.2., se puede observar esta interfaz configurada con la IP: 192.168.10.101 en el MASTER, y la IP: 192.168.10.102 en el SLAVE.

- Una vez que se tienen configuradas las interfaces de sincronización, se procede a configurar los parámetros de CARP, es decir las direcciones en común para cada red (WAN, LAN, DMZ). Tanto para el MASTER como para el SLAVE.

Esta configuración se la hace desde la pestaña Firewall -> Virtual IP. Tal como se observa en la figura 5.32.

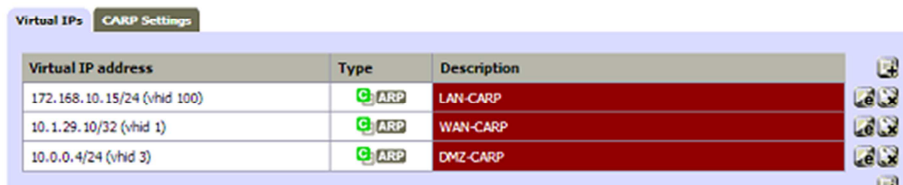
Firewall: Virtual IP Address: Edit

Edit Virtual IP	
Type	<input type="radio"/> Proxy ARP <input checked="" type="radio"/> CARP <input type="radio"/> Other <input type="radio"/> IP Alias
Interface	WAN
IP Address(es)	Type: Single address Address: 10.1.29.10 / 32 <small>This must be the network's subnet mask. It does not specify a CIDR range.</small>
Virtual IP Password	Enter the VHID group password.
VHID Group	1 Enter the VHID group that the machines will share
Advertising Frequency	Base: 1 Skew: 0 The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.
Description	WAN-CARP You may enter a description here for your reference (not parsed).

Figura 5. 32 Configuración Virtual IP para CARP en WAN

De igual manera, se debe configurar las interfaces LAN y DMZ, tal como se observa en la figura 5.33

Firewall: Virtual IP Addresses



Virtual IP address	Type	Description
172.168.10.15/24 (vhid 100)	CARP	LAN-CARP
10.1.29.10/32 (vhid 1)	CARP	WAN-CARP
10.0.0.4/24 (vhid 3)	CARP	DMZ-CARP

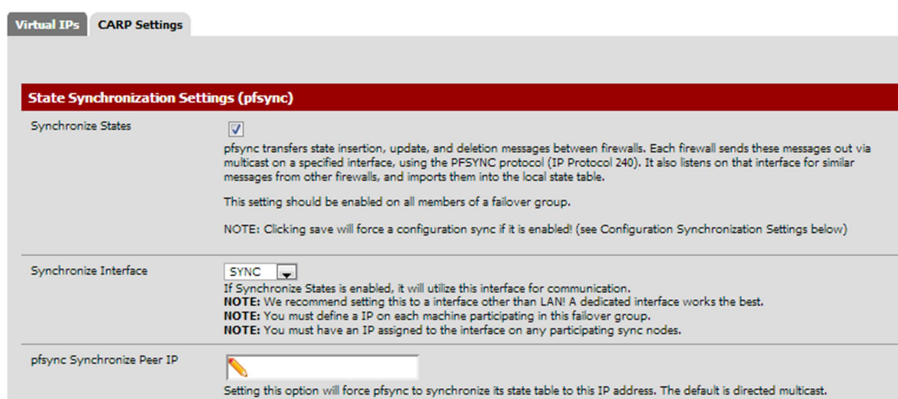
Figura 5. 33 Virtual IP's para configuración de CARP

Cabe recalcar que el password colocado en cada una de las configuraciones es el que se usará para identificar la infraestructura CARP del grupo configurado, es decir para WAN, LAN y DMZ. Además, el Vhid Group es el valor que se asignará a las comunicaciones entre los nodos, y la frecuencia con la que se anunciarán las opciones debe ser 0 para el caso del MASTER.

Una vez configuradas las Virtual IPs se puede observar en la figura 4.37 el resumen de estas configuraciones.

9. Luego se deben configurar las características de CARP en el MASTER. Aquí es en donde se dan los parámetros de PFSYNC y CARP para poder sincronizar los dos servidores.

Services: CARP Settings: Edit



State Synchronization Settings (pfsync)

Synchronize States

pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.

This setting should be enabled on all members of a failover group.

NOTE: Clicking save will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface

If Synchronize States is enabled, it will utilize this interface for communication.

NOTE: We recommend setting this to a interface other than LAN! A dedicated interface works the best.

NOTE: You must define a IP on each machine participating in this failover group.

NOTE: You must have an IP assigned to the interface on any participating sync nodes.

pfsync Synchronize Peer IP

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP: 192.168.10.102
Enter the IP address of the firewall to which the selected configuration sections should be synchronized.
NOTE: XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
NOTE: Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username: admin
Enter the webConfigurator username of the system entered above for synchronizing your configuration.
NOTE: Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password: [Masked]
Enter the webConfigurator password of the system entered above for synchronizing your configuration.
NOTE: Do not use the Synchronize Config to IP and password option on backup cluster members!

Synchronize Users and Groups:
When this option is enabled, this system will automatically sync the users and groups over to the other CARP host when changes are made.

Synchronize Certificates:
When this option is enabled, this system will automatically sync the Certificate Authorities, Certificates, and Certificate Revocation Lists over to the other CARP host when changes are made.

Synchronize rules:
When this option is enabled, this system will automatically sync the firewall rules to the other CARP host when changes are made.

Synchronize Firewall Schedules:
When this option is enabled, this system will automatically sync the firewall schedules to the other CARP host when changes are made.

Synchronize aliases:
When this option is enabled, this system will automatically sync the aliases over to the other CARP host when changes are made.

Synchronize NAT:

Synchronize Wake on LAN:
When this option is enabled, this system will automatically sync the WoL configuration to the other CARP host when changes are made.

Synchronize Static Routes:
When this option is enabled, this system will automatically sync the Static Route configuration to the other CARP host when changes are made.

Synchronize Load Balancer:
When this option is enabled, this system will automatically sync the Load Balancer configuration to the other CARP host when changes are made.

Synchronize Virtual IPs:
When this option is enabled, this system will automatically sync the CARP Virtual IPs to the other CARP host when changes are made.

Figura 5. 34 Configuración de CARP Setting MASTER

Como se ve en la figura 5.34, se habilitan algunas opciones de sincronización que se transmitirán a través de CARP entre los servidores Firewall. Además, se debe indicar los datos del servidor de destino que en este caso es la IP del Servidor SLAVE, y el password de administración del mismo.

10. Luego se realiza lo mismo para el servidor SLAVE, con la diferencia de que en este solo se configura la IP de destino y el password para acceder al MASTER.

Services: CARP Settings: Edit

Virtual IPs CARP Settings

State Synchronization Settings (pfsync)

Synchronize States

pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.

This setting should be enabled on all members of a failover group.

NOTE: Clicking save will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface

If Synchronize States is enabled, it will utilize this interface for communication.

NOTE: We recommend setting this to a interface other than LAN! A dedicated interface works the best.

NOTE: You must define a IP on each machine participating in this failover group.

NOTE: You must have an IP assigned to the interface on any participating sync nodes.

pfsync Synchronize Peer IP

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP

Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

NOTE: XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!

NOTE: Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username

Enter the webConfigurator username of the system entered above for synchronizing your configuration.

NOTE: Do not use the Synchronize Config to IP and username option on backup cluster members!

Synchronize Users and Groups

When this option is enabled, this system will automatically sync the users and groups over to the other CARP host when changes are made.

Synchronize Certificates

When this option is enabled, this system will automatically sync the Certificate Authorities, Certificates, and Certificate Revocation Lists over to the other CARP host when changes are made.

Synchronize rules

When this option is enabled, this system will automatically sync the firewall rules to the other CARP host when changes are made.

Synchronize Firewall Schedules

When this option is enabled, this system will automatically sync the firewall schedules to the other CARP host when changes are made.

Synchronize aliases

When this option is enabled, this system will automatically sync the aliases over to the other CARP host when changes are made.

Synchronize NAT

When this option is enabled, this system will automatically sync the NAT rules over to the other CARP host when changes are made.

Synchronize IPsec

When this option is enabled, this system will automatically sync the IPsec configuration to the other CARP host when changes are made.

Synchronize OpenVPN

When this option is enabled, this system will automatically sync the OpenVPN configuration to the other CARP host when changes are made. Using this option implies "Synchronize Certificates" as they are required for OpenVPN.

Synchronize DHCPD

When this option is enabled, this system will automatically sync the DHCP Server settings over to the other carp host when changes are made.

Synchronize Wake on LAN

Figura 5. 35 Configuración de CARP Setting SLAVE

11. Una vez terminada esta configuración, se la debe comprobar ingresando al menú Status -> CARP Failover; y se observa que las interfaces CARP se encuentran marcadas como MASTER en el servidor principal MASTER; y como BACKUP en el servidor secundario SLAVE.

Status: CARP

CARP Interface	Virtual IP	Status
vip100	172.168.10.15	MASTER
vip1	10.1.29.10	MASTER
vip3	10.0.0.4	MASTER

Note:
You can configure CARP settings here.

pfSync nodes:

```
1cee961f
7a8ee11f
d0b059fe
d9ae7ed7
```

Figura 5. 36 Status de Configuración de CARP en MASTER

Status: CARP

CARP Interface	Virtual IP	Status
vip100	172.168.10.15	BACKUP
vip1	10.1.29.10	BACKUP
vip3	10.0.0.4	BACKUP

Note:
You can configure CARP settings here.

pfSync nodes:

```
1cee961f
60b5311e
7a8ee11f
d0b059fe
d9ae7ed7
```

Figura 5. 37 Status de Configuración de CARP en SLAVE

5.1.3 Implementación de la SOLUCION C: Redistribución de Recursos de la Nube

En el capítulo 3, se determinó como vulnerabilidad la manera en que se encontraban distribuidos los elementos de la nube, es decir, la posición del servidor de almacenamiento externo FreeNAS. Este servidor contiene un espejo de todas las máquinas virtuales, para así garantizar alta disponibilidad de las mismas; era necesario que este se encuentre en una zona segura, que en el caso de la nube es la zona desmilitarizada DMZ.

Por lo tanto, para poder tener el servidor físico dentro de esta zona que contiene los servidores virtualizados, el plan de diseño propuesto indica que se deben crear dos vlan's en el servidor XCP para que por medio de la interfaz física Eth1 del mismo, puedan salir la red LAN hacia los usuarios, como también la red DMZ para conectar el servidor de almacenamiento FreeNAS a la DMZ.

Para realizar esta configuración se lo puede realizar mediante comandos o a su vez mediante la configuración manual por medio del entorno grafico XenCenter.

Desde la pestaña Networking, al igual que crear una nueva interfaz, se selecciona la opción de **External Network**, para poder configurarla como VLAN; tal como se observa en la figura 5.38.

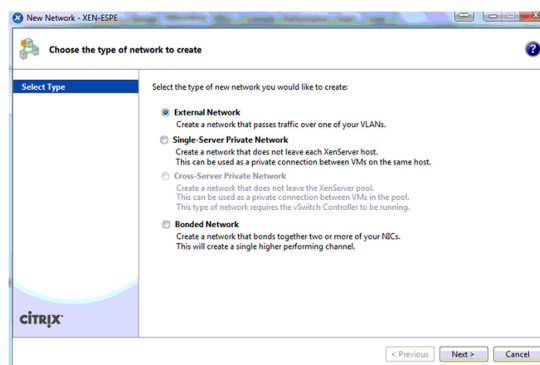


Figura 5. 38 Configuración de nueva Red en XCP

Luego, se coloca el nombre de la red y la tarjeta de red física a la cual se encuentra asociada, además del ID de la Vlan. Figura 5.39

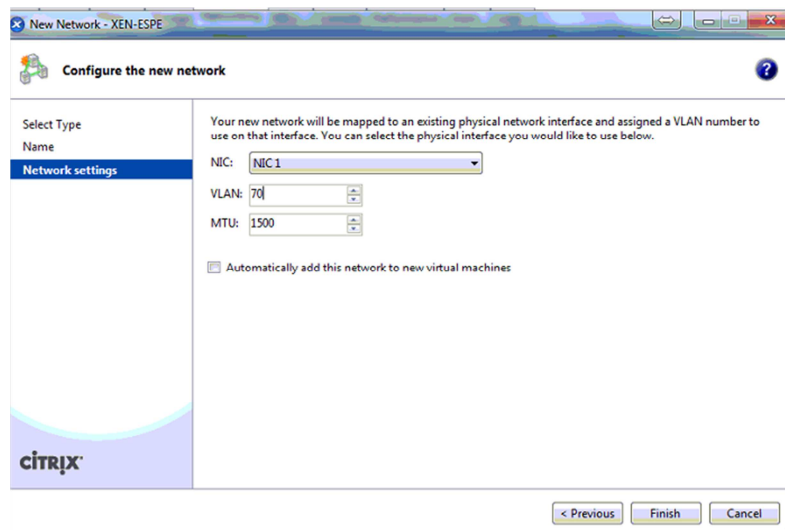


Figura 5. 39 Parámetros de VLAN

Esta configuración se la debe realizar una segunda vez para la creación de la VLAN LAN. Una vez creadas las dos VLANs se puede observar en la pestaña de **Networking** los cambios, tal como se observa en la figura 5.40.

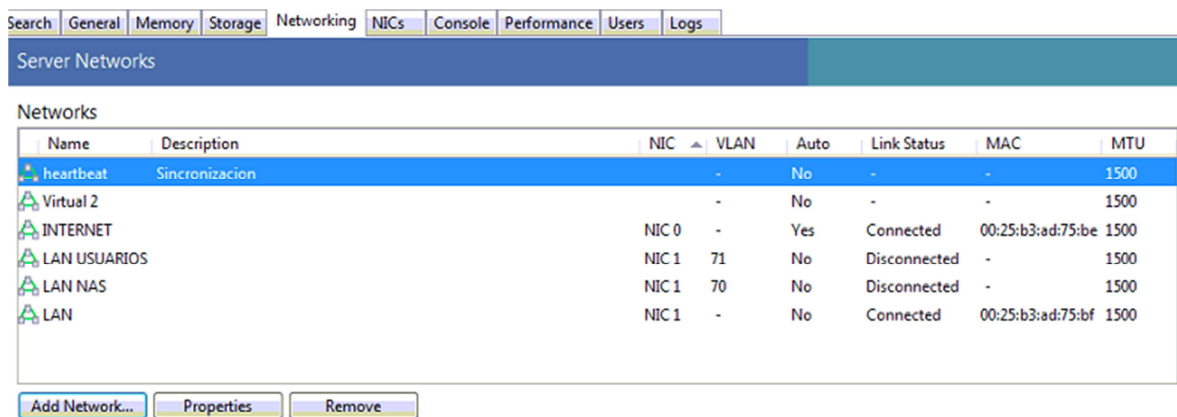


Figura 5. 40 VLAN's creadas (LAN y DMZ)

Una vez realizado esto, se procedió a configurar un switch 3Com, con los comandos básicos para la creación de las dos vlans. Figura 5.41.

```

COM5 - PuTTY
[4500]display interface
Aux2/0/0
Description : Aux Interface
Ethernet2/0/1 current state : UP
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware
Media type is twisted pair, loopback not set
Port hardware type is 100_BASE_TX
100Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is
Flow-control is not enabled
The Maximum Frame Length is 9216
Broadcast MAX-pps: 3000
Unicast MAX-ratio: 100%
Multicast MAX-ratio: 100%
Allow jumbo frame to pass
PVID: 70
Mdi type: auto
Port link-type: access
Tagged VLAN ID : none
Untagged VLAN ID : 70

COM5 - PuTTY
Ethernet2/0/2 current state : UP
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware
Media type is twisted pair, loopback not set
Port hardware type is 100_BASE_TX
100Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type
Flow-control is not enabled
The Maximum Frame Length is 9216
Broadcast MAX-pps: 3000
Unicast MAX-ratio: 100%
Multicast MAX-ratio: 100%
Allow jumbo frame to pass
PVID: 71
Mdi type: auto
Port link-type: access
Tagged VLAN ID : none
Untagged VLAN ID : 71

COM5 - PuTTY
Ethernet2/0/3 current state : UP
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address
Media type is twisted pair, loopback not set
Port hardware type is 100_BASE_TX
100Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autone
Flow-control is not enabled
The Maximum Frame Length is 9216
Broadcast MAX-pps: 3000
Unicast MAX-ratio: 100%
Multicast MAX-ratio: 100%
Allow jumbo frame to pass
PVID: 1
Mdi type: auto
Port link-type: trunk
VLAN passing : 1(default vlan), 70-71
VLAN permitted: 1(default vlan), 2-4094
Trunk port encapsulation: IEEE 802.1q
Last 300 seconds input: 0 packets/sec 198 bytes/sec
Last 300 seconds output: 1 packets/sec 158 bytes/sec
Input(total): 706 packets, 251549 bytes
567 broadcasts, 139 multicasts, 0 pauses
Input(normal): - packets, - bytes
- broadcasts, - multicasts, - pauses
  
```

Figura 5. 41 VLAN's creadas Switch 3Com

Posteriormente, se procedió a reconfigurar los firewalls PFSense con las nuevas interfaces Vlan creadas en el servidor XCP, ya que el firewall permite que exista comunicación desde el servidor hacia la red LAN y DMZ, fue necesario también crear las vlans en este para que funcione como switch en la red virtual.

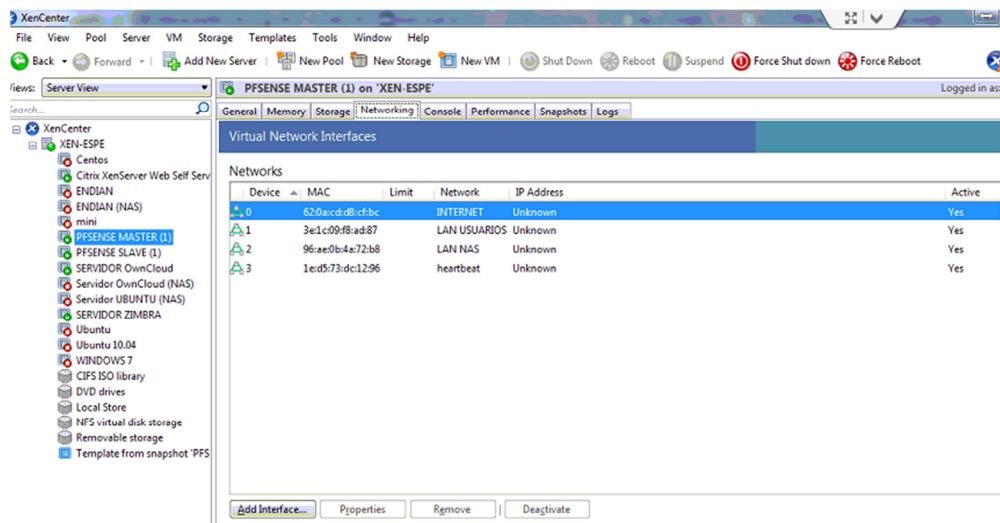


Figura 5. 42 Nuevas interfaces asignadas a PFSense

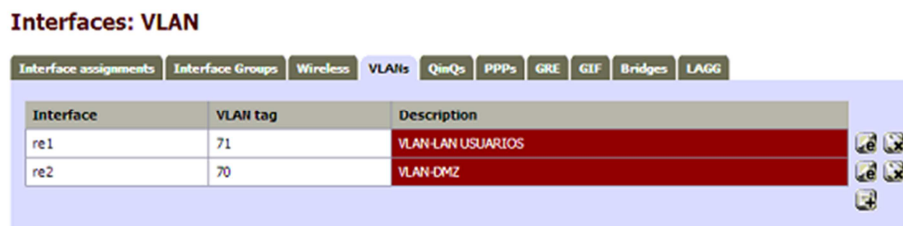


Figura 5. 43 VLAN's creadas en PFSense

Una vez que se comprobó la creación de las vlans, se procedió a cambiar la configuración de la IP del servidor FreeNAS, para poderlo introducir como parte de la red de servidores DMZ. Figura 5.44

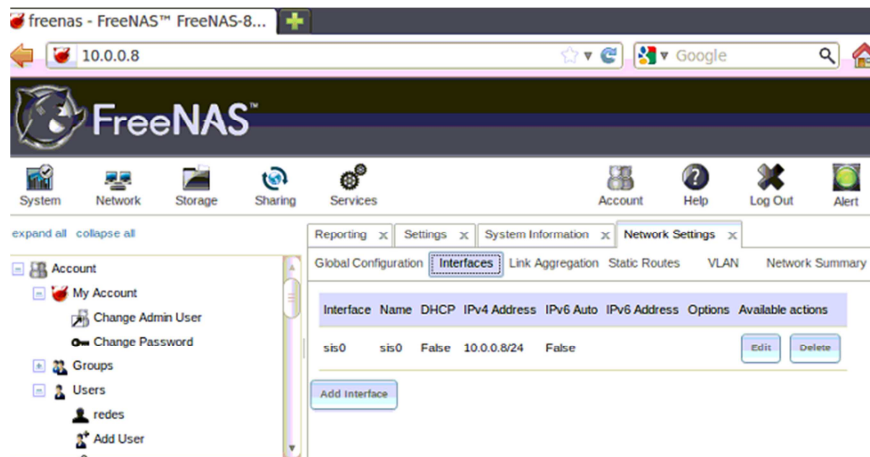


Figura 5. 44 Configuración IP FreeNAS

Adicionalmente, para que sirva la conexión entre el servidor XCP con la LAN y DMZ, fue necesario configurar dos rutas estáticas en el servidor XCP y dos rutas estáticas en el servidor FreeNAS, además de que en este fue necesario adicionar la IP del servidor XCP, de los servidores de la DMZ; para que este pueda tener comunicación con el servidor NAS. Ya que sin estas configuraciones no se podía tener comunicación entre los distintos servidores.

Como se puede apreciar en las figuras 5.45, 5.46 y 5.47.

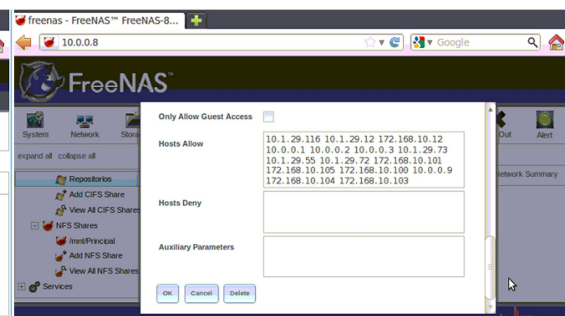
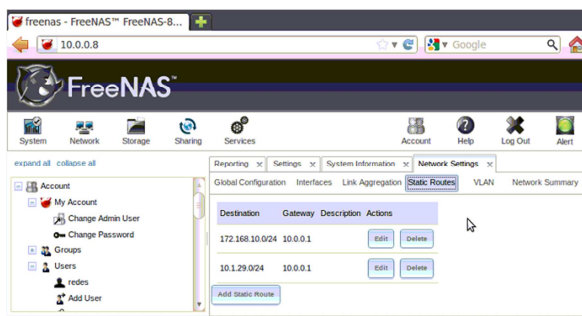
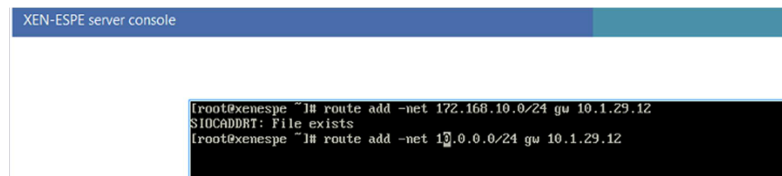


Figura 5. 45 Configuración de rutas estáticas Figura 5. 46 Ingreso de IP's permitidas



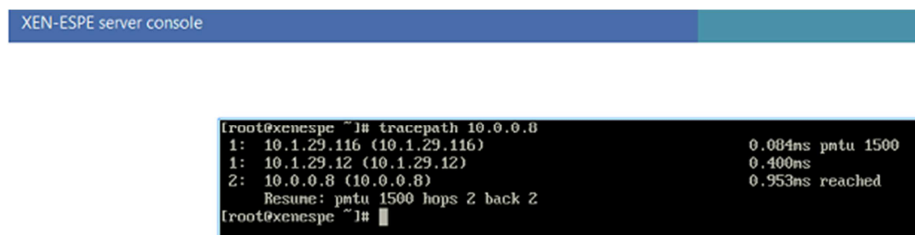
```
XEN-ESPE server console

[root@xenespe ~]# route add -net 172.168.10.0/24 gw 10.1.29.12
SIOCADDRT: File exists
[root@xenespe ~]# route add -net 10.0.0.0/24 gw 10.1.29.12
```

Figura 5. 47 Configuración de rutas estáticas en XCP

Como se puede observar en la figura 5.47, las rutas estáticas configuradas permiten que todos los paquetes de datos que vayan hacia la red 172.168.10.0 y hacia la red 10.0.0.0 con máscara de 24, salgan por la IP 10.1.29.12 que es la interfaz WAN del PFSense.

Una vez terminadas estas configuraciones se puede comprobar que existe comunicación entre el servidor XCP con el servidor NAS, realizando pruebas con el comando ping, y añadiendo los Storage Repositories en el servidor pero esta vez con la nueva dirección del servidor FreeNAS. Tal como se observa en las figuras 5.48, 5.49.



```
XEN-ESPE server console

[root@xenespe ~]# tracepath 10.0.0.8
  1:  10.1.29.116 (10.1.29.116)          0.004ms pmtu 1500
  1:  10.1.29.12 (10.1.29.12)           0.400ms
  2:  10.0.0.8 (10.0.0.8)               0.953ms reached
    Resume: pmtu 1500 hops 2 back 2
[root@xenespe ~]#
```

Figura 5. 48 Pruebas de conectividad entre XCP y FreeNAS

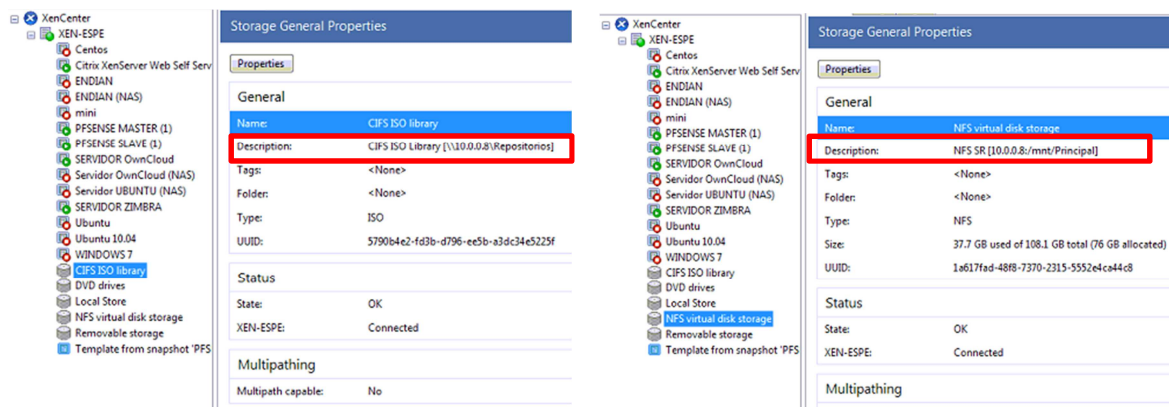


Figura 5. 49 Almacenamiento CIFS y NFS de FreeNAS en XCP

Además de estas soluciones de seguridad para IAAS, es importante cumplir con otros aspectos que hacen parte de la seguridad de la infraestructura; por lo tanto, se debe:

- Cumplir con un plan de mantenimiento (actualizaciones) de los servidores, a nivel de hardware como de software.

Actualización de la Plataforma XCP:

La versión de la plataforma del hipervisor es la 5.6 de XCP, misma que se detalla en la figura 4.41.

	XCP 1.0	XCP 1.1	XCP 1.5	XCP 1.6
Initial Release	March 2011	October 2011	February 2012 (beta only)	November 2012
Corresponding XS release	5.6 FP1 ↗	5.6 SP2 ↗	6.0 ↗	6.1 ↗
Dependencies				
Xen version	?	Xen 3.4.2	Xen 4.1.0	Xen 4.1.3
CentOS	5.x?	CentOS 5.x? (Linux kernel v2.6.32)	5.6 (Linux kernel v2.6.32)	5.7 (Linux kernel v2.6.32.43)
Open vSwitch	?	?	?	1.4.2
Limits (besides those listed for Xen)				
Configuration Limits				1.6 limits ↗
Feature				
IntelliCache	✓	✓	✓	✓
Resilient distributed management architecture	✓	✓	✓	✓
VM disk snapshot and revert	✓	✓	✓	✓
XenCenter management	✓ ¹⁾	✓ ¹⁾	✓ ¹⁾	✓
Conversion tools	✓	✓	✓	✓
Heterogeneous pools	✓	✓	✓	✓
Dynamic Memory Control	✓	✓	✓	✓
Performance alerting and reporting	✓	✓	✓	✓
Host power management	✓	✓	✓	✓
Live memory snapshot and revert	✓	✓	✓	✓
Web self-service with delegated admin ²⁾	✓	✓	✓	✓
Site recovery	✓	✓	✓	✓
Open vSwitch	✓	✓	✓ (default)	✓ (default)
GPU Pass-Through			✓	✓

Figura 5. 50 Características de la versión de XCP instalada [25]

Como se observa en la figura 5.50, esta versión es del año 2011 y contiene ciertas características a diferencia de las versiones más recientes.

Debido a que XCP es una versión Open Source, no se corre el riesgo de que la licencia instalada pueda llegar a vencer; por lo que a diferencia de otras plataformas de virtualización, no hace falta la actualización de la versión.

Si se quisiera tener las características de las otras versiones, se debería instalar la nueva versión en un servidor de backup, cargar una copia de las máquinas virtuales del servidor principal y luego probar su funcionamiento. Como se puede observar, esto implica un trabajo extra y sería necesario únicamente si se requirieran las características de las otras versiones en caso de que se quiera escalar la nube y brindar muchos más servicios como IPV6, NIC BONDING⁵⁵, templates adicionales, etc.

⁵⁵ **NIC BONDING:** Es un término utilizado para ampliar el ancho de banda disponible de una interfaz de red. Especialmente utilizado por el módulo Kernel de Linux , para que múltiples usuarios puedan unirse a varias interfaces de red por un mismo canal.

A pesar de esto, los administradores de la plataforma de la nube deben cumplir con un plan de actualizaciones de la consola de gestión XenCenter y de los pluggins que vienen en ella; mismos que se actualizan cada cierto tiempo en la página oficial de Citrix. [26]

Lastimosamente, XCP viene con un error en las versiones actuales, desde 2011, y que debe ser corregido por Citrix para las versiones futuras, este error aparecerá en la consola de administración, que en este caso es XenCenter. Después de 30 días de la instalación de XCP aparecerá un mensaje de versión vencida; por lo que es necesario actualizar la versión

Para actualizar la versión de XCP se debe hacer lo siguiente:

1. Desde la consola Shell de XCP se debe detener el servicio XAPI, con el siguiente comando:

```
/ Etc / init.d / xapi parada
```

2. Luego se edita el siguiente archivo:

```
/ var / xapi / state.db
```

3. En el archivo se debe buscar el campo:

```
('caducidad' '20130110T00: 00:00 Z ' )
```

4. A este campo se lo modifica para que se lea por 30 días o más:

```
('caducidad' '20130210T00: 00:00 Z ' )
```

5. Una vez realizado esto se debe reiniciar el servicio XAPI:

```
/ Etc / init.d / xapi inicio
```

Por lo tanto, se debe realizar esta tarea cada 30 días al igual que la actualización de los pluggins de XenCenter.

Actualización de Consola de Gestión XenCenter:

La plataforma XCP puede ser gestionada desde una consola de administración de Citrix XenServer en la cual el administrador puede manipular la plataforma y sus máquinas virtuales.

XenServer cuenta con diferentes versiones de XenCenter, pero solo una es OpenSource y no brinda todas las características que las demás versiones.

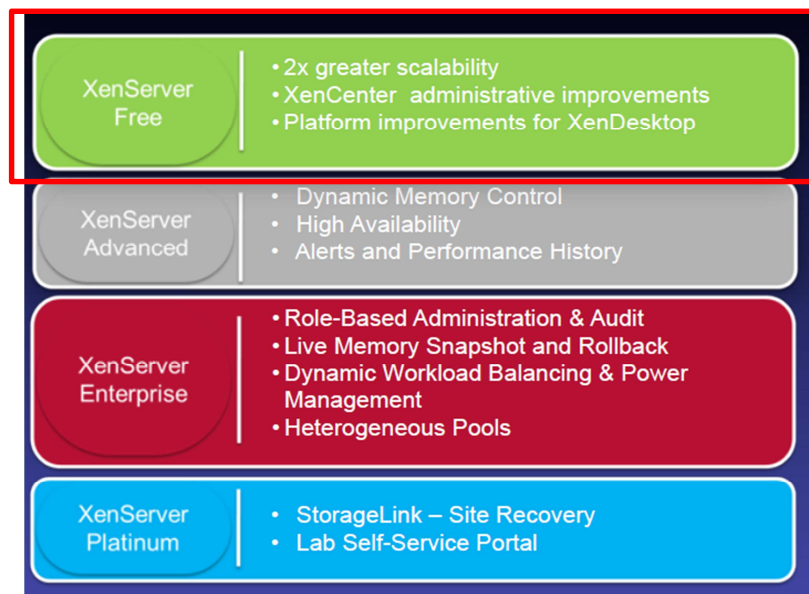


Figura 5. 51 Características de las versiones de XenCenter

Por lo tanto, la versión que se utilizara para gestionar la plataforma y las máquinas virtuales será XenServer Free.

Los costos de las diferentes versiones de XenCenter son las siguientes:

	Feature	Free	Advanced	Enterprise	Platinum
Free virtual infrastructure	XenServer hypervisor	✓	✓	✓	✓
	XenMotion® live migration	✓	✓	✓	✓
	VM Disk Snapshot and Revert	✓	✓	✓	✓
	XenCenter multi-server management	✓	✓	✓	✓
	Resilient distributed management architecture	✓	✓	✓	✓
	Conversion tools	✓	✓	✓	✓
Advanced management and automation	High availability		✓	✓	✓
	Memory optimization		✓	✓	✓
	Performance alerting and reporting		✓	✓	✓
	Automated workload balancing			✓	✓
	Heterogeneous pools			✓	✓
	Host power management			✓	✓
	Provisioning services (virtual)			✓	✓
	Role-based administration			✓	✓
	Live memory snapshots and reverts			✓	✓
	Citrix® StorageLink™			✓	✓
	Lifecycle management				✓
	Provisioning services (physical)				✓
	Site recovery				✓
	Cost per server	Free	\$1,000	\$2,500	\$5,000

Figura 5. 52 Características y costos de las versiones de XenCenter [27]

A pesar de utilizar una versión gratuita de XenCenter, es importante realizar actualizaciones cada 30 días al igual que XCP; siguiendo pasos a continuación:

1. Bajar la actualización de XenCenter de la página oficial de Citrix:
http://updates.xensource.com/XenServer/5.0.0/XenCenter?pool_5.0.0=0
2. Desde la consola de XenCenter, en la pestaña **Tools**, se selecciona la opción **Check for Updates**; misma que muestra una lista de los Updates disponibles descargados.
3. Seleccionar el update para la version de XenCenter instalada. Pulsar en el botón de **Assing Licence**.
4. Se especifica la versión de XenCenter instalada y seleccionar **OK**.

5. Finalmente, la licencia se actualiza y para comprobar este efecto, se debe reiniciar la consola de gestión de XenCenter.

Adicionalmente, es importante verificar que las configuraciones de **Updates Automáticos** del Snort y HAVP se generen en el tiempo especificado el momento en que se realizaron las configuraciones respectivas en cada uno.

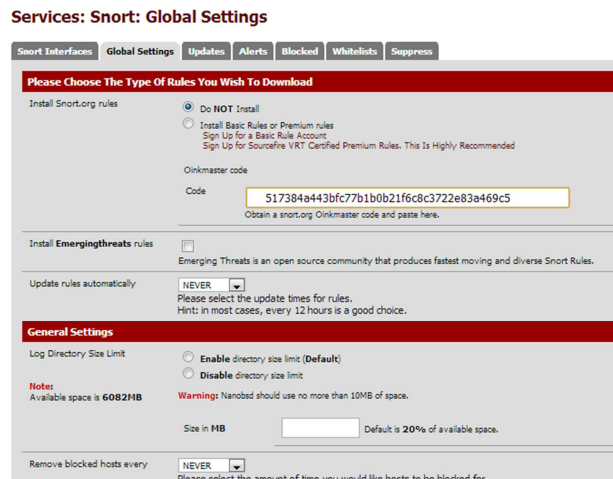
5.2 IMPLEMENTACIÓN DE CLOUD SECURITY EN PAAS

5.2.1 Implementación de la SOLUCIÓN A

Como se indicó en el capítulo 4 el firewall PFSense permite la instalación de paquetes adicionales, por lo que se instaló un IDS (Intrusion Detection System) llamado SNORT, para que monitoree y detecte intrusiones en la red, específicamente las interfaces WAN y LAN.

Por lo tanto, los pasos que se siguieron para su instalación y configuración son los siguientes:

1. Descarga e instalación del paquete SNORT.
2. Una vez instalado, se deben configurar los aspectos generales del IDS para su funcionamiento. Por lo que se debe empezar por descargar e instalar las reglas propias de SNORT para que pueda funcionar; para ello, se debe crear una cuenta en el sitio oficial de SNORT [33], y solicitar el código Oinkcode.



Services: Snort: Update Rules



Figura 5. 53 Código Oinkcode. Actualización de reglas

- Una vez instaladas y actualizadas las reglas, se debe configurar las interfaces a monitorear.

Services: Snort 2.9.2.3 pkg v. 2.5.4

	If	Snort	Performance	Block	Barnyard2	Description
<input type="checkbox"/>	WAN	ENABLED	AC-BNFA	ENABLED	DISABLED	MONITOREO INTERFACE WAN
<input type="checkbox"/>	LAN	ENABLED	AC-BNFA	ENABLED	DISABLED	MONITOREO INTERFACE LAN

Figura 5. 54 Configuración de interfaces a monitorear

- En cada interfaz se debe especificar las reglas que se activaran para el monitoreo, intervalo de actualizaciones de las reglas, el tipo de log generado en cada inspección; además, se debe activar el uso de HTTP

para realizar el monitoreo de la interfaz, se habilita la opción de habilitar escaneo. Y, se inician cada una de las interfaces configuradas.

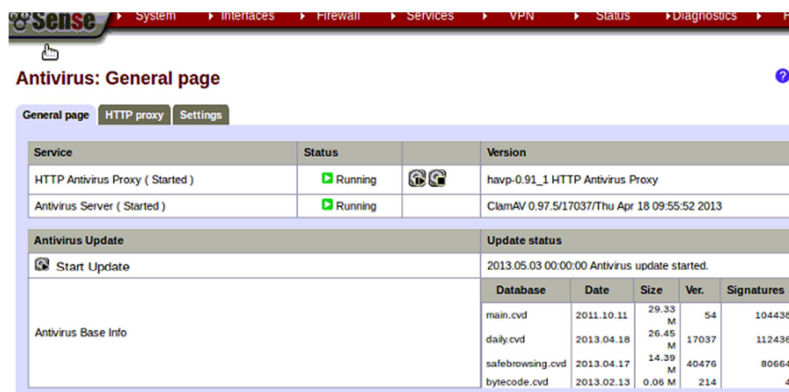
5. Finalmente, desde la pestaña de **Status**, seleccionar **Services**, se puede comprobar que el servicio de SNORT este activado.

5.2.2 Implementación de la SOLUCIÓN B

Como segunda solución se instaló HAVP (HTTP Proxy Antivirus), que tiene como misión actuar como filtro perimetral en un entorno determinado, es decir, se encuentra ubicado entre el punto de salida de una red privada y el punto de entrada a una red pública, que permite detectar y bloquear ataques externos hacia la red LAN. Además, cuenta con un anti virus llamado ClamAV, que escanea el tráfico de la red, detectando código malicioso en navegación HTTP.

Para colocarlo en funcionamiento se realizó lo siguiente:

1. Descarga e instalación del paquete HAVP desde PFSense.
2. Configuración y puesta en marcha de HAVP.



Service	Status	Version
HTTP Antivirus Proxy (Started)	Running	havp-0.91_1 HTTP Antivirus Proxy
Antivirus Server (Started)	Running	ClamAV 0.97.5/17037/Thu Apr 18 09:55:52 2013

Database	Date	Size	Ver.	Signatures
main.cvd	2011.10.11	29.33 M	54	104438
daily.cvd	2013.04.18	26.45 M	17037	1124366
safebrowsing.cvd	2013.04.17	14.39 M	40476	80664
bytecode.cvd	2013.02.13	0.06 M	214	41

Figura 5. 55 Configuración de HAVP

- Adicionalmente, en la pestaña de **HTTP Proxy**, se debe configurar la opción de proxy transparente para la red LAN, y en **Settings**, la opción de actualizar el antivirus cada 24 horas y que por cada detección, genere un Log.

Antivirus: HTTP proxy (havg + clamav)

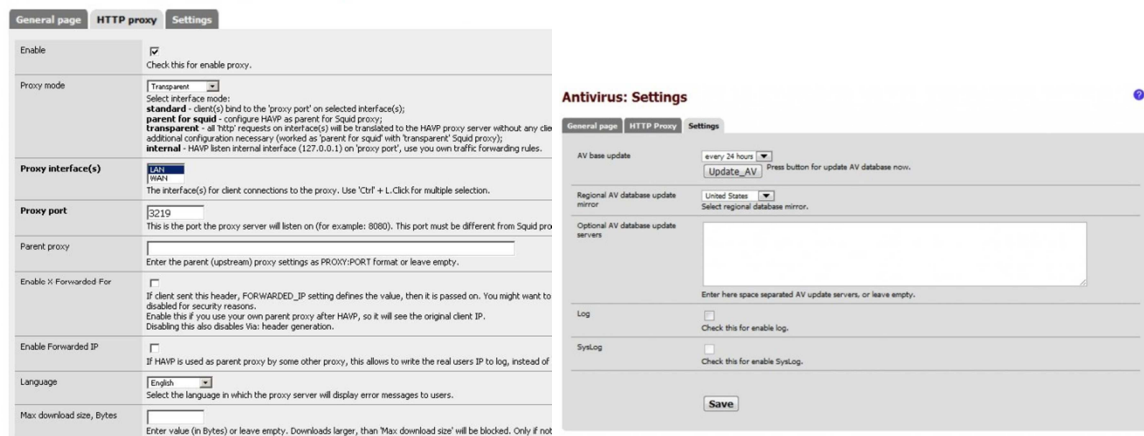


Figura 5. 56 Configuración de proxy y actualizaciones

- Para comprobar el funcionamiento de este paquete, desde la LAN, se intentó acceder a una página web para descargar un archivo de prueba de virus EICAR. [34]

```

C:\Windows\system32\cmd.exe
Configuración IP de Windows

Adaptador de LAN inalámbrica Conexión de red inalámbrica:
Estado de los medios . . . . . : medios desconectados
Sufijo DNS específico para la conexión . . : espe.int

Adaptador de Ethernet Conexión de área local:
Sufijo DNS específico para la conexión . . :
Vínculo dirección IPv6 local . . . : fe80::4434:ef09:8de1:2083::10
Dirección IPv4 . . . . . : 172.168.10.105
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 172.168.10.12

```

Figura 5. 57 IP de PC conectada a la LAN



Figura 5. 58 Bloqueo de página con virus por HAVP



Figura 5. 59 Lista de virus detectados por HAVP

5. Además de bloquear páginas con virus, se realizó una prueba cuando se requiere acceder a OwnCloud o Zimbra y estos servidores se encuentran inactivos; HAVP también muestra una pantalla con este error al tratar de ingresar a cualquiera de estos servicios.



Figura 5. 60 Prueba hacia IP de Zimbra

5.2.3 Implementación de la SOLUCIÓN C

Para gestionar la asignación de recursos y máquinas virtuales a usuarios PAAS de la nube, se procedió a cumplir con plan de gestión de usuarios, de la siguiente manera:

- A. Instalación de un servidor Windows Server 2008 con los servicios de DNS y Active Directory.

Cuando se instala XenCenter en una máquina para administrar el servidor XCP, este crea automáticamente una cuenta de super-usuario root para la administración y control total sobre el servidor; sin embargo, si se desea tener algunos administradores con distintos privilegios y roles de administración, XenCenter da la posibilidad de integrar usuarios configurados en Active Directory y asignarlos diferentes roles para administrar la nube XCP desde una consola XenCenter que se encuentre en red con el servidor.

Para implementar este servicio, se instaló en un servidor externo, Windows Server 2008, y se lo configuró con una IP estática dentro del rango Ip's que

proporciona el Switch del Datacenter de los Laboratorios del DEEE; tal como se detalla en la figura 4.4.

La figura 5.61 muestra la configuración de las zonas directa e inversa del DNS con los respectivos equipos configurados; entre ellos, la dirección del servidor XCP para poder gestionar diferentes tipos de usuarios administradores de la nube, basado en roles asignados.

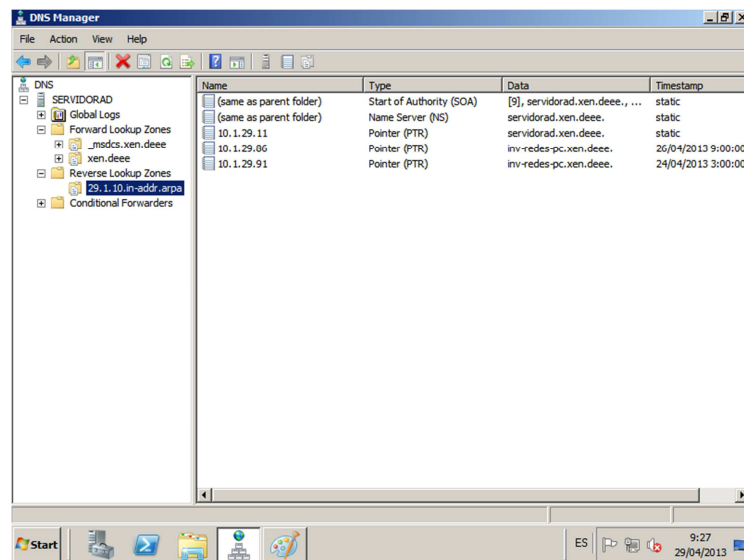


Figura 5. 61 Servidor DNS en Windows Server 2008

B. Manejo de usuarios desde Active Directory para establecer políticas de administración de los servicios de la nube desde XenCenter.

Para manejar incluir algunos usuarios administradores del servidor XCP en XenCenter, se crearon grupos y usuarios en Active directory, tal como se puede apreciar en las figuras 5.62 y 5.63.

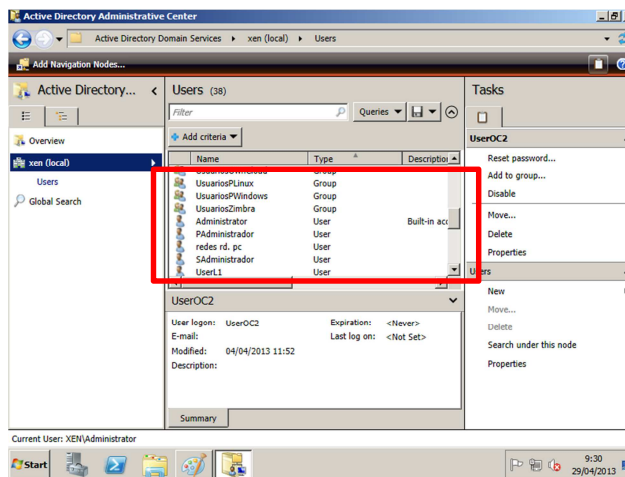


Figura 5. 62 Grupos Creados

En el recuadro rojo, se pueden observar los grupos creados, a los cuales se encuentran integrados los siguientes usuarios:

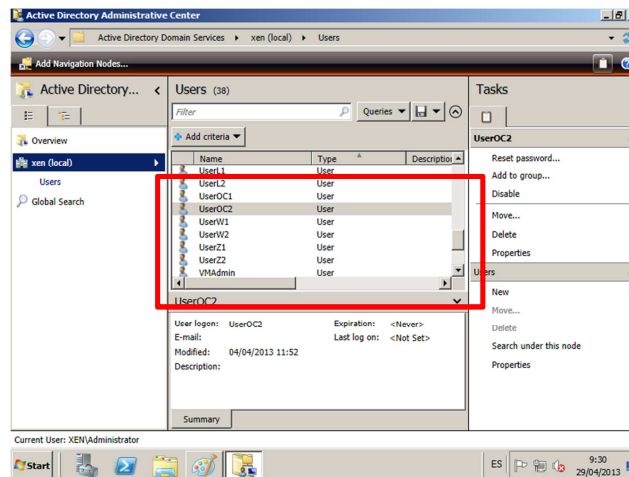


Figura 5. 63 Usuarios asignados a Grupos Creados

En la siguiente tabla se especifican los usuarios y los grupos a los cuales pertenecen, además de los roles asignados en XenCenter.

Tabla 5. 1 Usuarios y roles

N°	GRUPO	USUARIOS	ROL	CARACTERISTICAS
1	AdministradoresNube	PAdministrador	Pool Admin	Funciones iguales que administrador root. Puede administrar todas las características del servidor XCP.
		SAdministrador	Pool Operator	Puede hacer todo, como añadir / eliminar usuarios y modificar sus papeles. Este papel se centra principalmente en el host y el manejo de pools (creación de almacenamiento, pools, destion de usuarios, etc.)
		VMPowerAdmin	VM Power Admin	Crea y gestiona máquinas virtuales. Provisión de máquinas virtuales para uso de un operador de máquina virtual.
		VMAdmin	VM Admin	Iguals funciones que VM Power Admin, pero sin posibilidad de realizar snapshots en las máquinas virtuales.
		VMOperator	VM Operator	Similar a VM Administration, pero no puede crear / destruir máquinas virtuales, pero si detenerlas, reiniciarlas, apagarlas o encenderlas.
2	UsuariosOwnCloud	UserOC1	Read Only	Puede observar el pool donde se encuentra el servidor, sus recursos y los datos de rendimiento. Pero no puede realizar modificación alguna.
		UserOC2		
3	UsuariosZimbra	UserZ1		
		UserZ2		
4	UsuariosLinux	UserL1		
		UserL2		
5	UsuariosWindows	UserW1		
		UserW2		

Una vez especificado cada uno de los usuarios y sus roles, se procedió a atar al dominio XEN.DEEE el servidor XCP; se importaron los usuarios y se les asignaron roles de administración.

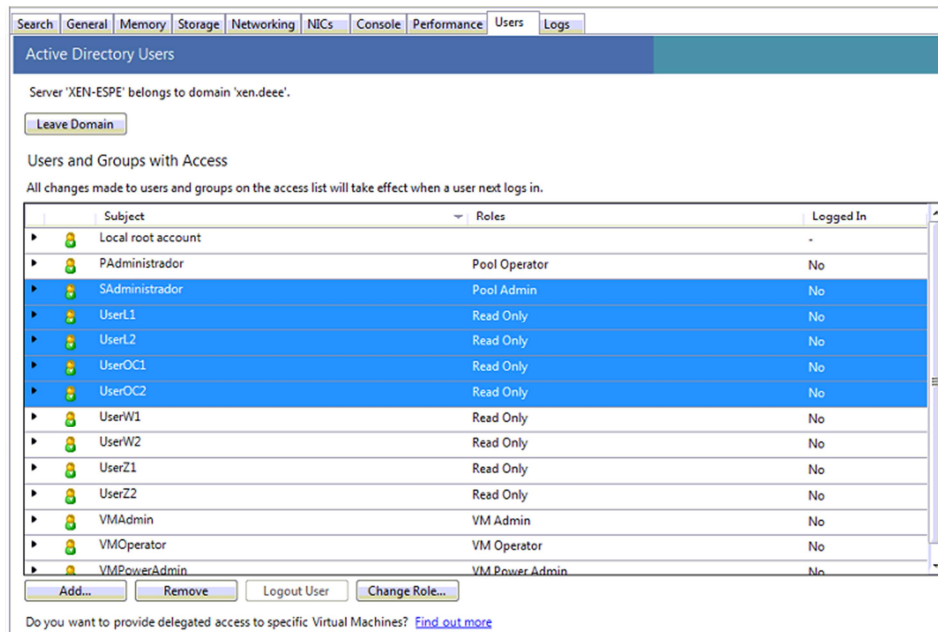


Figura 5. 64 Usuarios y roles en XenCenter

Para probar el funcionamiento del rol asignado a un usuario, se procedió a realizar la siguiente prueba:

Sobre el Servidor Xen – Espe, click derecho, seleccionar **Reconnect as**, con esto se terminará la sesión iniciada como root, y pedirá que se logee el nuevo usuario, por lo que al ingresar cualquiera de estos configurados, y tras intentar realizar modificaciones en la nube, en el caso de tener un rol de **Read Only**, saldrá un mensaje indicando que no posee permisos para realizar dicha acción.

- C. Instalación de una máquina virtual en XCP con el software de gestión Web Self Services para el manejo de las máquinas virtuales en caso de requerimiento de Plataforma como Servicio (PAAS).

XenCenter, al ser una herramienta de gestión de XenServer, brinda la posibilidad de instalar un appliance virtual como herramienta de gestión de para el manejo de las máquinas virtuales vía remota, según requerimientos de usuarios PAAS.

Para implementar este appliance se realizó lo siguiente:

1. Descarga desde el sitio oficial de Citrix, el appliance Web Self Service.
2. Instalación de WSS como una máquina virtual con los siguientes requerimientos.
 - 256MB de RAM
 - 1 GB de espacio en disco
 - Interfaz de red. (Conexión a red WAN)

```
NIT: Entering runlevel: 3
Entering non-interactive startup
Bringing up loopback interface: [ OK ]
Bringing up interface eth0: [ OK ]
Starting system logger: [ OK ]
Starting kernel logger: [ OK ]
Detecting Linux distribution version: [ OK ]
Starting xe daemon: [ OK ]
Starting Web Self Service:[ OK ]

CentOS release 5.5 (Final)
kernel 2.6.18-194.32.1.el5xen on an i686

webss login:

-----
Launch the web browser using the following URL(s):

https://10.1.29.100/
```

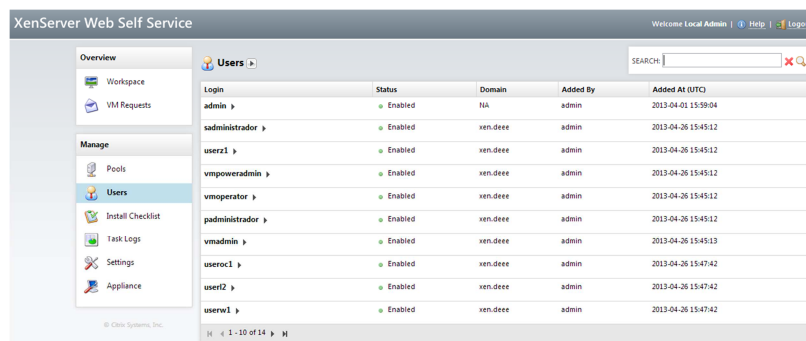
Figura 5. 65 Consola de WSS

Tal como se observa en la figura, se administra la consola desde la URL <https://10.1.29.100/>, tanto para los usuarios como para el administrador de la misma, que en este caso, se crea un Superadministrador por defecto root.

D. Pruebas de gestión de máquinas virtuales con los usuarios registrados en el Active Directory de Windows Server 2008.

Una vez instalado WSS, se puede acceder a el mediante la URL señalada, y se deben realizar las siguientes configuraciones:

1. Adición de Usuarios creados en el Active Directory.

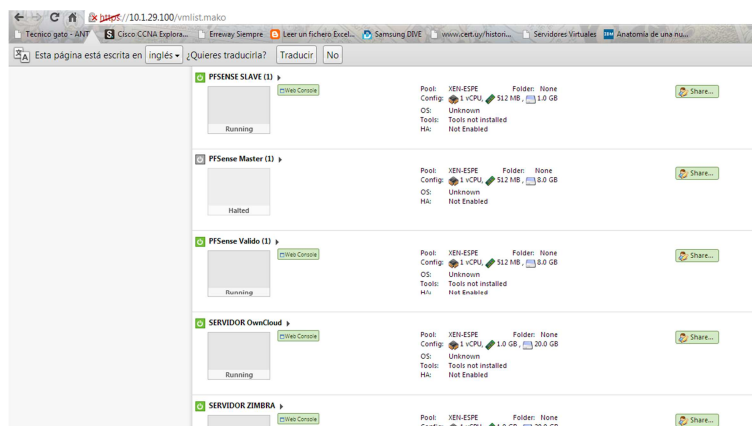


The screenshot shows the XenServer Web Self Service interface. The 'Users' section is active, displaying a table of users. The table has columns for Login, Status, Domain, Added By, and Added At (UTC). The users listed are:

Login	Status	Domain	Added By	Added At (UTC)
admin	Enabled	NA	admin	2013-04-01 15:59:04
sadministrador	Enabled	xen.deee	admin	2013-04-26 15:45:12
userz1	Enabled	xen.deee	admin	2013-04-26 15:45:12
vmpoweradmin	Enabled	xen.deee	admin	2013-04-26 15:45:12
vmoperator	Enabled	xen.deee	admin	2013-04-26 15:45:12
padministrador	Enabled	xen.deee	admin	2013-04-26 15:45:12
vmadmin	Enabled	xen.deee	admin	2013-04-26 15:45:13
useroc1	Enabled	xen.deee	admin	2013-04-26 15:47:42
userf2	Enabled	xen.deee	admin	2013-04-26 15:47:42
userw1	Enabled	xen.deee	admin	2013-04-26 15:47:42

Figura 5. 66 Usuarios de AD

2. Visualización de máquinas virtuales de XCP.



The screenshot shows the XenServer Web Self Service interface displaying a list of virtual machines. The table has columns for Name, Status, Pool, Config, Folder, OS, Tools, and HA. The VMs listed are:

Name	Status	Pool	Config	Folder	OS	Tools	HA
PFSense Slave (1)	Running	XEN_ESPE	1 vCPU, 512 MB, 1.0 GB	None	Unknown	Tools not installed	Not Enabled
PFSense Master (1)	Halted	XEN_ESPE	1 vCPU, 512 MB, 5.0 GB	None	Unknown	Tools not installed	Not Enabled
PFSense Valido (1)	Running	XEN_ESPE	1 vCPU, 512 MB, 5.0 GB	None	Unknown	Tools not installed	Not Enabled
SERVIDOR OwnCloud	Running	XEN_ESPE	1 vCPU, 1.0 GB, 20.0 GB	None	Unknown	Tools not installed	Not Enabled
SERVIDOR ZIMBRA	Running	XEN_ESPE	1 vCPU, 1.0 GB, 20.0 GB	None	Unknown	Tools not installed	Not Enabled

Figura 5. 67 Máquinas virtuales de XCP

- Para que un usuario PAAS pueda hacer un requerimiento o petición de una plataforma, debe logearse con su usuario, y mediante la herramienta de **VM Request** puede enviar a manera de mail un requerimiento específico al administrador de la plataforma, como se observa en la figura 5.68.

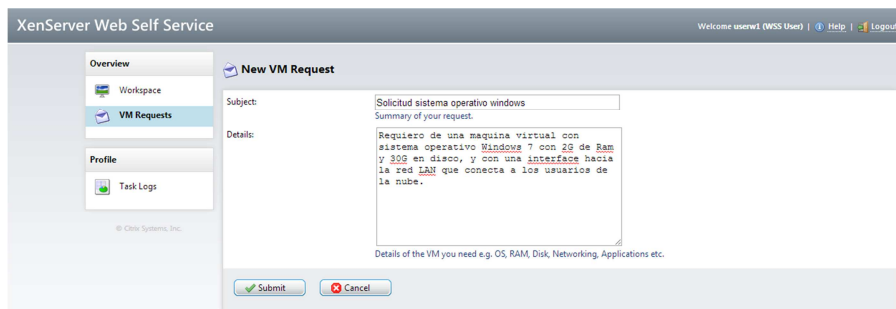
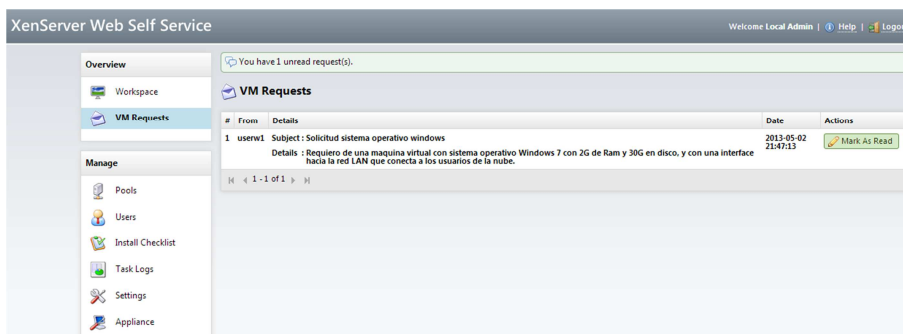


Figura 5. 68 Usuario UserW1 realizando una petición

Como se puede observar, el rol configurado para este usuario, limita su consola de gestión a realizar una petición para poder observar la plataforma o máquina virtual que requiera; y no le permite observar todo el contenido del servidor XCP

- Por otro lado, desde la consola del administrador, se puede observar este requerimiento, y este a su vez puede asignar la máquina virtual solicitada por este usuario.



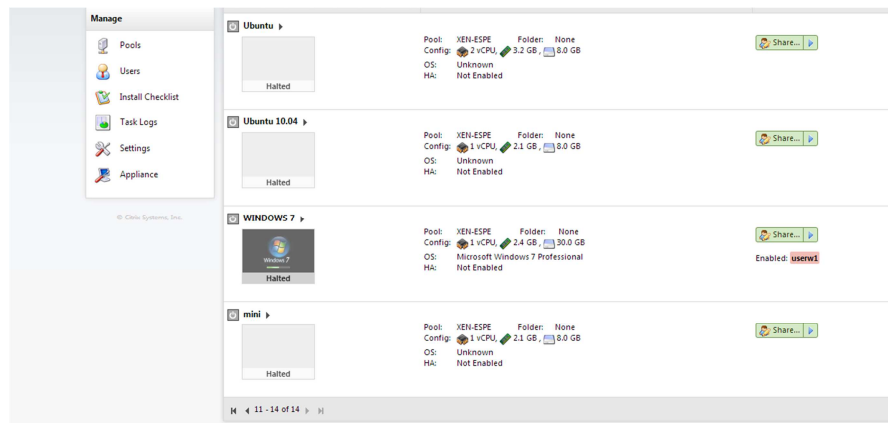


Figura 5. 69 Petición recibida por el administrador y asignación de requerimiento a Usuario

Como se puede observar, el administrador recibió el requerimiento de la plataforma por parte del usuario, y cumplió con asignarle el recurso solicitado.

5. Por otro lado, el usuario ya puede visualizar la plataforma que solicitó y manejarla de manera remota.

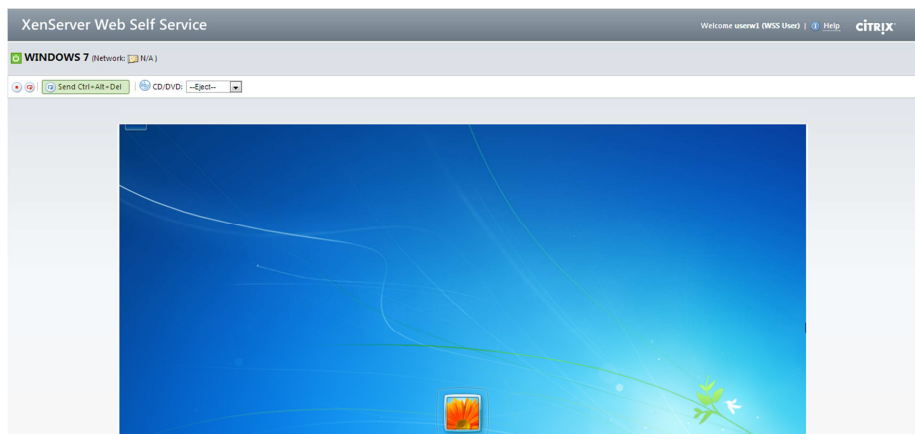


Figura 5. 70 Máquina virtual asignada a Usuario

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Cuando se tiene una nube de servicios Cloud Computing, es importante garantizar tanto del lado del proveedor como del cliente, esta cuenta con *Cloud Security*, a fin de garantizar la seguridad y la integridad de la información, de los sistemas y equipos que la conforman, para prevenir posibles intrusiones y ataques que pueda sufrir, ocasionando que la nube falle y colapsen sus servicios.
- La nube que se encontraba implementada en los laboratorios del DEEE, no brindaba Seguridad como Servicio, lo cual era un riesgo para el administrador y los usuarios de la misma; por lo tanto era indispensable dotarla de seguridad para cumplir con las normas básicas de seguridad establecidas para un sistema tecnológico que abarca información sensible y confidencial.
- Al realizar un análisis de la nube implementada en Xen Cloud Platform, se determinaron las vulnerabilidades a las que se encontraba expuesta, por lo tanto, los diseños y las implementaciones de las soluciones de Cloud Security; lograron proteger y resguardar todos los elementos sensibles que la componen; de tal manera que si algún intruso quisiese realizar un ataque

a los servicios o a las aplicaciones que ésta proporciona; no lograría obtener resultados positivos ya que las medidas de seguridad implementadas como alta disponibilidad de un Firewall, detección de intrusos, antivirus, manejo y autenticación de usuarios, etc., funcionan correctamente de tal manera que los usuarios de la nube tengan la seguridad de que sus datos están protegidos.

- La nube implementada, brinda servicios como plataforma, aplicaciones, software, capacidad de almacenamiento y seguridad; por lo tanto es importante llevar un control del estado de la plataforma y de los usuarios que tengan acceso a los diferentes servicios, ya que Cloud Security comprende también llevar un control y seguimiento del uso de la nube y de sus usuarios por parte del administrador de la nube.
- En el mercado existen diferentes equipos y software de distribución libre que brindan la posibilidad de implementarlos como soluciones de seguridad en diferentes entornos. La nube implementada está constituida en su mayoría, por software de distribución libre que funcionan sin ningún inconveniente, a pesar de que algunos de ellos no cuentan con requerimientos específicos que si poseen las versiones pagadas.
- *Cloud Computing* es una buena opción para implementar como solución en pequeñas y grandes empresas que manipulan información sensible, ya que ofrece ventajas como reducción de costos, alta disponibilidad de servicios y aplicaciones. Siempre y cuando el usuario o cliente de los servicios Cloud se cercioren de que su proveedor cumpla con los requisitos y políticas de seguridad.

6.2 RECOMENDACIONES

- Es necesario readecuar el cuarto de equipos en donde se encuentran los servidores de la nube ya que bajo las condiciones actuales no se encuentran dotados de toda la seguridad física que debería tener un datacenter para evitar riesgos como robo de equipos físicos e información, daños por desastres naturales, fallas eléctricas, etc.
- Se debe cumplir con un plan de actualizaciones de actualizaciones en todos los servidores y aplicaciones que conforman la nube, ya que una medida de seguridad mantener las plataformas actualizadas para garantizar su correcto funcionamiento, desempeño y funciones que cumplan para brindar servicios a los usuarios.
- Si los requerimientos de la nube aumentan debido a la demanda por parte de los usuarios, se debe considerar la opción de realizar un diseño para implementar alta disponibilidad en los servidores físicos, y un plan de adquisición de equipos nuevos para escalar la nube a un nivel más seguro y con mayor capacidad; ya que bajo las condiciones actuales no fue posible realizar esta implementación; por lo tanto no se tiene una alta disponibilidad del hipervisor, sino únicamente de las máquinas virtuales que lo conforman.

REFERENCIAS BIBLIOGRÁFICAS

- [A] Matiz N. (2013). *Implementación de Cloud Security para un sistema basado en Xen Cloud Platform*. Tesis. Escuela Politécnica del Ejército.
- [1] VMWare. (2012). Recuperado en Octubre de 2012, de <http://www.vmware.com/es/cloud-computing/>
- [2] Castellón, A. (2010, Mayo 27). *Cosas de Tecnología*. Recuperado en Octubre de 2012, de <http://www.tecnocosas.es/que-cloud-computing/>
- [3] Anónimo. (11 de Septiembre de 2012). *Wikipedia*. Recuperado en Octubre de 2012, de http://en.wikipedia.org/wiki/Cloud_computing_security
- [4] Pérez, P., Gutierrez, C., & fuente, S. d. (Octubre de 2001). *Inteco*. Recuperado en Octubre de 2012, de https://www.inteco.es/file/3LeSufa2tYmC_bcRKSfFbg
- [5] Amazon. (Noviembre de 2012). Recuperado en Noviembre de 2012, de <http://aws.amazon.com/es/ec2/>
- [6] (NIST Cloud Computing Normas Hojas de Ruta, 2011), NIST Special Publication 500 a 291. Recuperado en Noviembre de 2012, de http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024
- [7] INTECO-CERT. (Marzo de 2011). Recuperado en Noviembre de 2012, de *Riesgos y Amenazas en Cloud Computing*: http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

- [8] *Alcocer, A.* (10 de Junio de 2012). Recuperado en Noviembre de 2012, de <http://www.societic.com/2010/06/cloud-computing-tipos-de-nubes-de-aplicaciones/>
- [9] *Reese, G.* (2009). *En Cloud Application Architectures: Building Applications and Infrastructure in the Cloud Theory in Practice (o'Reilly) Series.* O'Reilly Media, Inc.
- [10] *Williams, D. M.* (2010). *In A quick start guide to Cloud Computing, moving your business into the cloud.*
- [11] *Stratec, B. S.-D.* (28 de Octubre de 2012). Recuperado en Diciembre de 2012, de <http://baesystemsdetica.blogspot.com/>
- [12] *Bookman, E.* (9 de Diciembre de 2009). Recuperado en Diciembre de 2012, de <http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-2010-future-threat-report/>
- [13] *Inter.net Datacenter.* (Noviembre de 2012). Recuperado en Diciembre de 2012, de <http://www.internetdatacenter.com.ar/faq2.html>
- [14] *Ponemon Institute.* (Abril de 2011). Recuperado en Diciembre de 2012, de <http://www.ca.com/~media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf>
- [15] *Symantec.* (3 de Mayo de 2012). Recuperado en Diciembre de 2012, de http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20120503_01
- [16] *Director, Richardson. R.* (Diciembre de 2010). Recuperado en Diciembre de 2012, de <http://gocsi.com/survey>

- [17] *Endian*. (Diciembre de 2012). Recuperado de <http://www.endian.com/es/>
- [18] *Revista It Now*. (25 de Septiembre de 2012). Recuperado en Diciembre de 2012, de <http://revistaitnow.com/2012/09/seguridad/mas-alla-del-firewall-y-la-seguridad-perimetral/>
- [19] *Tu VPN - Blog*. (Septiembre de 2012). Recuperado en Diciembre de 2012, de <http://blog.tuvpn.com/tag/tuneles-ssh2/?lang=es>
- [20] Villalón, A. H. (2 de Octubre de 2000). *Seguridad en Unix y Redes*. Recuperado en Enero de 2013, de <http://www.rediris.es/cert/doc/unixsec/unixsec.pdf>
- [21] López, P. A. (2010). *Seguridad Informática*. España
- [22] Myerson, J. (2011, Agosto 1). Recuperado en Enero de 2013, de <http://www.ibm.com/developerworks/ssa/cloud/library/cl-cloudsecurepolicy/>
- [23] Winkler, V. (2011). "Securing the Cloud: Cloud Computer Security Techniques and Tactics". Elsevier Inc.
- [24] *Xen*. (28 de Marzo de 2012). Recuperado en Enero de 2013, de http://wiki.xen.org/wiki/XCP/XenServer_Feature_Matrix
- [25] *Xen*. (27 de Noviembre de 2012). Recuperado en Enero de 2013, de http://wiki.xen.org/wiki/XCP_Release_Features
- [26] *Citrix Community*. (13 de Septiembre de 2011). Recuperado en Enero de 2013, de <http://community.citrix.com/display/xs/XenCenter+Plugins>

- [27] *101 Consulting*. (s.f.). Recuperado en Febrero de 2013, de http://www.101-consulting.com/index.php?option=com_content&view=category&layout=blog&id=51&Itemid=72
- [28] *Blog Virtualización & Cloud Computing*. (15 de Febrero de 2012). Recuperado el Febrero de 2013, de <http://www.josemariagonzalez.es/2012/02/15/como-configurar-high-availability-en-xenserver.html>
- [29] *Tissat*. (21 de Febrero de 2012). Recuperado en Marzo de 2013, de <http://tissat.wordpress.com/2012/02/21/cloud-comuting-taxonomia-por-niveles-o-modelos-de-servicio-iaas-paas-y-saas/>
- [30] *Blog de TresW*. (24 de Julio de 2012). Recuperado el Marzo de 2013, de <http://blog.tresw.com/watchguard/derrotando-a-los-botnets-del-futuro/>
- [31] *El Espectador.com*. (14 de Abril de 2009). Recuperado el Abril de 2013, de <http://www.elespectador.com/tecnologia/articulo-400077-aumenta-robo-de-identidad-web>
- [32] *RSA*. (2009). Recuperado el Abril de 2013, de http://www.rsa.com/solutions/business/wp/11021_CLOUD_WP_0209_SP.pdf
- [33] Recuperado en Mayo de 2013, de <http://www.snort.org/>
- [34] *HubPages*. (16 de Febrero de 2013). Recuperado el Mayo de 2013, de <http://skear.hubpages.com/hub/How-to-Set-Up-an-HTTP-Anti-Virus-Proxy-Using-pfSense-and-HAVP#>