



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE CIENCIAS DE LA
COMPUTACIÓN**

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

**TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL
TÍTULO DE INGENIERO DE SISTEMAS**

**TEMA: ANÁLISIS E IMPLEMENTACIÓN DE UN SERVIDOR DE
SERVICIOS DE RED PARA LA EMPRESA CEMYLUB
UTILIZANDO PLATAFORMAS Y HERRAMIENTAS DE
SOFTWARE LIBRE**

AUTOR: VILLACÍS MOYA EDISON RAFAEL

DIRECTOR: ING. ALDÁS MORENO ROMEL EDUARDO

SANGOLQUÍ

2016



**DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA**

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**ANÁLISIS E IMPLEMENTACIÓN DE UN SERVIDOR DE SERVICIOS DE RED PARA LA EMPRESA CEMYLUB UTILIZANDO PLATAFORMAS Y HERRAMIENTAS DE SOFTWARE LIBRE**" realizado por el señor **EDISON RAFAEL VILLACÍS MOYA** ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor **EDISON RAFAEL VILLACÍS MOYA** para que lo sustente públicamente.

Quito, 21 de enero del 2016



ING. GERMÁN NACATO CAIZA
DIRECTOR



DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

Yo, **EDISON RAFAEL VILLACÍS MOYA**, con cédula de identidad N° 171399079-2, declaro que este trabajo de titulación "**ANÁLISIS E IMPLEMENTACIÓN DE UN SERVIDOR DE SERVICIOS DE RED PARA LA EMPRESA CEMYLUB UTILIZANDO PLATAFORMAS Y HERRAMIENTAS DE SOFTWARE LIBRE**" ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Quito, 21 de enero del 2016

EDISON RAFAEL VILLACÍS MOYA
C.C. 171399079-2



**DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA**

AUTORIZACIÓN

Yo, **EDISON RAFAEL VILLACÍS MOYA**, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **“ANÁLISIS E IMPLEMENTACIÓN DE UN SERVIDOR DE SERVICIOS DE RED PARA LA EMPRESA CEMYLUB UTILIZANDO PLATAFORMAS Y HERRAMIENTAS DE SOFTWARE LIBRE”** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Quito, 21 de enero del 2016

EDISON RAFAEL VILLACÍS MOYA
C.C. 171399079-2

DEDICATORIA

Presento este proyecto de tesis con orgullo a la mujer que me ha traído a este mundo, un ser que con toda su bondad, paciencia, esfuerzo y dedicación me ha enseñado a lo largo de la vida a luchar por mis sueños y metas, mi madre Bertha Moya, quien ha sido mi fortaleza durante todo el recorrido de esta carrera.

A mi padre, hermano, sobrinos y cuñada que me han alentado para continuar con mi formación profesional, siendo pilares muy importantes en mi vida y demostrándome su apoyo incondicional para concluir esta meta.

AGRADECIMIENTOS

Doy gracias a Dios por brindarme la salud necesaria hasta hoy en día para lograr este objetivo planteado.

A mis padres Bertha y José por brindarme todo su apoyo incondicional, no solo durante etapa, sino a través de toda mi existencia.

A mi hermano Carlos quien me ha demostrado ser un gran ejemplo, ya que le considero un gran profesional y un excelente hermano.

A mis grandes amigos del colegio Henry, Paul y David, por demostrarme que a pesar de los años siempre puedo contar con todo su apoyo, consejos y amistad.

A mis grandes amigos de la universidad Willy, Vinicio, Darwin y Daniel por brindarme su amistad incondicional y conocimientos durante mi carrera, ya que gracias a ellos hoy puedo culminar mi proyecto de tesis.

ÍNDICE DE CONTENIDO

CERTIFICADO	ii
AUTORÍA DE RESPONSABILIDAD	iii
AUTORIZACIÓN (PUBLICACIÓN BIBLIOTECA VIRTUAL).....	iv
DEDICATORIA.....	v
AGRADECIMIENTOS	vi
ÍNDICE DE CONTENIDO	vii
ÍNDICE DE TABLAS	xii
ÍNDICE DE FIGURAS.....	xii
RESUMEN.....	xviii
ABSTRACT	xix
CAPÍTULO 1	1
1.1 Introducción	1
1.2 Planteamiento del problema	3
1.3 Justificación e importancia.....	4
1.4 Objetivos.....	5
1.4.1 Objetivo general.....	5
1.4.2 Objetivos específicos	6
1.5 Alcance.....	6
CAPÍTULO 2	8
2.1 ZIMBRA	8
2.1.1 Concepto	8
2.1.2 Arquitectura Zimbra	8
2.1.3 Componentes de la arquitectura Zimbra	9
2.1.3.1 Zimbra Core:	9
2.1.3.2 Zimbra LDAP:.....	9

2.1.3.3 Zimbra MTA:.....	10
2.1.3.4 Zimbra Store:.....	10
2.1.3.5 Zimbra SNMP	11
2.1.3.6 Zimbra Logger	11
2.1.3.7 Zimbra Spell	11
2.1.4 Servidor Zimbra	11
2.1.4.1 Perfiles de usuario.....	13
2.1.5 Cliente web	14
2.1.6 Beneficios de Zimbra	15
2.2 IPTABLES.....	16
2.2.1 Acerca de iptables y netfilter	16
2.2.2 Concepto	16
2.2.3 Tablas.....	17
2.2.3.1 Tabla Filter	18
2.2.3.2 Tabla Nat.....	18
2.2.3.3 Tabla Mangle.....	19
2.2.3.4 Tabla Raw	19
2.2.4 Reglas	20
2.3 SQUID.....	21
2.3.1 Concepto	21
2.3.2 Características de Squid	22
2.3.3 Squidguard	23
2.3.3.1 Características de Squidguard.....	23
2.3.4 Dansguardian	23
2.3.4 Soporte de Squid	24
2.3.5 Herramientas para Squid	25

2.3.5.1 Multitail	25
2.3.5.2 SquidView	25
2.3.5.2 Sarg.....	25
2.3.5.3 Calamaris	26
2.4 SNORT	27
2.4.1 Concepto	27
2.4.2 COMPONENTES DE SNORT.....	29
2.4.2.1 Decodificador de paquetes	29
2.4.2.2 Preprocesadores	30
2.4.2.3 Motor de detección	31
2.4.2.4 Módulo de captura de datos	32
2.4.2.5 Archivo de reglas.....	32
2.4.2.6 Plugins de detección	32
2.4.2.7 Plugins de salida	33
2.4.3 Personalización de reglas de snort	34
2.4.3.1 Estructura de una regla	35
2.4.3.2 Cabecera de una regla	35
2.5 NESSUS	35
2.5.1 Concepto	36
2.5.2 COMPONENTES BÁSICOS	37
2.5.2.1 Nessus cliente y servidor.....	37
2.5.2.2 Los plugins	38
2.5.2.3 La base de datos actualizada de vulnerabilidades.....	38
2.5.2.3 Informes completos	38
2.5.3 Descripción general de la interface de usuario de Nessus	39
2.5.4 Plataformas admitidas.....	40

2.5.5 Descripción general de directivas	40
CAPÍTULO 3	42
3.1 ZENTYAL.....	42
3.1.1 Instalación de Zentyal	42
3.1.2 Configuración de Zentyal	48
3.2 Configuración de Squid en Zentyal.....	51
3.3 Analogía de Zentyal en el archivo Squid.conf.....	53
3.3 Configuración de firewall con Zentyal	62
3.3.1 Acceso ssh y registro de todas las conexiones	69
3.4 Instalación de servidor de correo virtual Zimbra Collaboration Suite ..	70
3.4.1 Instalación de Zimbra Collaboration Suite en Centos	70
3.5 Instalación de nessus en Windows server 2008	80
3.5.1 Instalación de Windows server 2008.....	80
3.5.1.1 Pasos de instalación de Windows server.....	81
3.5.2 Instalación del servidor nessus	85
3.5.3 Configuración de nessus.....	89
3.5.3.4 Actualización de plugins de nessus	95
3.6 Instalación de EasyIDS en Centos 5.3	96
3.6.1 Instalación de easyids-snort.....	96
CAPÍTULO 4	104
4.1 Servicio de Proxy HTTP en Zentyal.....	104
4.1.1 Reglas de acceso	104
4.1.2 Filtrado de contenidos con Zentyal	105
4.1.3 Limitación de ancho de banda	110
4.2 Servicio de Firewall HTTP en Zentyal	111

4.3 Servicio de correo electrónico utilizando Zimbra Collaboration Suite	
8.0.7. 118	
4.3.1 Interfaz web de administrador	118
4.3.2 Interfaz web de usuario	122
4.3.2.1 Aplicaciones de Zimbra	122
4.3.2.2 Configuración de preferencias en zimbra	123
4.3.2.3 Uso del correo electrónico	125
4.3.2.4 Librería de direcciones	127
4.3.2.5 Uso del calendario	128
4.3.2.6 Opción de tareas	129
4.3.2.7 Etiquetas	130
4.4 Snort en EasyIDS	132
4.4.1 Menú de administración	132
4.5 Escaneo de vulnerabilidades utilizando Nessus	136
4.5.1 Menú de configuración	139
4.5.2 Teclas de acceso rápido de la interfaz	140
4.5.3 Políticas	141
4.5.3.1 Creación de una nueva política	142
4.5.3.2 Creación de una política avanzada	144
4.5.4 Exportación, importación y copia de políticas	144
4.5.5 Creación y programación de un análisis	145
CAPÍTULO 5	150
5.1 Conclusiones	150
5.2 Recomendaciones	151
5.3 Bibliografía	152

ÍNDICE DE TABLAS

Tabla 1	Perfiles de usuario	13
Tabla 2	Beneficios de Zimbra	15
Tabla 3	Targets o acciones con sus respectivas descripciones	17
Tabla 4	Cadenas usadas en la tabla filter y su descripción	18
Tabla 5	Cadenas usadas en la tabla nat	19
Tabla 6	Cadenas usadas en la tabla Mangles.....	19
Tabla 7	Cadenas usadas en la tabla raw	20
Tabla 8	Ventajas y desventajas de un sistema SNORT	27
Tabla 9	Módulos de Salida de Snort	33
Tabla 10	Métodos de entrega multimedia de Windows	81
Tabla 11	Directorios principales de Nessus	89
Tabla 12	Teclas de acceso rápido al interfaz principal y listas	140
Tabla 13	Teclas de acceso rápido de resultados y análisis	141
Tabla 14	Estados de análisis	145

ÍNDICE DE FIGURAS

Figura 1	Arquitectura del servidor zimbra (Sabater, 2008)	13
Figura 2	Esquema de uso de un proxy squid	22
Figura 3	Mecanismo	24
Figura 4	Arquitectura de snort.....	28
Figura 5	Flujo de datos del decodificador	30
Figura 6	Selección de idioma	43
Figura 7	Inicio del instalador de zentyal	43
Figura 8	Configuración del teclado.....	44
Figura 9	Selección del teclado	44
Figura 10	Configuración tarjetas de red	45
Figura 11	Nombre de la máquina.....	45
Figura 12	Nombre de usuario	46
Figura 13	Ingreso de contraseña del usuario	46

Figura 14 Progreso de la instalación.....	47
Figura 15 Finalización de la instalación.....	47
Figura 16 Entorno gráfico con la interfaz de administración	48
Figura 17 Perfiles y paquetes de zentyal	49
Figura 18 Acceso al dashboard de zentyal 1	50
Figura 19 Acceso al dashboard de zentyal 2	51
Figura 20 Configuración general proxy	52
Figura 21 Creación del objeto localnet	53
Figura 22 Definición de regla de acceso	54
Figura 23 Creación de las extensiones	55
Figura 24 Diagrama de configuración de squid para la red perimetral ...	56
Figura 25 Creación de la regla de acceso al perfil extensiones.....	57
Figura 26 Acceso dominios-denegados	58
Figura 27 Configuración de la regla de acceso dominios-denegados	58
Figura 28 Creación de dominios que van a ser denegados.....	59
Figura 29 Lista de dominios que van a ser denegados	59
Figura 30 Regla de control de acceso a dominios-denegados	60
Figura 31 Creación de la dirección mac	61
Figura 32 Miembros añadidos por mac.....	61
Figura 33 Regla de acceso para permitir el objeto macsredlocal	62
Figura 34 Interfaz externa de zentyal eth0	63
Figura 35 Interfaz externa de zentyal eth1	63
Figura 36 Flujos de tráfico en el cortafuego (S.L., 2014)	64
Figura 37 Reglas de filtrado del cortafuegos	65
Figura 38 Lista de reglas de filtrado de paquetes.....	66
Figura 39 Creación de una nueva regla	68
Figura 40 Acceso Log para redes externas.....	69
Figura 41 Edición de regla para servicio SSH	69
Figura 42 Reglas para permitir el acceso a conexiones shh	70
Figura 43 Edición del host en centos	71
Figura 44 Edición de la dirección ip y dominio del equipo	71
Figura 45 Verificación de la dirección IP del servidor	72

Figura 46 Preparación de servicios de Sendmail	72
Figura 47 Copia de archivos de instalación en OPT	73
Figura 48 Archivo webmin descomprimido.....	73
Figura 49 Archivo instalador deZimbra.....	74
Figura 50 Ingreso al directorio de Instalación.....	74
Figura 51 Verificación de librerías.....	75
Figura 52 Instalación de librerías con yum --y install	75
Figura 53 Instalación de /install.sh --platform-override	76
Figura 54 Selección de paquetes a instalar	76
Figura 55 Verificación de la integridad de la base de datos	77
Figura 56 Creación de usuario de zimbra	78
Figura 57 Verificación de funcionamiento de servicios.....	78
Figura 58 Aplicando configuraciones en Zimbra	79
Figura 59 Finalización de la instalación.....	79
Figura 60 Ingreso a la consola de administración de zimbra.....	80
Figura 61 Mensaje para acceder a BBS POPUP	82
Figura 62 Inserción de DVD.....	82
Figura 63 Selección del tipo de instalación	83
Figura 64 Dirección de instalación de Windows Server.....	84
Figura 65 Creación de la nueva partición de disco.....	84
Figura 66 Asistente de instalación de Nessus.....	86
Figura 67 Contrato de licencia de Nessus.....	86
Figura 68 Ubicación de la instalación de Nessus	87
Figura 69 Selección del tipo de instalación	87
Figura 70 Confirmación de la instalación de nessus	88
Figura 71 Finalización de la instalación de nessus	88
Figura 72 Servicio de tenable nessus iniciado	90
Figura 73 Interfaz de inicio de nessus.....	91
Figura 74 Interfaz de certificado de seguridad	91
Figura 75 Certificado de seguridad	92
Figura 76 Interfaz de registro de nessus	92
Figura 77 Interfaz de creación de usuario y contraseña	93

Figura 78 Interfaz de activación mediante código	93
Figura 79 Registro con código de activación.....	94
Figura 80 Actualización y descarga de plugins	94
Figura 81 Primera actualización de nessus.....	95
Figura 82 Autenticación de Nessus.....	95
Figura 83 Actualización diaria de plugins	96
Figura 84 Interfaz web de la configuración.....	96
Figura 85 Ejecución del instalador de easyids	97
Figura 86 Selección del idioma	97
Figura 87 Selección de la zona horaria	98
Figura 88 Selección de la contraseña del root	98
Figura 89 Mensaje de advertencia de instalación	99
Figura 90 Permitir lectura y escritura a vmnet0	99
Figura 91 Configuración de redes en easyids	100
Figura 92 Observación de lista de reglas de iptables	100
Figura 93 Ingreso a la interfaz desde otra máquina	101
Figura 94 Interfaz de easyids	101
Figura 95 Inicio de creación de reglas en snort.....	102
Figura 96 Listas de archivos de reglas de snort en easyids	102
Figura 97 Ingreso de regla con editor en el fichero ping.rules	103
Figura 98 Inclusión de una propia regla snort	103
Figura 99 Creación de nueva regla	104
Figura 100 Perfiles de filtrado	105
Figura 101 Umbral de contenido	106
Figura 102 Reglas de dominios y url	106
Figura 103 Lista por categorías.....	107
Figura 104 Categorías de dominios	108
Figura 105 Ficheros tipo mime.....	109
Figura 106 Extensiones de archivos	109
Figura 107 Creación de la regla de limitación de ancho de banda	110
Figura 108 Regla creada de limitación de ancho de banda.....	111
Figura 109 Creación del servicio SSH.....	112

Figura 110 Puerto destino del servicio ssh.....	112
Figura 111 Servicio ssh creado.....	113
Figura 112 Creación de la regla de bloqueo con el servicio ssh.....	113
Figura 113 Accediendo a it_bodega desde putty	114
Figura 114 Pantalla de error de conexión en la interfaz Putty	115
Figura 115 Pantalla de telnet	115
Figura 116 Creación del servicio zimbra	116
Figura 117 Puerto destino del servicio zimbra.....	116
Figura 118 Creación de la regla para el servicio zimbra.....	117
Figura 119 Pantalla de bloqueo hacia el administrador de zimbra	118
Figura 120 Ingreso al interfaz web de administrador	119
Figura 121 Interfaz web de administrador	119
Figura 122 Menú particular	120
Figura 123 Creación de una nueva cuenta	121
Figura 124 Creación de una nueva cuenta	121
Figura 125 Configuración general	122
Figura 126 Interface de usuario en zimbra	123
Figura 127 Ventana de preferencias en zimbra.....	125
Figura 128 Partes de la ventana del correo	127
Figura 129 Búsqueda de un contacto en zimbra	128
Figura 130 Uso del calendario en zimbra	129
Figura 131 Opción de tareas.....	130
Figura 132 Detalles de la tarea	130
Figura 133 Creación de etiquetas	131
Figura 134 Interfaz base de snort	132
Figura 135 Alertas generadas	133
Figura 136 Tráfico de red.....	133
Figura 137 Rendimiento del sistema	134
Figura 138 Rendimiento de Snort	134
Figura 139 Menú de ajustes.....	135
Figura 140 Estado del sistema.....	135
Figura 141 Menú de herramientas	136

Figura 142 Interfaz de acceso.....	136
Figura 143 Menú inicio de nessus.....	137
Figura 144 Opciones del menú	137
Figura 145 Opción de configuración	138
Figura 146 Perfil de usuario	138
Figura 147 Menú de configuración.....	140
Figura 148 Paso para agregar una nueva política.....	142
Figura 149 Segundo paso para agregar una política.....	143
Figura 150 Tercer paso para agregar una nueva política	143
Figura 151 Política avanzada.....	144
Figura 152 Exportación, importación y copia de políticas.....	144
Figura 153 Programación de un análisis	145
Figura 154 Creación de un nuevo scan.....	146
Figura 155 Pestaña de configuración del programa	147
Figura 156 Análisis modificado	147
Figura 157 Petición de mail para entrega de resultados	148
Figura 158 Estado del análisis	148
Figura 159 Informe de resultados de un análisis	149

CAPÍTULO 1

MARCO REFERENCIAL

1.1 Introducción

Gracias a la innovación de la tecnología en el campo de la computación hoy en día, se cuenta con una facilidad al momento de establecer una administración de redes dentro de una empresa, no obstante se debe tener en cuenta todos los aspectos que involucran a la seguridad en redes de datos en autenticación, confidencialidad, autorización e integridad; así también como en la seguridad de sus equipos, servicios y datos.

Toda organización que se enlaza mediante una red local o al internet deben conocer los riesgos que pueden correr los recursos conectados en las mencionadas redes, para de tal manera diseñar un óptimo modelo de investigación e implementación sobre seguridades que brinden la adecuada protección mediante medios que involucren un entorno fiable.

Las redes constituyen sistemas acordes de interconexión entre dispositivos separados que permiten compartir información y recursos tales como periféricos, estaciones de trabajo, servidores, etc. Es por ello que una red bien protegida puede brindar la rapidez y confiabilidad de comunicación que resulta fundamental para la eficiencia dentro de una empresa.

Ante esta necesidad de seguridad, han surgido herramientas para la protección de los sistemas, estas herramientas llamados firewalls permiten la conectividad en la red con un grado de defensa al restringir el acceso no autorizado, permitiendo al mismo tiempo comunicaciones confirmadas. Dentro de esta herramienta debemos considerar establecer políticas de

seguridad propia en cada estación de trabajo disponible, considerando la autenticación y encriptación de los datos.

Navegar mediante el internet sin un servidor de seguridad aumenta la vulnerabilidad de la información que pueden provocar pérdidas irremediables, es por eso que se debe implementar un proxy para interceptar las conexiones de red que el usuario realiza al servidor del destino mediante un intermediario.

A medida que los sistemas de seguridad son más eficientes, los ataques son cada vez más perfeccionados, detectando con más frecuencia intrusos de tal forma que comprometen nuestra confidencialidad y disponibilidad, hoy en día tenemos los IDS (Intrusion Detection System) que permiten a las organizaciones proteger sus sistemas a medida que incrementan su conectividad hacia la red.

La información que maneja cada empresa es vital, por lo cual se debe mantener de acuerdo a lo requerido por las políticas de la organización, siendo hoy en día, la tecnología de la información una herramienta importante para el desarrollo, se debe tener en cuenta el escaneo en los sistemas de cómputo para encontrar vulnerabilidades e identificar potenciales puntos de acceso para los intrusos.

Así mismo cuando se trabaja en una empresa pequeña o mediana debemos tomar en consideración el presupuesto que se quiere invertir para poder dar soluciones en cuanto a un servicio de correo empresarial ya que hoy en día es un elemento de comunicación básico para cualquier compañía, para lo cual se debe disponer de un sistema de correo eficiente y adaptado a las necesidades de sus usuarios.

1.2 Planteamiento del problema

Actualmente las empresas son dependientes de sus redes informáticas perimetrales, en el cual se encuentran expuestas contra amenazas deliberadas ya que en las mencionadas redes locales circula información que puede ser robada, alterada o destruida; y aún más si las mismas tienen acceso a internet por que las hace más vulnerable y es más difícil la prevención y detección de ataques.

En su mayoría las organizaciones no invierte un capital necesario para establecer un nivel de seguridad apropiado para evitar que exista un daño y/o perdida de la información que pueda llegar a comprometer la continuidad de la ejecución de trabajo que se realicen en dichas organizaciones y mucho menos en un servidor de correo, una de estas es la empresa CEMYLUB ya que necesita implementar servicios de red para mejorar el rendimiento laboral al manejar información dentro de su dependencia.

Cuando no se tiene conocimiento del alcance que tienen los sistemas informáticos, ni lo indefensos que pueden ser y si estos son llevados a internet por los mismos funcionarios de la empresa CEMYLUB, existe una fuga de información hacia el exterior cayendo en ataques externos o virus informáticos.

CEMYLUB no cuenta con servicio de correo corporativo, firewall, proxy, de detección de intrusos y un servicio de escaneo de vulnerabilidades. La falta de estas medidas de seguridad es un problema que se encuentra en crecimiento ya que cada vez existe un mayor número de atacantes que día a día van adquiriendo más habilidad; cabe mencionar que también se encuentran fallas de seguridad provenientes del interior de la mencionada organización.

Todas estas desventajas que se han presentado en la empresa CEMYLUB al no contar con estos tipos de servicios de red han provocado que las actividades de los usuarios se hagan cada vez más lentas, caer en la llamada lista negra de envío y recepción de correo por producir spam, estaciones de trabajo infectadas, vulnerables a los hackers, acceso a la web por parte de los usuarios sin ningún nivel de control de acceso, toda la actividad de manejo de dinero a través de aplicaciones web estaría sujeta a fraudes.

1.3 Justificación e importancia

La implementación de los servicios de red proporcionan niveles de seguridad que van a contribuir a que no existan fallos dentro de la red perimetral que pueden llegar a ser muy costosos en lo relativo a la productividad, eficiencia, pérdida de datos e información importante; así como va a ayudar a la medición para la detección de riesgos y vulnerabilidades que existan en la mencionada red.

Los servicios de red tienden a ser un motivo de descuido hoy en día en las empresas, si no se conoce las fases de seguridad que comprende tanto la protección física de los dispositivos como también la confidencialidad, integridad y autenticidad de la información para mantener la operación, producción y administración organizacional.

El servicio de correo tiene una gran importancia en toda empresa por ser un medio de comunicación constante, el mismo que debe ser rápido y sin interrupción. Por lo cual es necesario implementar y poner en funcionamiento un servicio de correo con una plataforma que cumpla con estas características.

El servicio de firewall a nivel de seguridad externa como interna para empresa deberá ser el punto principal de aseguramiento de información como de la red de una empresa. Por lo cual se necesitar tener un firewall

propio de la empresa para tener un control del mismo y no depender de servicio de terceros.

El servicio de proxy para control de navegación web a nivel de red interna en una empresa es muy importante para tener un control de acceso a páginas de internet y optimizar el uso del mismo para empresa. La empresa necesita tener su propio servicio de proxy para control el acceso a páginas de internet que sean de uso según los fines de negocio de la empresa, también así proporcionándonos ahorro de tráfico de red, filtrado en contenidos y acepta una gran demanda de usuarios.

Toda empresa debe tener en su red servicios de detección de intrusos como también servicio de escaneo de vulnerabilidades para tener una óptima visión de que la red de la empresa como su información no está expuesta a terceros. Por lo cual es necesario tener estos dos servicios para evitar fraudes.

Es por ello que esta implementación sobre los servicios de red por parte de la carrera de Ingeniería de Sistemas e Informática en donde se llevara a cabo reglas, políticas y procedimientos que nos conlleven un buen desarrollo de un modelo de seguridad en la red perimetral de la empresa CEMYLUB.

1.4 Objetivos

1.4.1 Objetivo general

Implementar servicios de red como son: servicio de correo, firewall, proxy, detección de intrusos y escaneo de vulnerabilidades utilizando herramientas de software libre para mantener la confidencialidad, integridad y disponibilidad de la información.

1.4.2 Objetivos específicos

- Implementar una aplicación de servicio de correo electrónico de código abierto totalmente funcional y de alto rendimiento, que ofrezca las herramientas necesarias para compartir recursos en la red.
- Definir políticas de red mediante un servidor de firewall, el cual brinde seguridad a la red local, controlando las comunicaciones e impidiendo ataques de usuarios malintencionados ya sean internos o externos.
- Configurar un servidor proxy con autenticación de usuarios controlando el acceso a los recursos usando diferentes criterios de acceso analizando el tráfico generador mediante la herramienta de Squid.
- Escanear e identificar vulnerabilidades a equipos o protocolos en nuestra red perimetral, reduciendo los riesgos de las redes de datos mediante un servidor Nessus.
- Crear e interpretar reglas que nos ayuden a analizar nuestros sistemas de información que circulan por la red de datos, protegiendo en tiempo real ante posibles intrusiones configuradas en el IDS Snort.

1.5 Alcance

El proyecto estará enfocado al análisis, selección e implementación de arquitecturas tecnológicas a utilizar, verificando la infraestructura tecnológica de la empresa para definir una estrategia de la implementación de los siguientes servicios:

- Servicio de correo utilizando Zimbra.
- Firewall utilizando IpTables.
- Proxy utilizando Squid.
- Detección de intrusos utilizando Snort.
- Escaneo de vulnerabilidades utilizando Nessus.

Realizar las configuraciones adecuadas para optimizar la funcionalidad de los servicios implementados en el servidor, realizando las respectivas pruebas de funcionalidades y puesta en producción.

CAPÍTULO 2

MARCO TEÓRICO

2.1 ZIMBRA

2.1.1 Concepto

Zimbra Collaboration Suite (ZCS) es una herramienta de soporte al trabajo colaborativo de nivel empresarial, la cual está orientada a la mensajería de código libre y ofrece un servicio de correo electrónico fiable de alto rendimiento, teniendo herramientas adicionales como libreta de contactos, mensajería instantánea, tareas, enlaces, documentos web, voz sobre ip, a través de una interfaz unificada vía web que puede ser consultada en cualquier momento y desde cualquier ubicación con un dispositivo que tenga acceso al Internet.

2.1.2 Arquitectura Zimbra

Zimbra instala todo un sistema de correo electrónico, el cual está basado en paquetes libres, ya que se trata de una recopilación de paquetes existentes y comprobados como Postfix, MySQL el cual almacena las prioridades y meta datos de los mensajes y los mensajes de correo son almacenados directamente en el sistema de ficheros, Lucene que concede a los usuarios a restablecer la información de mensajes en numerosas carpetas de correo, OpenLDAP, esta última proporcionándonos autenticación. Zimbra presenta una interfaz de webmail amigable para el usuario con apoyo a Ajax (Asynchronous Java Script And XML) que define parámetros de configuración tanto en los equipos conectados en red como a los usuarios dando una arquitectura estándar.

Por otro lado Zimbra permite la edición de los mensajes en formatos HTML (Hyper Text MarkupLanguage); así como una búsqueda interesante de mensajes en grandes archivos de correo gracias a sus filtros de búsqueda, reenvíos (forward) y varios alias para las cuentas de usuarios. Su arquitectura se encuentra basada en servicios web y varias API's.

Hablando en términos empresariales el mencionado servidor de correo beneficia a la empresa con bajos costos de operación y una mejor imagen corporativa; así como un mantenimiento y administración simplificada en cada puesto informático de trabajo que se instale, siendo así Zimbra una solución de calidad para integraciones en el sistema de información y también interactúa con los sistemas profesionales de sus clientes.

2.1.3 Componentes de la arquitectura Zimbra

Zimbra está conformado por componentes dentro de su arquitectura los cuales son:

2.1.3.1 Zimbra Core:

Posee Librerías, rendimiento, mecanismos de monitoreo y ficheros de configuración.

2.1.3.2 Zimbra LDAP:

LDAP es un protocolo de aplicación para acceder a un directorio estructurado y distribuido para encontrar numerosa información en un entorno de red.

Zimbra LDAP posee un directorio de usuarios basado por defecto en OPEN DLAP (Protocolo Ligero de Acceso a Directorios) el cual gestiona el almacén de usuarios y permite configurar la utilización de directorios LDAP

externos así como el Active Directory de Microsoft, aparte que ofrece el soporte para la replicación.

Se puede utilizar la arquitectura LDAP en otra LDAP disponible que ya se encuentra creada el cual nos va ayudar a la centralización de cuentas de un usuario dentro de la instalación.

2.1.3.3 Zimbra MTA:

Enruta los paquetes recibidos a través de SMTP hacia los buzones usando protocolos de transferencia de correo local. A estos también se los vincula componentes de antispam y antivirus.

Componentes en el servidor de correo Zimbra:

- MTA (Agente de transferencia de correo)
- Almacén de buzón de mensajes por IMAP4 y POP3
- Filtros antivirus y antispam

2.1.3.4 Zimbra Store:

Usando Jetty almacena el correo electrónico, para lo cual las cuentas se las puede modificar en el servidor y este se encuentra integrado con un servidor de buzón de correo conformado por:

- Almacén de datos, el cuál es una base de datos MS SQL que identifica el buzón con la cuenta de usuario perteneciente en el directorio LDAP.
- Almacén de mensajes, el cual contiene todos los mensajes en formato MIME.
- Almacén de índices.

2.1.3.5 Zimbra SNMP

Paquete opcional, pero a la misma vez recomendado toma los datos periódicos del estado del sistema ya que monitoriza por SNMP (Simple Network Management Protocol), pero si no se lo instala no abra ningún problema, nuestro sistema funcionara correctamente.

2.1.3.6 Zimbra Logger

Genera informes mediante syslog y seguimiento de mensajes. Debe ser instalado, ya que existe la probabilidad que ciertas estadísticas no podrían ser vistas en la consola de administración.

2.1.3.7 Zimbra Spell

Es un paquete opcional que utiliza el proyecto de código abierto para ofrecer la corrección ortográfica (Aspell) dentro de la web basado en el cliente.

Una de las ventajas es que todos estos paquetes son instalados en un mismo servidor o en varios servidores, donde un servidor puede ser dedicado a cada componente. Zimbra fue diseñado con esto en mente para permitir la escalabilidad y facilidad en la administración

2.1.4 Servidor Zimbra

Zimbra server conocido también como el núcleo de Zimbra Collaboration Suite. Modelado sobre una arquitectura demasiado estable, debido a su código abierto. El servidor brinda soporte a muchos protocolos, los cuales hacen que los usuarios de plataformas populares logren interactuar.

Zimbra se caracteriza ya que tiene soporte a (SMTP, POP3, LDAP, IMAP), se puede incluir servicios de red como antivirus y antispam (Clam/AV, Spamassassin) y tiene la capacidad de migración de otros servicios de correos como Sendmail.

La velocidad del servidor zimbra es altamente veloz, eficaz y posee una escalabilidad en forma horizontal ya que los host tienen su propio almacén de correo y configuraciones, lo cual permitirá agregar más estaciones con distintos subdominios y manteniendo la misma dirección central dentro del dominio principal.

El MTA (agente de transferencia de correos) envía los mensajes de correo al servidor Zimbra, esta arquitectura por debajo está basada en Postfix, integrado a través del mismo. También tolera los principales protocolos que ya se conocen de cifrado de canal, SSL y TLS (Seguridad de la capa de transporte).

Los Zimlets son pequeños programas creados como un mecanismo para integrar datos y contenido de terceros con las funciones de Cliente web de Zimbra. Los Zimlets permiten trabajar con diferentes tipos de contenido en tus mensajes de correo. A continuación se muestra en la figura 1, la arquitectura del servidor Zimbra.

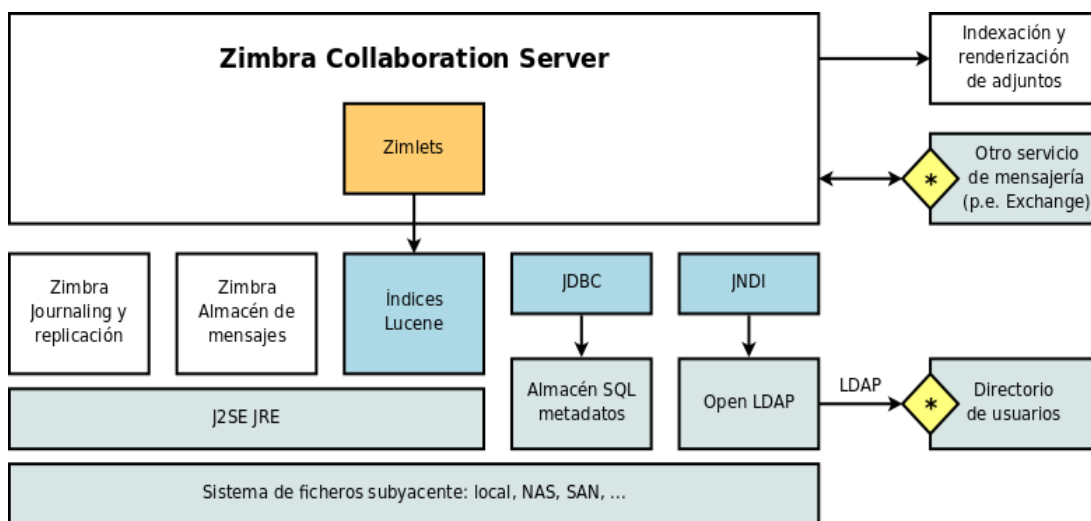


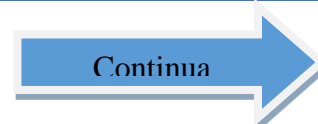
Figura 1 Arquitectura del servidor zimbra (Sabater, 2008)

2.1.4.1 Perfiles de usuario

En zimbra se tiene perfiles de usuarios o conocido también como COS (Class Of Service), dependiendo de las versiones ya sea estándar o avanzada las cuales definen todas las características en las cuentas de sus clientes, a continuación se cita la tabla 1 correspondiente a los perfiles de usuario y sus características en la versión avanzada.

**Tabla 1
Perfiles de usuario**

COMPONENTE	CARACTERÍSTICA
E-mail	<ul style="list-style-type: none"> • Crear y enviar nuevos mensajes de correo. • Incluir documentos adjuntos a los mensajes. • Leer y contestar mensajes de correo. • Reenvío de mensajes de correo electrónico a uno o más destinatarios. • Adaptar la vista del correo electrónico mediante la función de conversación o verlo en formato tradicional. • Búsqueda de mensajes, documentos adjuntos.
Libreta de direcciones	<ul style="list-style-type: none"> • Crear y manejar múltiples libretas de direcciones. • Crear fácilmente contactos de los correos



	<ul style="list-style-type: none"> recibidos. • Importar y exportar listas de contactos. • Compartir la libreta de contacto.
Agenda	<ul style="list-style-type: none"> • Crear y gestionar múltiples agendas. • Crear citas, encuentros, y eventos. • Asistente de horario "Libre/Ocupado" • Importar y exportar agendas. • Compartir sus agendas.
Tareas	<ul style="list-style-type: none"> • Crear múltiples listas de tareas. • Crear tareas. • Agregar archivos adjuntos a sus tareas. • Gestionar una tarea, establecer la prioridad, y un seguimiento del progreso. • Compartir sus listas de tareas.
Maletín	<ul style="list-style-type: none"> • Guardar cualquier tipo de archivo en su maletín para que, cuando abra sesión en cualquier ordenador, se conecte a su cuenta y pueda acceder a él. • Crear carpetas para organizar los ficheros que guarde. • Compartir las carpetas de su maletín.
Preferencias	<ul style="list-style-type: none"> • Gestionar las preferencias para e-mail, libretas de direcciones y agendas. • Crear filtros de correos. • Configurar el reenvío a otra cuenta de correo • Crear mensajes de notificación y designar cuándo activarlos y desactivarlos, como por ejemplo un mensaje de vacaciones. • Elección de idioma.

2.1.5 Cliente web

Zimbra integra un cliente web basado en Ajax (Asynchronous Java Script And XML), el cual comprende: correo electrónico, contactos, calendario compartido, VoIP y aplicaciones. Todo esto incorporado en los navegadores web más usados como Firefox, Chrome e Internet Explorer y dependiendo del uso de Javascript será la experiencia del usuario. Para estaciones antiguas no hay ningún problema ya que el cliente web de Zimbra admite usar una versión simplemente con HTML.

Una de las ventajas del cliente web es que brinda una gran utilidad al permitir accederlo desde cualquier lugar, ya que se puede sincronizar mediante dispositivos móviles, desde la mayoría de navegadores y también es compatible con clientes propietarios como Microsoft Outlook, Novel Evolution y Apple Mail.

2.1.6 Beneficios de Zimbra

Zimbra proporciona flexibilidad ya que se personaliza según las necesidades de la organización, libertad debido a que utiliza el cliente web de Zimbra con otros programas tradicionales, como plataforma mixta, durabilidad porque es un servidor de correo electrónico y calendario extraordinariamente fiable y ampliable, además posee bajo mantenimiento ya que su gestión es completamente sencilla. En la tabla 2 se muestra los beneficios para el usuario y el administrador.

Tabla 2

Beneficios de Zimbra

BENEFICIOS PARA EL USUARIO	BENEFICIOS PARA EL ADMINISTRADOR
<ul style="list-style-type: none"> • Accesible desde cualquier lugar. • Elección del cliente: webmail Zimbra, Zimbra Desktop, Zimbra Mobile, Ms Outlook. • Aumento de la colaboración y la productividad. • Todas las funciones disponibles para dentro de una misma interfaz: mensajes de correo 	<ul style="list-style-type: none"> • Escalabilidad hasta millones de buzones, fiabilidad. • Administración simple (consola de administración AJAX). • Optimización del almacenamiento. • Fiabilidad de los componentes de código abierto. • Menor costo de inversión que

Continúa



electrónico, libretas de archivos taras	calendarios, direcciones,	las soluciones propietarias. • Accesible desde cualquier lugar: Firefox, IE, Safari, independiente del sistema operativo: Windows, MAC, Linux.
---	------------------------------	---

(Quer System Informática, 2010)

2.2 IPTABLES

2.2.1 Acerca de iptables y netfilter

“Netfilter es un conjunto de ganchos (Hooks), es decir, técnicas de programación que se emplean para crear cadenas de procedimientos como manejador dentro del núcleo de GNU/Linux y que son utilizados para interceptar y manipular paquetes de red. El componente mejor conocido es el cortafuegos, el cual realiza procesos de filtración de paquetes. Los ganchos son también utilizados por un componente que se encarga del NAT (Network Address Translation o Traducción de dirección de red). Estos componentes son cargados como módulos del núcleo”. (Dueñas, 2013).

2.2.2 Concepto

Es una herramienta que se encarga de configurar las reglas de cortafuegos IP de kernel, también se le considera un sistema de clasificación de paquetes, es decir filtra dichos paquetes, traduce direcciones de red y los manipula antes de enrutarlos.

Iptables es una estructura de tabla genérica y posee un conjunto de reglas, cada regla posee ciertas características las cuales los paquetes deben cumplir; además para cada regla se asocia un target o acción, estas reglas son las encargadas de decidir qué hacer con el paquete.

Algunas ventajas de trabajar con IPtables se muestran a continuación:

- Especificación de puertos de origen y destino.
- Da soporte a protocolos TCP/UDP/ICMP.
- Soporte para interfaces de paquetes origen y destino.
- Permite un número ilimitado de reglas.
- Redireccionamiento de puertos.
- Estable y seguro.
- Enmascaramiento.

A continuación en la tabla 3 se indican las acciones o targets más usadas:

Tabla 3
Targets o acciones con sus respectivas descripciones

ACCIONES (TARGETS)	DESCRIPCIÓN
ACCEPT	Deja pasar el paquete a la siguiente etapa de procesamiento. Detiene el paso en la cadena actual, y empieza en la etapa siguiente.
DROP	Descontinúa el proceso del paquete completamente. No compara con cualquier otra regla, cadena o tablas.
QUEUE	Envía el paquete a la cola.
RETURN	Regresa el paquete hasta encontrar o cumplir con la regla comparada.

(Zwicky Elizabeth, 2000)

2.2.3 Tablas

Cada target hace uso de tres tablas las cuales se describen a continuación:

2.2.3.1 Tabla Filter

Es la tabla por defecto, esta se encarga de filtrar únicamente los paquetes y contiene las cadenas: INPUT, OUTPUT y FORWARD, (de entrada, salida y reenvió). Las cadenas son listas de reglas que sirven para marcar un conjunto de paquetes y cada una de ellas posee una función específica como se muestra en la siguiente tabla 4.

Tabla 4

Cadenas usadas en la tabla filter y su descripción

CADENAS	DESCRIPCIÓN
INPUT	Decide el destino de los paquetes entrantes localmente en el servidor.
OUTPUT	Se usa para filtrar paquetes que son generados localmente en el servidor con destinos externos, permite modificar el destino de los paquetes.
FORWARD	Se usa para decidir qué hacer con los paquetes que llegan a una interfaz y tienen como destino otra.

2.2.3.2 Tabla Nat

Esta tabla se refiere a los paquetes enrutados en un sistema de enmascaramiento, y trabaja de la siguiente forma; cuando un flujo de paquetes atraviesa la tabla el primer paquete es admitido y el resto se identifica automáticamente como parte del flujo, las cadenas usadas en esta tabla se muestra a continuación en la tabla 5.

Tabla 5
Cadenas usadas en la tabla nat

CADENA	DESCRIPCIÓN
PREROUTING	Altera los paquetes recibidos por medio de una interfaz de red al momento de llegar.
OUTPUT	Se encarga de alterar los paquetes generados localmente antes de ser enviados por una interfaz.
POSTROUTING	Esta cadena altera los paquetes antes de que sean enviados a través de una interfaz.

2.2.3.3 Tabla Mangle

La tabla MANGLE marca los paquetes entrantes generados localmente, esta marca permite un tratamiento específico para dichos paquetes, además tiene la función de modificar los paquetes y sus cabeceras como el TTL (Time To Life/ tiempo de vida) y el TOS (Type Of Service/ Tipo De Servicio), la tabla MANGLE usa las siguientes cadenas que se muestran en la tabla 6.

Tabla 6
Cadenas usadas en la tabla Mangles

CADENA	DESCRIPCIÓN
PREROUTING	Esta se encarga de alterar los paquetes entrantes antes de ser enviados o enrutados.
OUTPUT	Esta cadena altera los paquetes generados localmente antes de ser enviados por medio de una interfaz.

2.2.3.4 Tabla Raw

Es una tabla nueva y se utiliza para configurar excepciones en el rastreo de paquetes en conjunto con la única acción o target NOTRACK, en la mayoría de Kernels no la incluyen a excepción que se encuentren parchados y trabaja con relación a las cadenas PREROUTING y OUTPUT que a continuación se muestra en la tabla 7.

Tabla 7

Cadenas usadas en la tabla raw

CADENA	DESCRIPCIÓN
PREROUTING	Para los paquetes que llegan a través de cualquier interfaz de red y para los paquetes generados por los procesos locales.
OUTPUT	

2.2.4 Reglas

Una regla de iptables se compone de uno o más criterios de coincidencia que determinan cual paquete de red es afectado (todas las opciones de comparación se deben cumplir por la regla para coincidir con un paquete) y una especificación de destino que determina como se verán afectados los paquetes de red.

El sistema mantiene los contadores de paquetes y bytes por cada regla. Cada vez que un paquete llega a una regla y coincide con los criterios de la regla, el contador de paquetes se incrementa, y el contador de bytes se incrementa por el tamaño del paquete coincidente.

Tanto la coincidencia y la porción de destino de la regla son opcionales. Si no hay criterios de coincidencia, todos los paquetes se consideran de igualar. Si no existe una especificación de destino, no se hace nada a los

paquetes (procesamiento procede como si la regla no hizo existir sino que los contadores de paquetes y bytes se actualizan).

2.3 SQUID

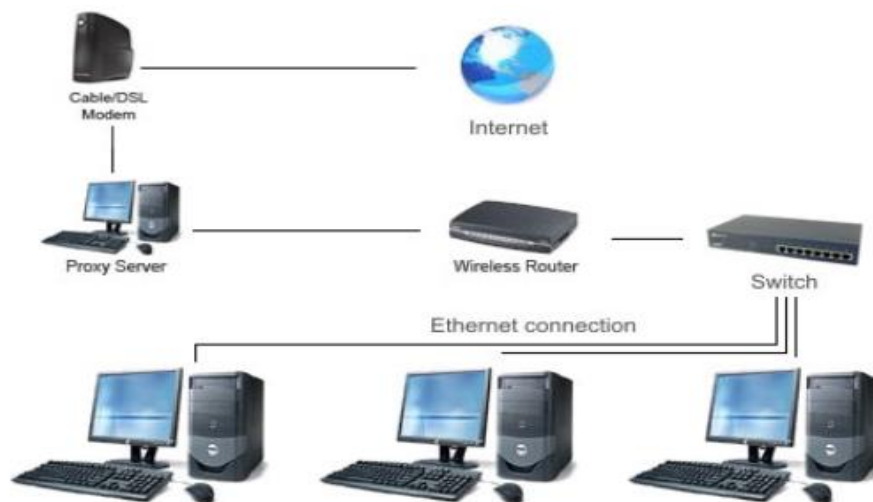
2.3.1 Concepto

Gracias a la robustez de Squid, se lo usa principalmente como servidor proxy para limitar el acceso a páginas web, descargas de archivos multimedia para no saturar el ancho de banda, restricción de redes e incluso restricción de direcciones IP específicas.

Posee una amplia variedad de utilidades, como acelerar un servidor web, guardando en caché peticiones repetidas a DNS (Domine Name System) y otras búsquedas para un grupo de usuarios que comparten recursos de la red, también caché de web, además de agregar seguridad filtrando el tráfico.

Squid está orientado principalmente a HTTP y FTP pero es compatible con otros protocolos como Internet Gopher. Además implementa algunas modalidades de cifrado como TLS, SSL, y HTTPS.

Squid está conformado por un programa principal como servidor, un programa para búsqueda en servidores DNS, programas opcionales para reescribir solicitudes y realizar autenticación y algunas herramientas para administración y herramientas para clientes. Al iniciar Squid da origen a un número configurable de procesos de búsqueda en servidores DNS, cada uno de los cuales realiza una búsqueda única en servidores DNS, tal como se indica la figura 2. (Dueñas, 2013).



**Figura 2 Esquema de uso de un proxy squid
(Rice, 2010)**

2.3.2 Características de Squid

Algunas de las principales características de Squid se presentan a continuación:

- Es un software libre que fue Liberado bajo la Licencia GNU General Public License (GPL)
- Soporta los protocolos IPv4 e IPv6.
- Soporta protocolos como TCP, UDP, ICP.
- Cache de contenido para aceleración web con soporte de diferentes sistemas de archivos para el almacenamiento del cache.
- Controles de acceso avanzados basados en ACL (Access Control List).
- Registro de Logs y soporte SNMP (Simple Network Management Protocol).
- Soporte de plugins para autenticación de usuarios y grupos.
- Integración de filtros de URL's y contenido como squidGuard y DansGuardian.

2.3.3 Squidguard

Es un sistema de filtrado web por listas negras, quiere decir que se tiene una gran lista de direcciones electrónicas y dominios a los que se les puede denegar o permitir acceso al usuario, debido a que se conoce que hay webs que contienen virus y todo tipo de malware también que hay páginas que se dedican a instalar spyware, además existen páginas que no son nada productivas en horario laboral, de modo que si se las conoce, se puede evitar que usuarios ingresen.

2.3.3.1 Características de Squidguard

- Liberado bajo la Licencia GNU General Public License (GPL).
- Controla el acceso a URL's para protocolos HTTP y HTTPS.
- Control basado en: Direcciones IP, Usuarios NCSA, Usuarios y Grupos LDAP, Usuarios y Grupos MySQL.
- Permite el uso de listas blancas para excluir sitios bloqueados (falsos positivos) por alguna categoría de lista negra.
- Permite re direccionar las peticiones denegadas a una página HTML informativa

2.3.4 Dansguardian

DansGuardian es una herramienta de código abierto desarrollada en C++, actúa como un filtro de contenidos de sitios web muy potente, este se sitúa o actúa entre el navegador cliente y el proxy, interceptando y modificando la comunicación entre ambos, también permite una configuración flexible adaptándose a las necesidades del usuario.

El mecanismo de funcionamiento de DansGuardian es el siguiente: los usuarios mediante navegadores web realizan peticiones de páginas que son recibidas por DansGuardian y solo son re direccionadas al servidor proxy SQUID aquellas que superen la fase de filtrado, ver figura 3.

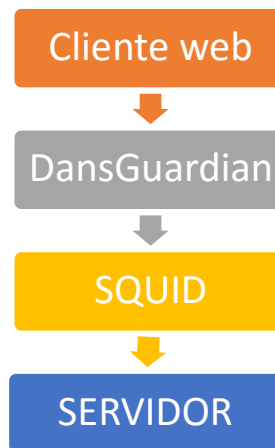


Figura 3 Mecanismo

2.3.4 Soporte de Squid

Squid provee soporte para los controles de accesos para los clientes basados en varios criterios de autenticación como:

- Direcciones IP: listas, rangos, subredes.
- Direcciones MAC: Solo redes locales.
- Usuarios y Grupos LDAP: OpenLDAP, Active Directory.
- Kerberos.
- RADIUS.
- Active Directory (Single Sign On).
- NTLM (Single Sign On).
- PAM (Linux).
- Horarios.

Además Squid brinda soporte robusto y extensible para controlar peticiones basadas en el destino y contenido, creando reglas para las siguientes:

- URL's destino, ejemplo: "http://porn.com/downloads/free/"
- Nombres de dominio DNS destino, ejemplo: "dl.fileshare.com"

- Direcciones IP, ejemplo: "http://18.1.3.22/downloads/"
- Expresiones regulares para las URL's destino, ejemplo: .mp3, .torrent, .rar, .avi.
- Tipos MIME para contenido multimedia: audio/mpeg, application/x-messenger, application/x-flv.
- Control de acceso para peticiones y respuestas HTTP: *POST*, *GET*.

2.3.5 Herramientas para Squid

Squid dispone de algunas herramientas para obtener información sobre las peticiones al proxy en tiempo real para realizar análisis de logs de acceso a Squid, a continuación algunas de estas herramientas:

2.3.5.1 Multitail

Multitail es un programa de línea de comando para la visualización de múltiples archivos de log en tiempo real, además posee el soporte de coloreado de logs basado en esquemas, multitail ya incluye el esquema de colores para los logs de acceso de squid. (Medina, 2012)

2.3.5.2 SquidView

Squidview es una interfaz en línea de comando para visualizar las conexiones activas del proxy squid, algunas de sus funcionalidades son: (Medina, 2012)

- Ver quién (usuario/host) se encuentra navegando en tiempo real.
- Que sitios/urls son los que se están visitando en el preciso momento.
- Ver el número de conexiones y ancho de banda consumido.

2.3.5.2 Sarg

SARG es una herramienta de análisis de logs de Squid Mediante los reportes de uso web: (Medina, 2012)

- Top Ten de sitios más visitados
- Reportes diarios, semanales y mensuales
- Accesos por usuarios
- Tiempos de navegación
- Descargas

2.3.5.3 Calamaris

Calamaris genera reportes y estadísticas del uso del proxy, además de poseer algunas características: (Medina, 2012)

- Reportes web y por correo.
- Total de peticiones realizadas al proxy.
- Total de usuarios que usan el proxy.
- Total de ancho de banda usado.
- Cantidad de peticiones en cache.
- Cantidad de ancho de banda ahorrado.
- Porcentaje de ancho de banda ahorrado.
- Otras estadísticas sobre dominios visitados, tipos de archivos descargados.

Al implementar un servidor proxy con sistemas GNU/Linux vinculado con el proxy cache squid y todos los demás sistemas permiten la implementación rápida, segura y económica al basarse en software libre y estándares abiertos, además de permitir que pueda ser modificado, extendido y mejorado para integrarlo con otros estándares para el filtrado de contenido web mediante la vinculación de plugins o interconexión con otros servicios o equipos de red basados en tecnologías y software libre y/o privativas.

2.4 SNORT

2.4.1 Concepto

Es un IDS o método de detección de intrusos en tiempo real, además es un instrumento de seguridad muy utilizada en Linux y Windows, con la cual se puede reforzar un equipo o red, implementa un mecanismo de detección de ataques de barrido de puertos que permite rastrear, prevenir y responder ante alguna irregularidad anticipadamente diagnosticada como muestras que sean determinados como ataques, intentos de explotar alguna debilidad en el sistema o red, y realiza un análisis de protocolos, además ilustra de forma muy clara las IP's que han intentado escanear en el equipo.

Snort es gratuito y trabaja con S.O. como Windows y UNIX, por ello es uno de los más utilizados, presenta una gran cantidad de herramientas de filtros o patrones que son ya predefinidos, una gran ventaja es que tiene actualizaciones constantes ante los casos de ataques que hayan sido detectadas a través de los distintos anuncios de seguridad. A continuación se describe una tabla 8 con las ventajas y desventajas de Snort.

Tabla 8

Ventajas y desventajas de un sistema SNORT

VENTAJAS	DESVENTAJAS
Una sub red completa puede ser cubierta por un IDS	No pueden analizar trafico cifrado
permiten detectar ataques DOS	Son tan efectivos como la última actualización de patrones
son livianos y fáciles de implementar	Dificultad para realizar análisis en redes saturadas
Pueden proveer información acerca de un ataque en tiempo real	Cuando la máquina "cae" también lo hace el IDS

Continua 

Pueden analizar tráfico cifrado	No indican si un ataque ha sido exitoso o no
---------------------------------	--

El mencionado IDS brinda un lenguaje para poder realizar reglas flexibles, robustas y simples. Al momento de su instalación este ya suministra muchos filtros o reglas de backdoor, ddos, finger, ftp, ataques web, escaneos NMap.

También puede actuar como sniffer de red ya que podría mostrar por consola en tiempo real lo que sucede en nuestro tráfico de red y como registro de paquetes ya que concede almacenar mediante un archivo todos los logs en registro de texto plano como en cualquier base de datos (MySQL, Oracle o PostgreSQL). Para luego realizar un análisis con posterioridad, o simplemente actúa como un NIDS ya que registra los paquetes sospechosos que traspasan en la red, para que esto suceda Snort emplea unos ficheros de configuración que permiten a los ficheros de firmas o reglas cual van a ser utilizado para determinar si un paquete se debe considerar sospechosos o no. A continuación se muestra en la figura 4 la arquitectura de Snort.

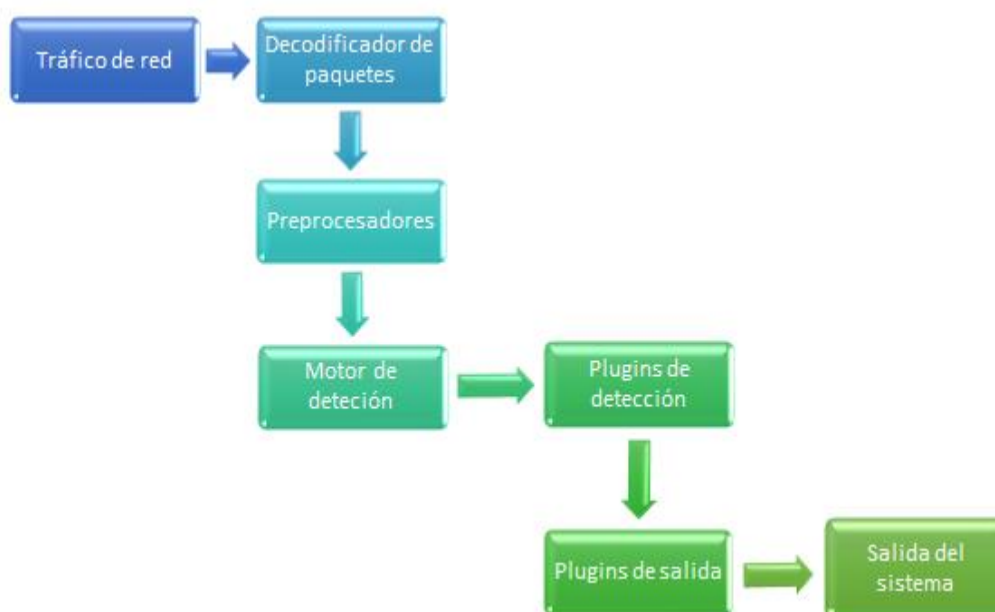


Figura 4 Arquitectura de snort

2.4.2 COMPONENTES DE SNORT

Los elementos que componen el esquema básico de la arquitectura de Snort son:

- Decodificador de paquetes.
- Preprocesadores.
- Motor de detección.
- Módulo de captura de datos.
- Archivo de reglas.
- Plugins de detección.
- Plugins de salida.

2.4.2.1 Decodificador de paquetes

Es el componente que se ocupa de tomar los paquetes de diferentes interfaces de red para luego procesarlos o enviarlos inmediatamente al motor de detección, utilizando la librería libcap para almacenarlos en una estructura de datos en la que se basan el resto de capas de la pila de protocolos actuales en las descripciones de los protocolos de Enlace de Datos y TCP/IP.

Cuando los paquetes son obtenidos, Snort descifra los componentes de un protocolo en particular para cada uno de los paquetes. El decodificador de paquetes es en sí una sucesión de decodificadores, es por eso que cada uno de ellos descifra los componentes de protocolo específicos, esto funciona sobre la pila de protocolos de red los que empiezan con el bloque más bajo, los protocolos de la capa de Enlace de Datos, decodificando cada protocolo según la ascendencia en la pila de protocolos de red, como se muestra en la figura 5.

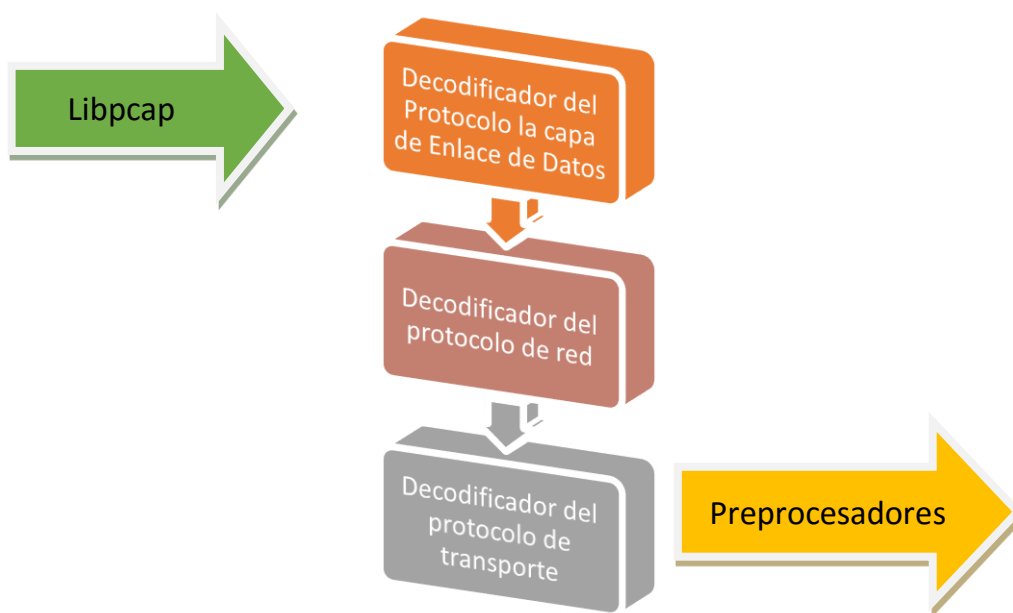


Figura 5 Flujo de datos del decodificador

2.4.2.2 Preprocesadores

Son los que conceden expandir las funcionalidades elaborando los datos para ser analizados para su detección contra reglas del motor. Existen algunos tipos de preprocesadores y estos dependen del tráfico que se desea analizar (preprocesadores http, telnet).

El protocolo TCP/IP está basado en capas y cada una de ellas tiene una tarea determinada y para que esta trabaje perfectamente precisa una información (cabecera). Los datos que viajan a través de la red perimetral en paquetes de manera individual casi siempre llegan a su destino final desorganizado y el destinatario se encarga de ordenar los paquetes y darles un sentido.

Snort lee todo el tráfico de red y lo interpreta, además de llevar un riguroso control en los paquetes que se envían mediante la red dándole un diseño a la información. Los preprocesadores son elementos de Snort que no necesitan de reglas ya que el conocimiento sobre el ataque depende del módulo preprocesador. Cuando llega un paquete se puede aplicar a este las reglas ya cargadas en Snort, por lo que toman la información que viaja por la

red de manera desordenada y brindarle forma para que esta información logre ser interpretada, una vez realizada dicha tarea se aplicaran las reglas (rules) para la búsqueda de una determinada amenaza.

2.4.2.3 Motor de detección

Examina mediante una comparación los paquetes de entrada según sea su tipo (TCP, UDP, ICMP o IP) en base a las reglas ya definidas para detectar los ataques y amenazas ya que este motor de detecciones se trata de la parte más esencial de Snort, actualmente se encuentra introducido en la versión 2.0 y necesita que Snort trabaje en redes Gigabyte, es por esto que se ha reescrito totalmente el motor usando algoritmos de búsqueda multipatrón.

Para cada prototipo de paquete existe un árbol RTN en el cual se encuentran reservadas las reglas del sistema, cuando un árbol RNT es elegido según el protocolo se recorren los nodos RNT relacionando con los parámetros de las reglas y una vez ubicado el grupo de reglas que coincide con este paquete se recorrerán los nodos OTN, donde se guardan los payloads de las reglas. Para definir si un nodo OTN pertenece al paquete recibido se busca relacionar el campo payload de la regla con los datos del paquete, luego de esto se determina si un texto se encuentra dentro de otro.

Los componentes que influyen en el tiempo de respuesta y en la carga del motor de detección son:

- Las características de la estación.
- Número de reglas determinadas.
- La carga en la red.

2.4.2.4 Módulo de captura de datos

Este se encarga de ejecutar la captura de todo el tráfico que va por la red perimetral, empleando enormemente los recursos de procesamiento y minimizando el extravío de paquetes a tasas de inyección elevadas.

Los preprocesadores y el motor de detección para la obtención de paquetes deben recurrir a una biblioteca de sniffing de paquetes externos como lo es Libpcap, ya que Snort no cuenta con obtención de paquetes propios, esta mencionada librería captura los paquetes directamente de la tarjeta de interfaz debido a su autodeterminación de la plataforma, el cual puede ser utilizada en varios sistemas operativos. Mediante esto existe una facilidad de la captura de “paquetes raw” determinados por el sistema operativo, el paquete raw trabaja en su forma original, sin modificación; tal cual como fluye en la red del cliente al servidor. El paquete raw lleva toda la información de cabecera de protocolo de salida íntegra y fija por el S.O. que para descifrar la información del protocolo y remitir los datos de carga más convenientes correctamente. Snort utiliza la información de cabecera del protocolo, la cual fue retirada por el sistema operativo para detectar ciertas formas de ataques.

2.4.2.5 Archivo de reglas

Las reglas o firmas es el modelo que se busca dentro de los paquetes de datos, estas son usadas por el motor de detección para relacionar los paquetes recibidos y difundir las alertas en caso de haber similitud entre el contenido de los paquetes y las firmas

2.4.2.6 Plugins de detección

Son los componentes del software, los cuales son compilados con la herramienta Snort y se utilizan para cambiar el motor de detección.

2.4.2.7 Plugins de salida

Son los que permiten definir qué alertas se guardan así como el lugar, la manera y los determinados paquetes de red que se generaron por el sistema de login y alerta de Snort, estos pueden ser archivos de texto, bases de datos, servidores syslog, ect.

A continuación se muestra en la tabla 9 los módulos de Salida de Snort.

Tabla 9
Módulos de Salida de Snort

NOMBRE	DESCRIPCIÓN
Syslog	Envía las alarmas al syslog
Alert_Fast	Muestra información sobre el: tiempo, mensaje de alerta, clasificación, prioridad de la alerta, IP, puerto de origen y destino.
Alert_Full	Muestra información sobre el: tiempo, mensaje de alerta, clasificación, prioridad de la alerta, IP, puerto de origen/destino e información completa de la cabecera de los paquetes registrados.
Alert_smb	Permite a Snort realizar llamadas al cliente de SMB y enviar mensajes de alerta a hosts Windows (WinPopUp).
Alert_Unixsock	Manda las alertas a través de un socket, para que las escuche otra aplicación.
Log_tcpdump	Guarda los paquetes que han generado las alertas en el formato tcpdump.
Database	Snort admite directamente cuatro tipos de salida a base de datos: MySQL, PostgreSQL, Oracle y unixODBC. El módulo de salida de base



Continua

	de datos requiere parámetros y configuraciones, dentro del archivo de configuración y en tiempo de compilación.
CSV	El plugin de salida CSV permite escribir datos de alerta en un formato CSV fácilmente importable a una base de datos.
Unified	Es un formato binario básico para registrar los datos y usarlos en el futuro. Los dos argumentos admitidos son filename y limit.
Log Null	A veces es útil ser capaz de crear las reglas que provocarán alertas sobre ciertos tipos de tráfico, pero no causarán entradas en los archivos de log.
Eventlog	Registra las alertas para visualizarse a través del visor de sucesos de un sistema Windows. Esta opción es solo válida sólo para Windows.

2.4.3 Personalización de reglas de snort

El lenguaje usado es flexible y potente dentro de Snort y existen reglas que son utilizadas por el motor de detección para relacionar los paquetes obtenidos y producir las alertas en caso de existir similitud en el contenido de los paquetes mencionados y las firmas. Existe un archivo llamado "Snort.conf" el cual admite agregar o quitar clases enteras de reglas. Al final de este archivo se puede visualizar todos los conjuntos de reglas de alertas, las cuales se pueden detener comentando la línea.

Snort admite mucha diversidad para agregar nuevas reglas. También se puede modificar nuestras reglas minimizando los falsos positivos, el planteamiento de todo esto es generar nuevas reglas avanzadas, en relación a los servicios que van a ser monitorizados.

2.4.3.1 Estructura de una regla

Las reglas de Snort deberán escribirse en una sola línea, si esto no sucede se debe que usar el carácter de escape (\).

Estas reglas se pueden dividir en dos secciones lógicas: cabecera de la regla y opciones.

- La cabecera abarca la operación de la regla en sí, protocolo IP, máscaras de red, puertos origen/destino y destino del paquete o dirección de la operación.
- Las opciones comprenden los mensajes y la información indispensable para la resolución tomada por parte de la alerta en manera de opciones.

2.4.3.2 Cabecera de una regla

La cabecera permite determinar el origen y destino del mensaje y sobre esta información efectúa una determinada acción. La estructura de la cabecera de una regla está compuesta por:

- **Acción de la regla:** alert
- **Protocolo:** tcp
- **Dirección IP origen:** \$EXTERNAL_NET (toda la red)
- **Puerto IP origen:** any (cualquiera)
- **Dirección IP destino:** \$HOME_NET (toda nuestra red)
- **Puerto IP destino:** any (cualquiera)
- **Dirección de la operación:** -> (puede ser ->, <-,)

2.5 NESSUS

2.5.1 Concepto

Nessus es un sistema de aplicación de escaneo de vulnerabilidades, que es utilizado para grandes redes, ya que actúa en todo tipo de máquinas, con la mayoría de sistemas operativos y con todo tipo de servicios. Por ser software libre, hace que sea muy adecuado para el presupuesto de seguridad desde un equipo pequeño hasta un gran servidor de una empresa corporativa debido a su fiabilidad.

Nessus empieza escaneando los puertos nmap con su mismo escáner de puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, así como los plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes. (Cesar Bastidas, 2012)

Nessus permite desarrollar auditorías en forma remota en una red perimetral para definir si la misma ha sido comprometida o utilizada de manera inapropiada.

A demás brinda la capacidad de controlar de forma local una estación determinada para el respectivo análisis de vulnerabilidades, definición de compatibilidad, abuso de directivas de contenido.

A continuación también se muestran los productos oficiales de Nessus:

- Nessus®
- Nessus Perimeter Service
- Nessus Auditor Bundles
- Nessus Home

2.5.2 COMPONENTES BÁSICOS

Lo que hace que Nessus sea una gran herramienta es la arquitectura única en el que se construye. La flexibilidad y el ingenio de la arquitectura de Nessus han tomado todos los elementos del ciclo de vida de la seguridad en consideración, la ejecución de lotes a gran escala de análisis de vulnerabilidad que capturan los datos, informes gráficos e hipervínculos que representan los datos, las descripciones de arreglos que son invaluable en la remediación de parche, todos estos aspectos crean los cimientos de una postura de seguridad confiable. Los componentes de esta arquitectura son:

- El cliente y servidor (Client/Server)
- Los plugins
- La base de datos actualizada de vulnerabilidades.
- Informes completos

2.5.2.1 Nessus cliente y servidor

Esta arquitectura cliente/servidor proporciona la suficiente flexibilidad para implementar el analizador (servidor) y conectarse con la interfaz general de usuario (cliente) desde cualquier explorador web, de este modo se reducen costos de administración ya que varios clientes pueden acceder a un único servidor.

Nessus adopta un modelo cliente/servidor para su ejecución. Esto permite que el analista de seguridad se desprenda de la exploración de vulnerabilidades mientras Nessus siga haciendo su tarea.

Pero esto es solo un beneficio más respecto a las ventajas que propone esta estructura cliente/servidor para un analizador de vulnerabilidades. Otro aspecto importante es que se encuentra relacionado con la escalabilidad que brinda justamente este tipo de arquitectura en la cual al mejorar las

características de potencia de la porción servidor, se mostrara un incremento directamente proporcional respecto de la velocidad con la que serán llevadas a cabo las tareas de análisis.

2.5.2.2 Los plugins

Cada test de seguridad está compuesta como plugin externo, y se agrupa en una de 42 familias. De esta manera, se puede incluir fácilmente las pruebas, es decir seleccionar plugins específicos o elegir una familia entera de modo que no se tendrá que leer el código del motor de servidores Nessus. La lista completa de plugins de Nessus se encuentra disponible en la página web oficial de Nessus.

2.5.2.3 La base de datos actualizada de vulnerabilidades

Tenable quien diseña la mayoría de los plugins, especifica su desarrollo en comprobaciones de seguridad correspondientes a vulnerabilidades actualizadas y divulgadas. La base datos de comprobaciones de seguridad se actualiza diariamente, además Tenable deja a disposición todas las comprobaciones de seguridad más recientes en la página web: <http://www.nessus.org/scripts.php>.

2.5.2.3 Informes completos

Nessus proporciona informes completos acerca de las vulnerabilidades de seguridad que existen en su red y además les da un valor dependiendo del riesgo que presente cada amenaza en el siguiente orden:

- Low (bajo riesgo)
- Medium (mediano riesgo)
- High (alto riesgo)

- Critical (riesgo critico)

Además de informar el riesgo de la vulnerabilidad de la red también Nessus proporciona información de cómo mitigar dichas amenazas es decir ofrece soluciones a estos problemas.

2.5.3 Descripción general de la interface de usuario de Nessus

Nessus posee una interfaz de usuario web del analizador Nessus que está conformado por un servidor HTTP y cliente web, de modo que no requiere de ningún otro programa además del servidor Nessus. La misma base de código son usadas por todas las plataformas, gracias a esto se eliminan la mayor parte de errores específicos de las plataformas ya que se permite una complementación más rápida de nuevas características, algunas de las características principales se muestran a continuación:

- Generación de archivos de tipo .nessus que pueden ser usados por los productos de Tenable como estándar para directivas de análisis y datos de vulnerabilidad.
- Implementa una sesión de directivas, una lista de destinos y los resultados de los análisis se pueden almacenar todos juntos en un único archivo de extensión .nessus estos se pueden exportar con facilidad.
- La interface de usuario expone los resultados de los análisis en tiempo real, de modo que no se espera a que se dé por finalizado el análisis para poder observar los resultados.
- El analizador Nessus posee una interfaz unificada que es independiente de la plataforma base, existen iguales funcionalidades en Mac OS X, Windows y Linux.
- Si por algún motivo el usuario se desconectara los análisis seguirán ejecutándose en el servidor.
- Nessus puede cargar los informes de los análisis gracias a su interface de usuario y así comparar con otros informes.

- Se puede contar con un asistente de directivas de esta manera le puede ayudar a crear rápidamente directivas de análisis eficientes para poder auditar una red.

2.5.4 Plataformas admitidas

Gracias a la interface de usuario de Nessus que es un cliente web, esta puede ser ejecutada en todas las plataformas mediante un explorador web actual. Cabe mencionar que como requisito mínimo Nessus puede ser ejecutado desde Microsoft Internet Explorer 9, y se puede lograr una óptima ejecución si se usa los siguientes navegadores:

- Microsoft Internet Explorer 10
- Mozilla Firefox 24
- Google Chrome 29
- Opera 16
- Apple Safari 6

También puede usarse en dispositivos móviles con los siguientes navegadores:

- Chrome 29 (para Android)
- Safari (IOS 7)

2.5.5 Descripción general de directivas

Una directiva de Nessus se conforma por opciones de configuración que estén relacionadas con la ejecución de un análisis de vulnerabilidades. Entre estas alternativas se incluyen las siguientes:

- Parámetros que verifican aspectos técnicos del análisis, tales como tiempos de espera, cantidad de hosts, tipo de analizador de puertos, etc.

- Credenciales para análisis locales (por ejemplo, Windows, SSH), análisis de bases de datos Oracle autenticados, autenticación basada en HTTP, FTP, POP, IMAP o Kerberos.
- Especificaciones de análisis pormenorizados en función de plugins o familias.
- Comparaciones de directivas de compatibilidad de bases de datos, nivel de detalle de los informes, configuración de los análisis para la detección de servicios, comprobaciones de compatibilidad de Unix, etc.

CAPÍTULO 3

INSTALACIÓN Y CONFIGURACIÓN

3.1 ZENTYAL

Zentyal es una herramienta que permite administrar servicios de red a través una sola aplicación, puede actuar como Gateway, Servidor de seguridad (UTM), Servidor de oficina, Servidor de infraestructura de red y Servidor de comunicaciones.

3.1.1 Instalación de Zentyal

Zentyal fue preparado para ser instalado en una máquina (real o virtual) de forma exclusiva. Esto no impide que se pueda instalar cualquier otro servicio o aplicación adicional, no gestionado a través de la interfaz de Zentyal, que deberá ser instalado y configurado manualmente.

La instalación puede realizarse de las siguientes formas:

- Utilizando el instalador de Zentyal (opción recomendada).
- A partir de una instalación de Ubuntu Server Edition.

En el segundo caso se requiere añadir los repositorios oficiales de Zentyal y tras actualizar los paquetes disponibles, se procede a la instalación de aquellos módulos que se deseen.

Utilizando el instalador de Zentyal es más sencillo la instalación y despliegue de Zentyal, ya que todas las dependencias se encuentran en un sólo CD o USB y además se incluye un entorno gráfico que permite usar el interfaz web desde el propio servidor.

1. En primer lugar se selecciona el idioma, lo cual en dicho caso será el español como se muestra a continuación en el figura 6.

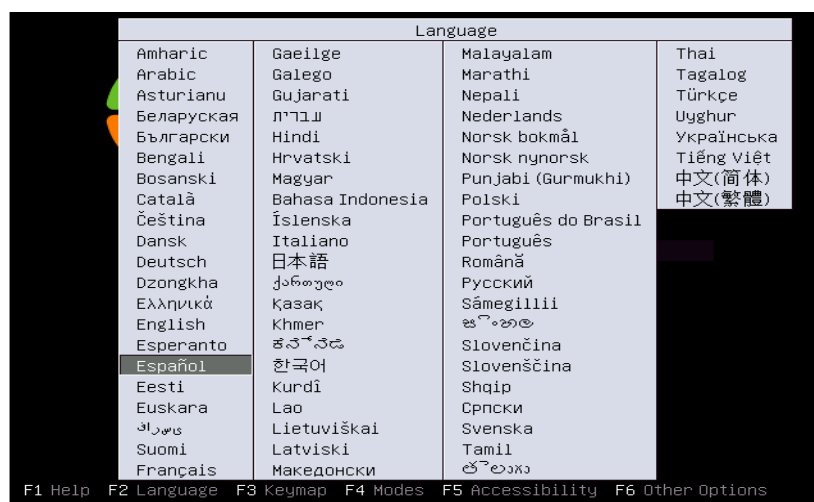


Figura 6 Selección de idioma

2. Se puede instalar usando la opción por omisión que elimina todo el contenido del disco duro y crea las particiones necesarias para Zentyal usando LVM (logical volumen manager) se puede seleccionar la opción expert mode que permite realizar un particionado personalizado. La mayoría de usuarios deberían elegir la opción por omisión a no ser que requieran instalar en un servidor con RAID por software o se necesite realizar un particionado más específico a necesidades concretas, tal como se muestra en el figura 7.



Figura 7 Inicio del instalador de zentyal

3. Se puede usar la detección automática de la distribución del teclado, que hará unas cuantas preguntas para asegurarse del modelo que se encuentra usando o se puede seleccionar manualmente escogiendo la opción (no), como muestra el figuras 8 y 9.



Figura 8 Configuración del teclado

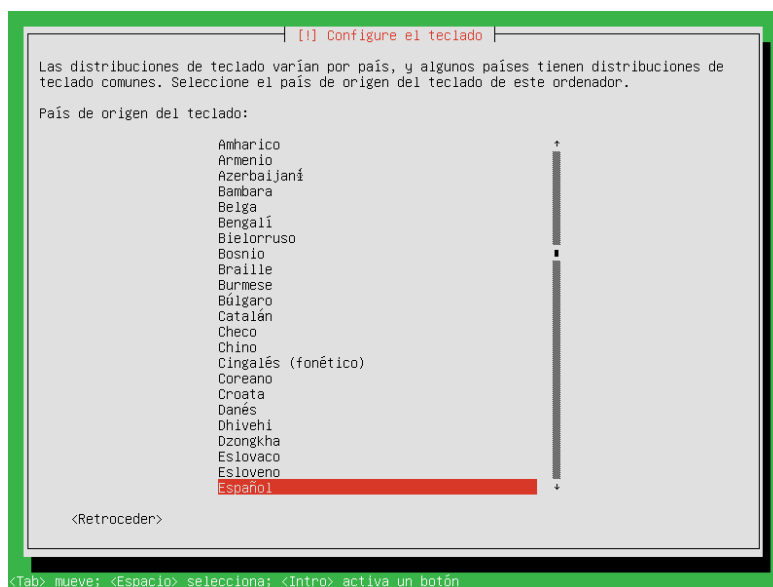


Figura 9 Selección del teclado

Sea el caso de que se disponga de más de una interfaz de red, el sistema preguntara cual se debe usar durante la instalación. Si solo se posee una, no habrá dicha pregunta, como se muestra en el figura 10.

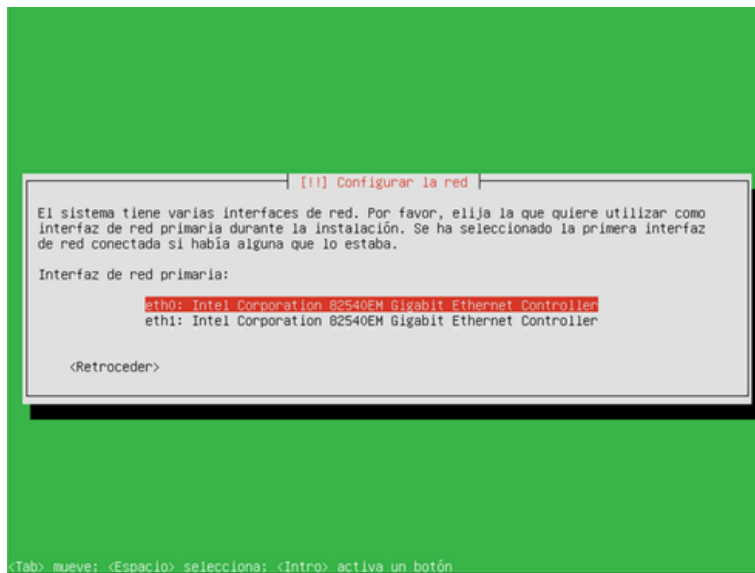


Figura 10 Configuración tarjetas de red

4. A continuación se selecciona un nombre para el servidor, el cual es de gran importancia para la identificación de la maquina dentro de la red. El servidor DNS registrará automáticamente dicho nombre, ver figura 11.

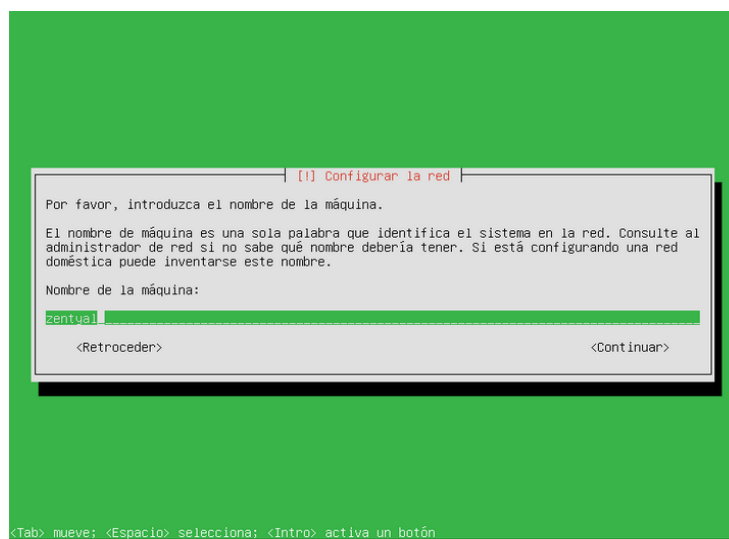


Figura 11 Nombre de la máquina

5. A continuación hay que indicar el nombre de usuario y contraseña usado para identificarse ante el sistema. Este usuario tendrá privilegios de administración el cual además será usado para acceder a la interfaz de Zentyal, ver gráfico 12.

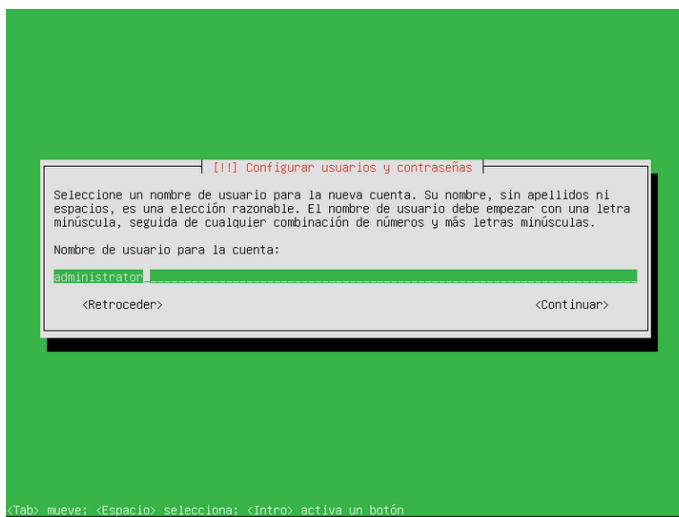


Figura 12 Nombre de usuario

6. Luego el sistema pedirá la contraseña para el usuario administrador. Cabe destacar que el anterior usuario con esta contraseña podrá acceder tanto al sistema como a la interfaz web de Zentyal, por lo que hay que tener cuidado en elegir una contraseña segura, ver gráfico 13.

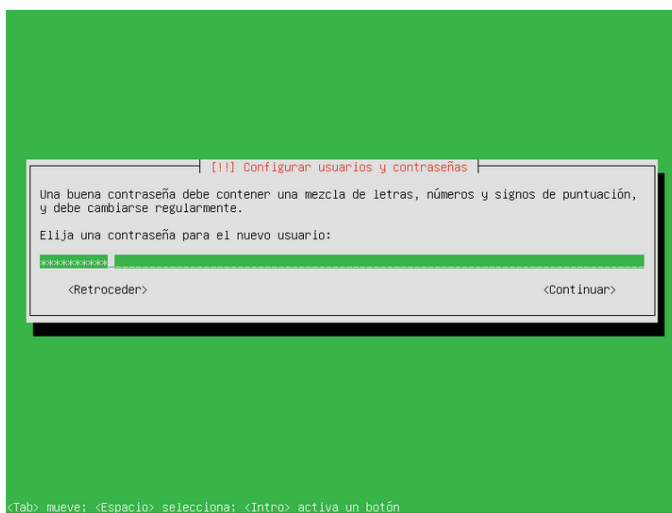


Figura 13 Ingreso de contraseña del usuario

7. Alrededor de unos 20 minutos el sistema básico se instalará mostrándose una barra de su progreso, el tiempo de progreso dependerá del servidor, ver figura 14.

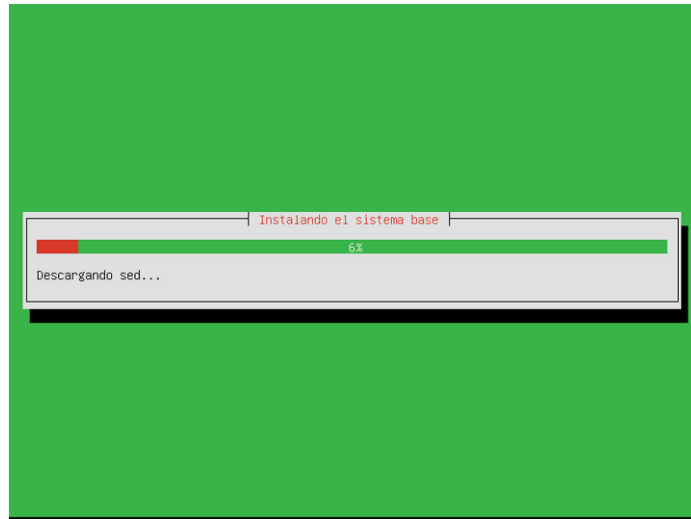


Figura 14 Progreso de la instalación

8. Una vez que se haya completado la instalación del sistema base, se puede continuar con la extracción del disco de instalación y reiniciar, ver figura 15.

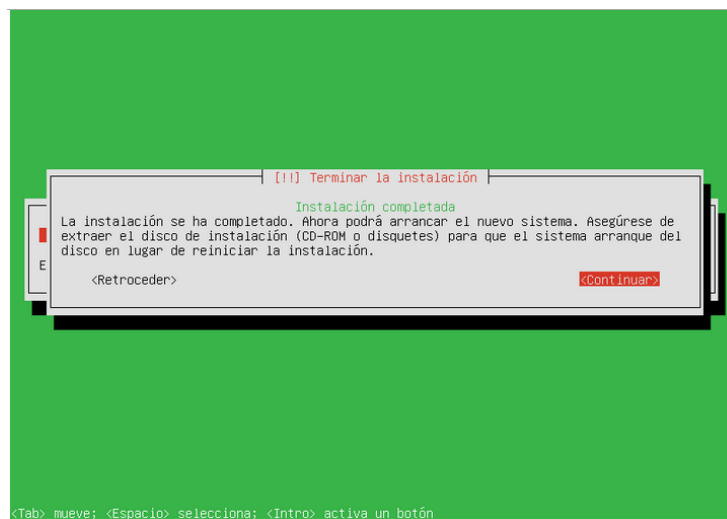


Figura 15 Finalización de la instalación

9. Al reiniciarse el sistema, arrancara en una interfaz gráfica con un navegador el cual permite acceder a la interfaz de administración; en este primer reinicio el sistema inicia la sesión de usuario automáticamente, pero posteriormente requerirá autenticarse antes de hacer login en el sistema, ver figura 16.

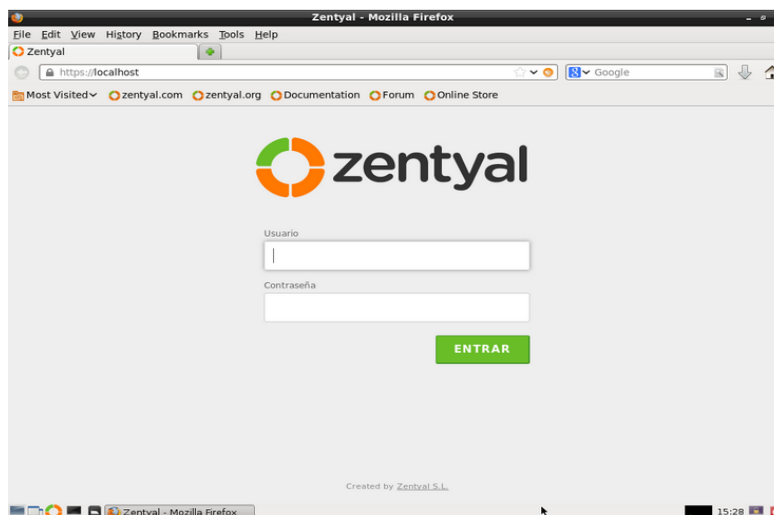


Figura 16 Entorno gráfico con la interfaz de administración

3.1.2 Configuración de Zentyal

Una vez que el usuario se haya autenticado por primera vez en la interfaz web comenzara un asistente de configuración, en primer lugar se podrá seleccionar qué funcionalidades se quiere incluir en el sistema.

Para simplificar nuestra selección, en la parte superior de la interfaz contamos con unos perfiles prediseñados, ver figura 17. Estos perfiles son simplemente conjuntos de paquetes relacionados por funcionalidad, no hay ningún problema en añadir o eliminar módulos más adelante. Los perfiles que ofrece Zentyal son los siguientes:

- **Zentyal Gateway:** Zentyal actúa como puerta de enlace de la red local ofreciendo un acceso a Internet seguro y controlado. Zentyal además protege la red local contra ataques externos, intrusiones,

amenazas a la seguridad interna y posibilita la interconexión segura entre redes locales a través de Internet u otra red externa.

- **Zentyal Infrastructure:** Zentyal administra la infraestructura de la red local con los servicios básicos: DHCP, DNS, NTP, servidor HTTP, entre otras.
- **Zentyal Office:** Zentyal interviene como servidor de recursos compartidos, dominios y directorio de usuarios de red local como ficheros, impresoras, calendarios, contactos, perfiles de usuarios y grupos.
- **Zentyal Unified Communications:** Zentyal se convierte en el centro de comunicaciones de la empresa, incluyendo correo, mensajería instantánea.



Figura 17 Perfiles y paquetes de zentyal

El sistema comenzará con el proceso de instalación de los módulos requeridos, mostrando una barra de progreso donde además se puede leer una breve introducción sobre las funcionalidades y servicios adicionales disponibles en Zentyal Server y los paquetes comerciales asociados.

El sistema solicitará información sobre la configuración de red, definiendo para cada interfaz de red si es interna o externa, es decir, si va a ser utilizada para conectarse a Internet u otras redes externas, o bien, si está conectada a la red local.

Posteriormente, se puede configurar el método y parámetros de configuración (DHCP, estática, IP asociada, etc.). Si existiera error en cualquiera de estos parámetros no es crítico dado que se los puede modificar desde el interfaz de Zentyal en cualquier otro momento.

A continuación ya se puede acceder al DASHBOARD, ver figura 18 y 19.

Figura 18 Acceso al dashboard de zentyal 1

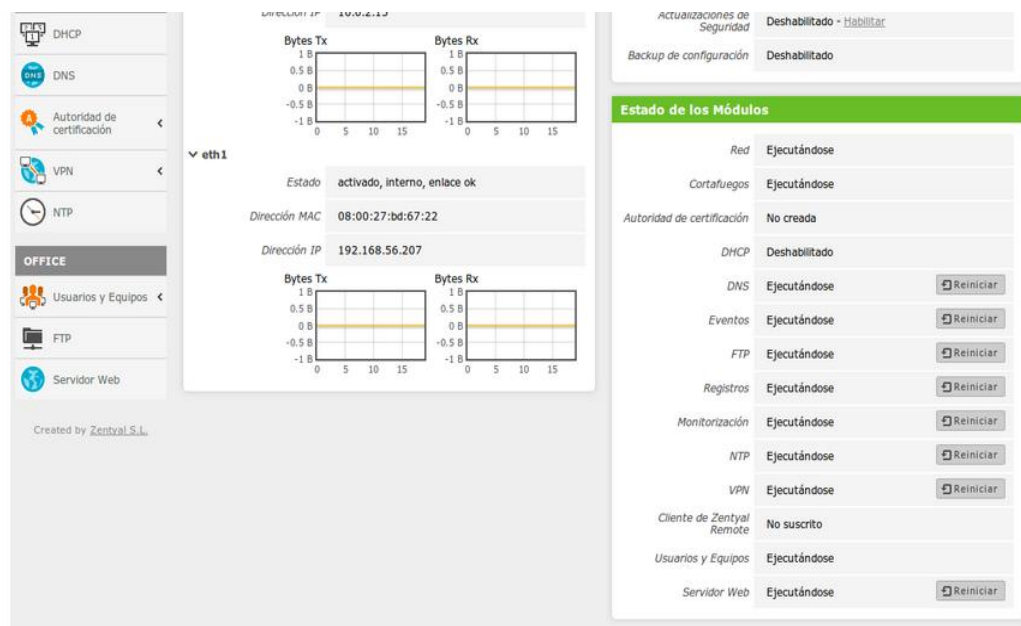


Figura 19 Acceso al dashboard de zentyal 2

3.2 Configuración de Squid en Zentyal

Zentyal utiliza Squid para proxy HTTP junto a Dansguardian para el control de contenidos y trabaja en un entorno gráfico, pero internamente posee archivos de configuración donde trabajan mediante comandos. A continuación se muestra la dirección donde está ubicado el archivo y el nombre del mismo.

`/etc/zentyal/squid.conf`

Dentro del mencionado archivo se puede observar líneas de comandos en un código de programación que visiblemente no se las puede observar, ya que al momento de configurar el paquete proxy, crear o modificar reglas de acceso en Zentyal se maneja en la interfaz gráfica.

Para la configuración del proxy HTTP se puede definir si va a realizarse en modo proxy transparente para exigir la política establecida o va ser de modo proxy manual, el puerto a ser utilizado es el 3128. El proxy solamente va aceptar conexiones que sean de las interfaces de redes internas. Dentro

del archivo de configuración por comandos se puede visualizar la siguiente línea:

```
http_port 3128
```

Se puede definir una capacidad para la memoria cache que va a ser utilizado en el disco temporalmente almacenando contenidos web, el administrador decide la capacidad ideal dependiendo de las características del servidor donde se ha instalado Zentyal y el tráfico en la red perimetral.

Una ventaja del proxy HTTP es que puede quitar anuncios de las páginas web, con lo cual mediante esto ahorrará ancho de banda y riesgos de confianza en algunos sitios web, para activar este servicio, se activará la opción bloqueo de anuncios, ver figura 20.

The screenshot shows the 'Proxy HTTP' configuration window in Zentyal. It is divided into several sections:

- Configuración General:** Contains several checkboxes: 'Proxy Transparente' (unchecked), 'Habilitar Single Sign-On (Kerberos)' (unchecked), and 'Bloqueo de Anuncios' (checked). Below the 'Bloqueo de Anuncios' checkbox is the text 'Quitar anuncios de todo el tráfico HTTP'. There are also input fields for 'Puerto' (set to 3128) and 'Tamaño de los ficheros de caché (MB)' (set to 100). A 'CAMBIAR' button is located at the bottom of this section.
- Excepciones en la caché:** A section with a '+ AÑADIR NUEVO/A' button.
- Excepciones en la Caché y Autorización:** Another section with a '+ AÑADIR NUEVO/A' button.
- Añadiendo un/a nuevo/a nombre de dominio:** A section for adding domain exceptions. It includes an input field for 'Dirección del nombre de dominio' (containing 'www.dominio.com') and a checked checkbox for 'Omitir Proxy Transparente'. 'AÑADIR' and 'CANCELAR' buttons are at the bottom.

Figura 20 Configuración general proxy

3.3 Analogía de Zentyal en el archivo Squid.conf

A medida que se va creando las reglas en la interfaz de Zentyal, se va generando una serie de código de programación en el archivo squid.conf, donde se encuentran los comandos del Squid nativo, a continuación se realizará la analogía entre la interfaz gráfica de zentyal y sus sentencias dentro del archivo mencionado:

- **Restricción de accesos por horarios**

Denegar el acceso en ciertos horarios permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple y consiste en denegar el acceso en horarios y días de la semana, ver figura 21.

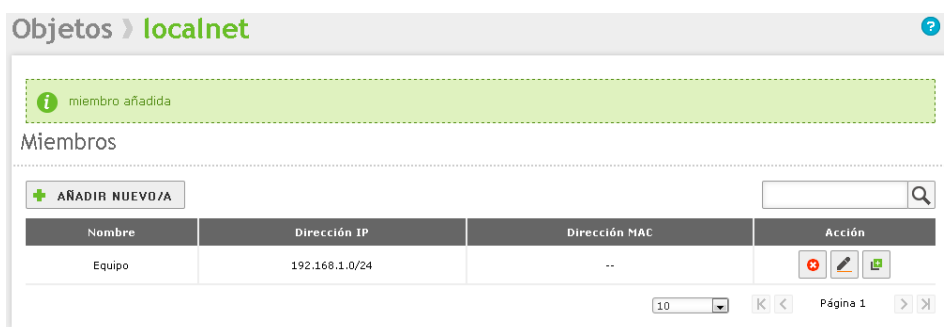


Figura 21 Creación del objeto localnet

Los días de la semana se definen con letras correspondiente al nombre en inglés:

- **S** - Domingo
- **M** - Lunes
- **T** - Martes
- **W** - Miércoles
- **H** - Jueves
- **F** - Viernes
- **A** - Sábado

La definición para el horario correspondería a:

```
acl localnet src 192.168.1.0/24
acl matutino time MTWHF 09:00-15:00
```

A continuación se visualizará en la figura 22 la definición de la regla de acceso.

Reglas de acceso

Añadiendo un/a nuevo/a regla

Período de tiempo | Período de tiempo en el cual se aplicará esta regla
 De Para Días de la semana L M X J V S D

Origen
 Objeto de red

Decisión
 Aplicar perfil de filtrado

Período de tiempo	Origen	Decisión	Acción
09:00-15:00 Días laborables	Objeto: localnet	Aplicar el perfil 'matutino'	<input type="button" value="✖"/> <input type="button" value="✎"/> <input type="button" value="📄"/>

Figura 22 Definición de regla de acceso

La definición de la Regla de Control de Acceso sería:

```
http_access allow matutino localnet
```

- **Restricción de acceso a contenidos por extensión**

Denegar el acceso a ciertos tipos de extensiones de archivo permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple y consiste en denegar el acceso a ciertos tipos de extensiones que coincidan con lo establecido en una Lista de Control de Acceso, ver figura 23.



Figura 23 Creación de las extensiones

En primer lugar se genera una lista, la cual contiene extensiones de archivos que se desean bloquear. Por ejemplo:

\.avi\$	\.rm\$	\.ace\$
\.mp4\$	\.wma\$	\.bat\$
\.mp3\$	\.wmv\$	\.exe\$
\.mp4\$	\.wav\$	\.lnk\$
\.mpg\$	\.doc\$	\.scr\$
\.mpeg\$	\.xls\$	\.sys\$
\.mov\$	\.mbd\$	\.zip\$
\.ra\$	\.ppt\$	\.rar\$
\.ram\$	\.pps\$	

La lista se genera en la siguiente ruta:
/etc/zentyal/squid/listas/extensiones.

Se define una lista de control de acceso que a su vez defina al archivo `/etc/zentyal/squid/listas/extensiones`. Esta lista se denomina como "extensiones". De modo tal, la línea correspondiente quedaría del siguiente modo:

```
acl extensiones urlpath_regex "/etc/zentyal/squid/listas/extensiones"
```

La definición para contenidos correspondería a:

```
acl localhost src 127.0.0.1/8
```

```
acl localnet src 192.168.1.0/24
```

```
acl extensiones urlpath_regex "/etc/zentyal/squid/listas/extensiones"
```

A continuación se muestra en la figura 24 la configuración que se ha realizado en las líneas de comando arribas mencionadas.

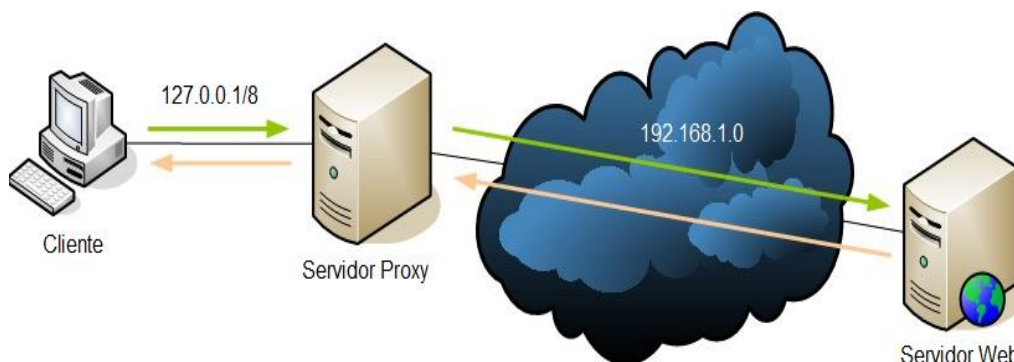


Figura 24 Diagrama de configuración de squid para la red perimetral

En la figura 25 se crea la regla de acceso al perfil extensiones.

Proxy HTTP

Reglas de acceso
















Editando regla

Período de tiempo | Período de tiempo en el cual se aplicará esta regla
 De 00:00 Para 00:00 Días de la semana L M X J V S D

Origen
 Objeto de red: localnet

Decisión
 Aplicar perfil de filtrado: extensiones

CAMBIAR **CANCELAR**

Período de tiempo	Origen	Decisión	Acción
Siempre	Objeto: localnet	Aplicar el perfil 'extensiones'	  
Siempre	Objeto: IT_Aula	Aplicar el perfil 'IT_PX_Denegadas'	  
Siempre	Objeto: IT_Invitados	Aplicar el perfil 'IT_PX_Invitados'	  
Siempre	Objeto: IT_Visitantes	Aplicar el perfil 'IT_PX_Visitantes'	  
Siempre	Cualquiera	Aplicar el perfil 'IT_PX_Internet_Limitado'	  




10   Página 1 

Figura 25 Creación de la regla de acceso al perfil extensiones

A continuación se especificará y modificará una Regla de Control de Acceso existente agregando con un símbolo de “!” que se denegará el acceso a la Lista de Control de Acceso denominada extensiones:

`http_access allow localnet !extensiones`

- **Restricción de acceso a sitios de internet**

Denegar el acceso a determinados sitios de red permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es simple y consiste en denegar el acceso a nombres de dominio o direcciones de internet que contengan patrones en común.

A continuación se crea la regla de acceso, la cual se le va a llamar dominios-denegados, ver figura 26.

Proxy HTTP

Perfiles de Filtrado

Añadiendo un/a nuevo/a Perfil de filtrado

Nombre

Figura 26 Acceso dominios-denegados

Una vez creada la regla, se puede configurar para poder utilizarla de acuerdo a las necesidades de bloqueo que se requiera, ver figura 27, 28 y 29.

Perfiles de Filtrado > dominios-denegados

Configuración Reglas de dominios y URLs Categorías de dominios Tipos MIME Extensiones de archivo

Umbral de filtrado de contenido

Umbral | Esto especifica cuan estricto es el filtro

Deshabilitado ▾

i No se puede activar el filtro antivirus porque el módulo antivirus no se ha instalado. Si desea filtrar los virus, primero debe instalarlo, luego [activar el módulo](#) y regresar aquí

Figura 27 Configuración de la regla de acceso dominios-denegados

Perfiles de Filtrado > dominios-denegados

Configuración **Reglas de dominios y URLs** Categorías de dominios Tipos MIME Extensiones de archivo

Configuración del filtrado de dominio

Bloquear dominios y URLs no listados
 Si esta opción está habilitada, cualquier dominio o URL que no esté en la sección *Reglas de dominios*, ni en *Ficheros de listas de dominios* debajo será prohibido.

Bloquear sitios especificados sólo como IP

CAMBIAR

Reglas de dominios y URLs

Añadiendo un/a nuevo/a dominio de internet o URL

Dominio o URL

Decisión

Figura 28 Creación de dominios que van a ser denegados

Perfiles de Filtrado > dominios-denegados

Configuración **Reglas de dominios y URLs** Categorías de dominios Tipos MIME Extensiones de archivo

Configuración del filtrado de dominio

Bloquear dominios y URLs no listados
 Si esta opción está habilitada, cualquier dominio o URL que no esté en la sección *Reglas de dominios*, ni en *Ficheros de listas de dominios* debajo será prohibido.

Bloquear sitios especificados sólo como IP

CAMBIAR

Reglas de dominios y URLs

	Dominio o URL	Decisión	Acción
<input type="checkbox"/>	youtube.com	Denegar	<input type="button" value="✖"/> <input type="button" value="✎"/>
<input type="checkbox"/>	twitter.com	Denegar	<input type="button" value="✖"/> <input type="button" value="✎"/>
<input type="checkbox"/>	facebook.com	Denegar	<input type="button" value="✖"/> <input type="button" value="✎"/>

Figura 29 Lista de dominios que van a ser denegados

Esta lista puede contener cualquier expresión regular que se considere sea usualmente utilizadas en las direcciones de ciertos sitios.

.facebook.com
 .twitter.com
 .youtube.com

La lista se genera en la siguiente ruta: /etc/zentyal/squid/listas/dominios-denegados.

Se añade una lista de control, denominada dominios-denegados, de acceso tipo **dstdomain** (dominios de destino), que define a la lista en el archivo /etc/zentyal/squid/listas/dominios-denegados.

```
acl dominios-denegados dstdomain "/etc/zentyal/squid/listas/dominios-denegados"
```

Se crea la regla de control de acceso que deniega el acceso a sitios que estén incluidos en la lista de dominios, ver figura 30.



Figura 30 Regla de control de acceso a dominios-denegados

```
http_access allow localnet !expreg-denegadas !dominios-denegados
```

- **Con soporte para direcciones MAC**

Como medida de seguridad y para especificar un equipo en común se puede bloquear mediante direcciones MAC, ver figura 31.

Objetos > macsredlocal

Miembros

Añadiendo un/a nuevo/a miembro

Nombre

Dirección IP
 /

Dirección MAC *Opcional*

Figura 31 Creación de la dirección mac

Se crea un archivo denominado: /etc/zentyal/squid/listas/macsredlocal.

Donde el contenido será una lista de direcciones MAC a la cual se aplicarán reglas de control de acceso, ver figura 32.

00:01:80:41:9C:8A

00:16:E3:9D:CD:77

00:08:A1:84:18:AD

Objetos > macsredlocal

Miembros

Nombre	Dirección IP	Dirección MAC	Acción
evillacis	192.168.4.11/32	00:01:80:41:9C:8A	<input type="button" value="✖"/> <input type="button" value="✎"/> <input type="button" value="📄"/>
hpadilla	192.168.4.13/32	00:16:E3:9D:CD:77	<input type="button" value="✖"/> <input type="button" value="✎"/> <input type="button" value="📄"/>
vortege	192.168.4.12/32	00:08:A1:84:18:AD	<input type="button" value="✖"/> <input type="button" value="✎"/> <input type="button" value="📄"/>

10

Figura 32 Miembros añadidos por mac

Se crea la lista de control de acceso denominada macsredlocal de tipo arp y cuyos elementos que la conforman están en el archivo /etc/zentyal/squid/listas/macsredlocal:

```
acl macsredlocal arp "/etc/zentyal/squid/listas/macsredlocal"
```

Se crea la regla de control de acceso que permite a los miembros de la lista de control de acceso hacer algo, ver figura 33.

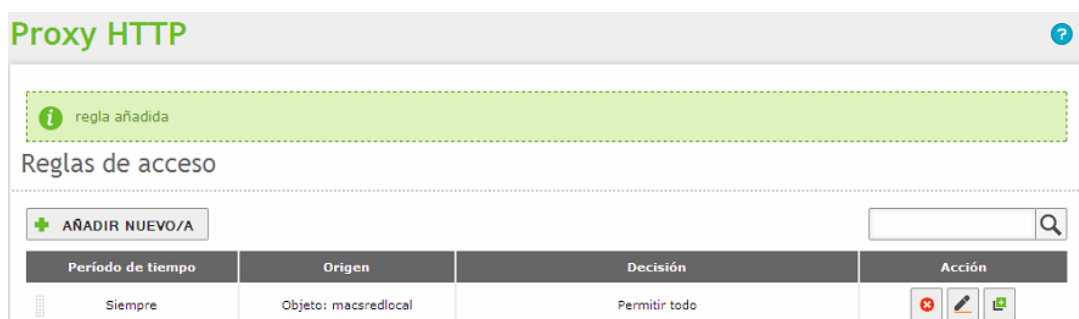


Figura 33 Regla de acceso para permitir el objeto macsredlocal

```
http_access allow macsredlocal
```

3.3 Configuración de firewall con Zentyal

Zentyal emplea para su módulo de cortafuegos el subsistema del kernel de Linux llamado Netfilter, este sistema proporciona funcionalidades de filtrado, permite definir reglas para gestionar el tráfico y redirección de conexiones.

La matriz de seguridad de Zentyal está basada en intentar proporcionar la máxima seguridad posible en su configuración predeterminada, procurando a la vez minimizar los esfuerzos a realizar después de añadir un nuevo servicio.

Cuando Zentyal interviene de cortafuegos, normalmente se instala entre la red interna y el router conectado a Internet. La interfaz de red que conecta la máquina con el router debe etiquetarse como interface externa para permitir al cortafuegos crear unas políticas de filtrado más estrictas para las conexiones procedentes de fuera, ver figura 34 y 35.

Interfaces de Red



The screenshot shows the configuration page for the network interface eth0. At the top, there are two tabs: 'eth0' (selected) and 'eth1'. Below the tabs, the 'Nombre' field contains 'eth0'. The 'Método' dropdown menu is set to 'Estático'. A checkbox labeled 'Externo (WAN)' is checked, with a tooltip that reads 'Marque aquí si está usando Zentyal como gateway y este interfaz está conetado a su router a Internet'. The 'Dirección IP' field contains '190.57.185.130' and the 'Máscara de red' dropdown menu is set to '255.255.255.252'. At the bottom, there is a 'CAMBIAR' button.

Figura 34 Interfaz externa de zentyal eth0

Interfaces de Red

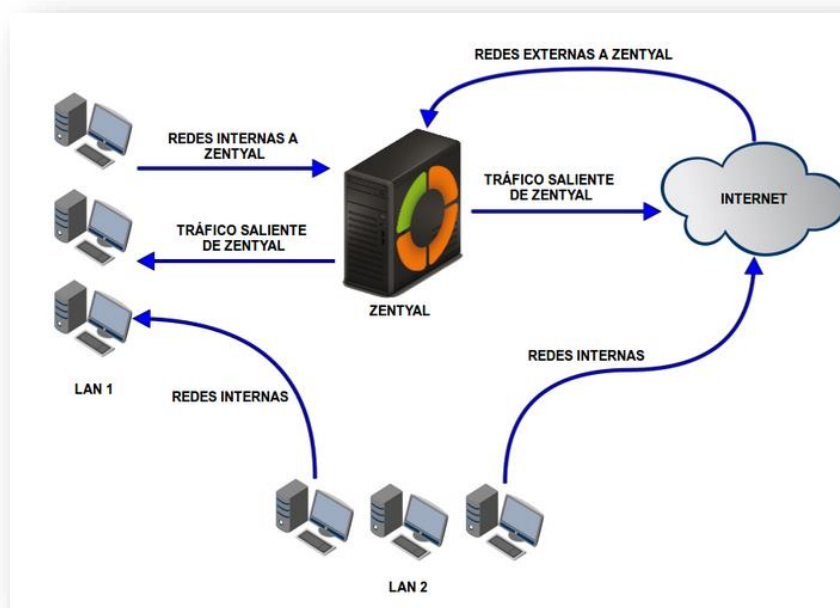


The screenshot shows the configuration page for the network interface eth1. At the top, there are two tabs: 'eth0' and 'eth1' (selected). Below the tabs, the 'Nombre' field contains 'eth1'. The 'Método' dropdown menu is set to 'Estático'. A checkbox labeled 'Externo (WAN)' is checked, with a tooltip that reads 'Marque aquí si está usando Zentyal como gateway y este interfaz está conetado a su router a Internet'. The 'Dirección IP' field contains '192.168.4.1' and the 'Máscara de red' dropdown menu is set to '255.255.255.0'. At the bottom, there is a 'CAMBIAR' button.

Figura 35 Interfaz externa de zentyal eth1

Por defecto la política para las interfaces externas es denegar todo intento de nueva conexión a Zentyal, mientras que para las interfaces internas se deniegan todos los intentos de conexión a Zentyal excepto los que se realizan a servicios definidos por los módulos instalados. Los módulos agregan reglas al cortafuegos para permitir estas conexiones, aunque siempre pueden ser cambiadas posteriormente por el administrador. La configuración predeterminada tanto para la salida de las redes internas como desde del propio servidor es permitir toda clase de conexiones.

La determinación de las políticas del cortafuegos se hacen desde el cortafuegos hacia el filtrado de paquetes, ver figura 36.



**Figura 36 Flujos de tráfico en el cortafuego
(S.L., 2014)**

Cada una de las secciones que se puede observar en el diagrama controla diferentes flujos de tráfico dependiendo del origen y destino, ver gráfico 37.

1. **Reglas de filtrado desde las redes internas a Zentyal.-** permite acceder al servidor de ficheros de Zentyal a los clientes de la red interna.
2. **Reglas de filtrado para las redes internas.-** restringe el acceso a Internet a ciertos clientes de la red interna, además impide que la red DMZ acceda a otros segmentos de la LAN.
3. **Reglas de filtrado desde la redes externas a Zentyal.-** permite que cualquier cliente en Internet tenga acceso a un servidor web desplegado en Zentyal.
4. **Guilabel (Reglas de filtrado para el tráfico saliente de Zentyal).-**
Son conexiones del proxy que se hacen por petición de un usuario interno.

Packet Filter



Figura 37 Reglas de filtrado del cortafuegos

Se debe tener en cuenta que admitir conexiones desde Internet a los diferentes servicios de Zentyal puede ser potencialmente peligroso, es































recomendable estudiar las implicaciones en la seguridad antes de modificar el tercer conjunto de reglas.

Zentyal proporciona una forma sencilla de definir las reglas que conforman la política de un cortafuego. La definición de estas reglas usa los conceptos de alto nivel introducidos anteriormente: los Servicios de red para especificar a qué protocolos y puertos se aplican las reglas y los Objetos de red para especificar sobre qué direcciones IP de origen o de destino se aplican, ver figura 38.

Filtrado de paquetes › Desde redes internas hacia Zentyal

Configurar reglas

[+ AÑADIR NUEVO/A](#) 🔍

Decisión	Origen	Servicio	Descripción	Acción
↑	Cualquiera	Samba	--	  
↑	Cualquiera	Kerberos	--	  
⊖	Cualquiera	LDAP	--	  
↑	Cualquiera	NTP	--	  
↑	Cualquiera	DNS	--	  
↑	Cualquiera	DHCP	--	  
↑	Cualquiera	TFTP	--	  
↑	Cualquiera	SSH	--	  
↑	Cualquiera	Administración Web de Zentyal	--	  
⊖	IT_Invitados	Nessus	--	  





10   Página 1  

Figura 38 Lista de reglas de filtrado de paquetes

Habitualmente toda regla posee un Origen y un Destino los cuales pueden ser Cualquiera, una dirección IP o un Objeto en el caso que se requiera especificar más de una dirección IP o direcciones MAC. En determinadas secciones el Origen o el Destino son suprimidos ya que su

valor es conocido a priori; será siempre Zentyal tanto el Destino en Tráfico de redes internas a Zentyal y Tráfico de redes externas a Zentyal como el Origen en Tráfico de Zentyal a redes externas.

Así mismo cada regla siempre tiene asociado un Servicio para especificar el protocolo y los puertos (o rango de puertos). Los servicios con puertos de origen son útiles para reglas de tráfico saliente de servicios internos, por ejemplo un servidor HTTP interno, mientras que los servicios con puertos de destino son útiles para reglas de tráfico entrante a servicios internos o tráfico saliente a servicios externos. Se debe destacar que hay una serie de servicios genéricos los cuales son muy útiles para el cortafuegos como Cualquiera para seleccionar cualquier protocolo y puertos, Cualquier TCP o Cualquier UDP para seleccionar cualquier protocolo TCP o UDP respectivamente.

El parámetro de mayor relevancia será la Decisión a tomar con las conexiones nuevas. Zentyal permite tomar tres tipos distintos de decisiones:

- Aceptar la conexión.
- Denegar la conexión ignorando los paquetes entrantes y haciendo suponer al origen que no se ha podido establecer la conexión.
- Registrar la conexión como un evento y seguir evaluando el resto de reglas.

Las reglas son introducidas en una tabla donde son evaluadas desde el principio hasta el final (desde arriba hacia abajo), una vez que una regla (ACEPTAR / DENEGAR) acepta una conexión, no se sigue evaluando el resto. Las reglas de REGISTRAR producen el registro, pero siguen procesando. Una regla genérica al principio, puede hacer que otra regla más específica posterior no sea evaluada. Es por esto por lo que el orden de las reglas en las tablas es muy importante. Existe la opción de aplicar un no lógico a la evaluación de miembros de una regla con Coincidencia Inversa para la definición de políticas más avanzadas, ver gráfico 39.

Añadiendo un/a nuevo/a regla

Decisión:

Origen: Coincidencia inversa:

Destino: Coincidencia inversa:

Servicio: Coincidencia inversa:

Si la selección inversa está marcada, la regla será aplicada cualquier servicio excepto el seleccionado

Descripción: Opcional

Figura 39 Creación de una nueva regla

Si se requiere registrar las conexiones a un servicio, primero se tiene la regla que registra la conexión y luego la regla que acepta la conexión. Si estas dos reglas están en el orden inverso, no se registrará nada ya que la regla anterior ya acepta la conexión. De igual forma, si se quiere restringir la salida a Internet, primero se deniega explícitamente los sitios o los clientes y luego se permitirá la salida al resto, invertir el orden daría acceso a todos los sitios a todos los hosts.

Por defecto, la decisión es siempre denegar las conexiones y tendremos que añadir reglas que las permitan explícitamente. Hay una serie de reglas que se añaden automáticamente durante la instalación para definir una primera versión de la política del cortafuegos: se permiten todas las conexiones salientes hacia las redes externas, Internet, desde el servidor Zentyal (en Tráfico de Zentyal a redes externas) y también se permiten todas las conexiones desde las redes internas hacia las externas (en Tráfico entre redes internas y de redes internas a Internet). Asimismo cada módulo instalado añade una serie de reglas en las secciones Tráfico de redes internas a Zentyal y Tráfico de redes externas a Zentyal normalmente permitiendo las conexiones desde las redes internas pero denegándolas desde las redes externas. Esto ya se hace implícitamente, pero facilita la gestión del cortafuegos puesto que de esta manera para permitir el servicio solamente hay que cambiar el parámetro Decisión y no es necesario crear

una regla nueva. Cabe destacar que estas reglas solamente son añadidas durante el proceso de instalación de un módulo por primera vez y no son modificadas automáticamente en el futuro.

Finalmente, existe un campo opcional que es descripción para comentar el objetivo de la regla dentro de la política global del cortafuegos.

3.3.1 Acceso ssh y registro de todas las conexiones

En primer lugar se debe crear una regla la cual permitirá el log de todas las conexiones ssh, ver figura 40.



The screenshot shows a web-based configuration interface for a firewall rule. The title is "Filtrado de paquetes > Desde redes externas hacia Zentyal". Below the title, it says "Editando regla". The configuration fields are: "Decisión:" with a dropdown menu set to "LOG"; "Origen:" with a dropdown menu set to "Cualquiera"; "Servicio:" with a dropdown menu set to "ssh" and an "Inverse match:" checkbox that is unchecked; and "Descripción:" with an empty text input field. Below the description field, there are two buttons: "Cambiar" and "Cancelar".

Figura 40 Acceso Log para redes externas

A continuación se debe crear una nueva regla la cual permitirá la entrada ssh y su respectivo registró desde las redes externas, ver figura 41.



The screenshot shows the same web-based configuration interface for a firewall rule. The title is "Filtrado de paquetes > Desde redes externas hacia Zentyal". Below the title, it says "Editando regla". The configuration fields are: "Decisión:" with a dropdown menu set to "ACCEPT"; "Origen:" with a dropdown menu set to "Cualquiera"; "Servicio:" with a dropdown menu set to "ssh" and an "Inverse match:" checkbox that is unchecked; and "Descripción:" with an empty text input field. Below the description field, there are two buttons: "Cambiar" and "Cancelar".

Figura 41 Edición de regla para servicio SSH

Finalmente se observarán todas las reglas de filtrado que se crearon, las cuales permitirán el log y el acceso a las conexiones SHH en Zentyal, ver figura 42.

Decisión	Origen	Servicio	Descripción	Action
	Cualquiera	ssh	--	
	Cualquiera	ssh	--	

Figura 42 Reglas para permitir el acceso a conexiones ssh

3.4 Instalación de servidor de correo virtual Zimbra Collaboration Suite

Para poder instalar Zimbra Collaboration Suite, se debe hacer una previa instalación de Centos, en este caso la versión es Centos 6.5.

3.4.1 Instalación de Zimbra Collaboration Suite en Centos

Una vez instalado Centos 6.5, se procede a prepararlo para la instalación de Zimbra, siguiendo esta serie de pasos:

- Reiniciar el equipo.
- En la ventana de bienvenido presionar el botón **adelante**.
- Deshabilitar el cortafuegos y presionar el botón **adelante**.
- Deshabilitar SELinux y presionar el botón **adelante**.

1. Antes de iniciar la instalación se debe editar el host, vim/etc/hosts y se cambiara la configuración de la siguiente manera en la configuración actual, ver figura 43.

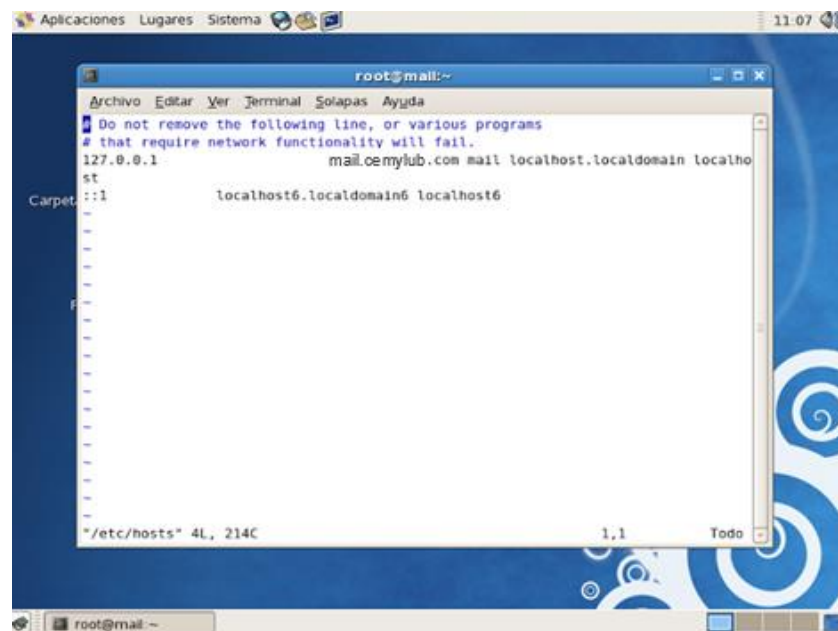


Figura 43 Edición del host en centos

2. A continuación se añade la dirección IP del servidor o equipo donde se va a instalar zimbra así como también el nombre del dominio, ver figura 44.

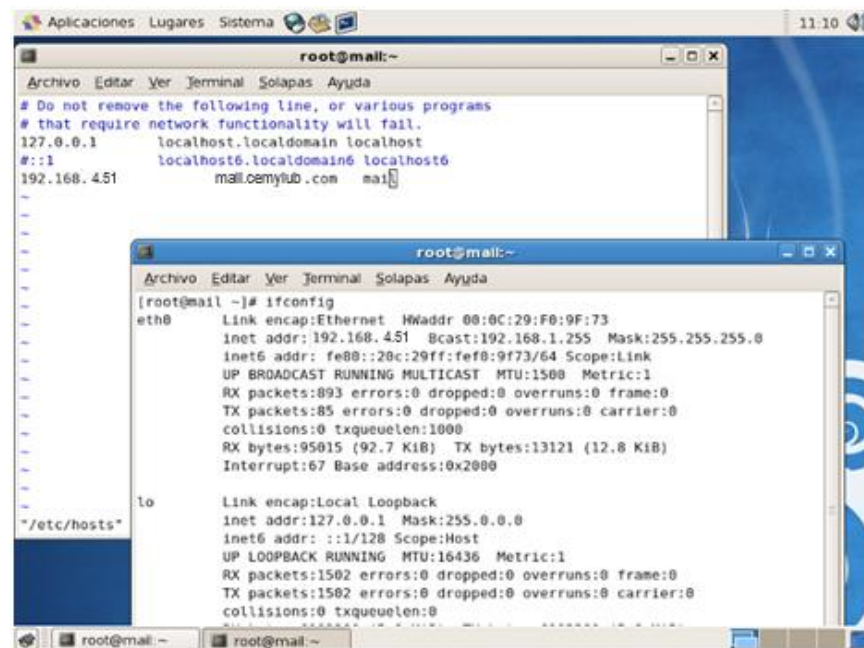
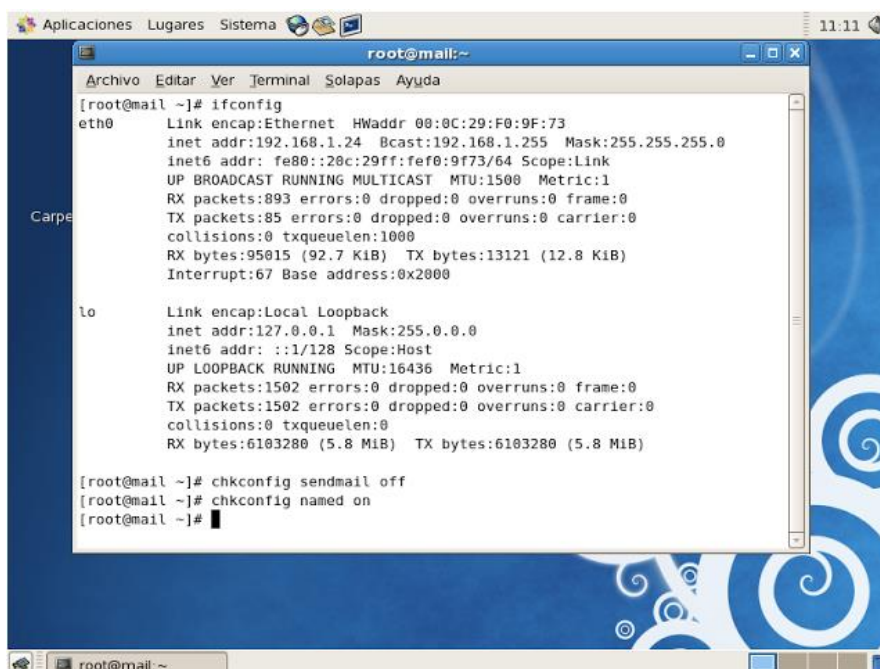


Figura 44 Edición de la dirección ip y dominio del equipo

3. Se verifica la dirección IP del servidor, a continuación se revisará que el servicio de sendmail y NFS no estén corriendo, de esta manera no creará un conflicto en el puerto 25, como se muestra a continuación en la figura 45.



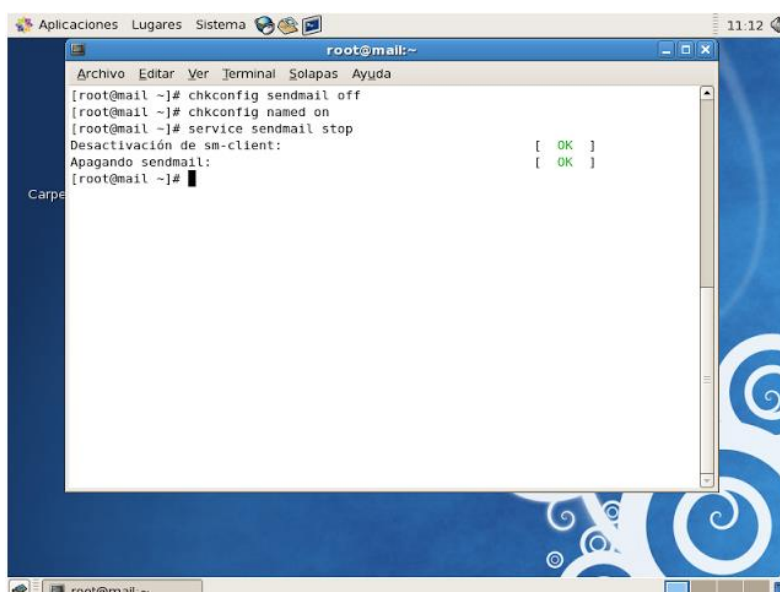
```
[root@mail ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F0:9F:73
          inet addr:192.168.1.24  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe0:9f73/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:893 errors:0 dropped:0 overruns:0 frame:0
          TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:95015 (92.7 KiB)  TX bytes:13121 (12.8 KiB)
          Interrupt:67  Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1502 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1502 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6103280 (5.8 MiB)  TX bytes:6103280 (5.8 MiB)

[root@mail ~]# chkconfig sendmail off
[root@mail ~]# chkconfig named on
[root@mail ~]#
```

Figura 45 Verificación de la dirección IP del servidor

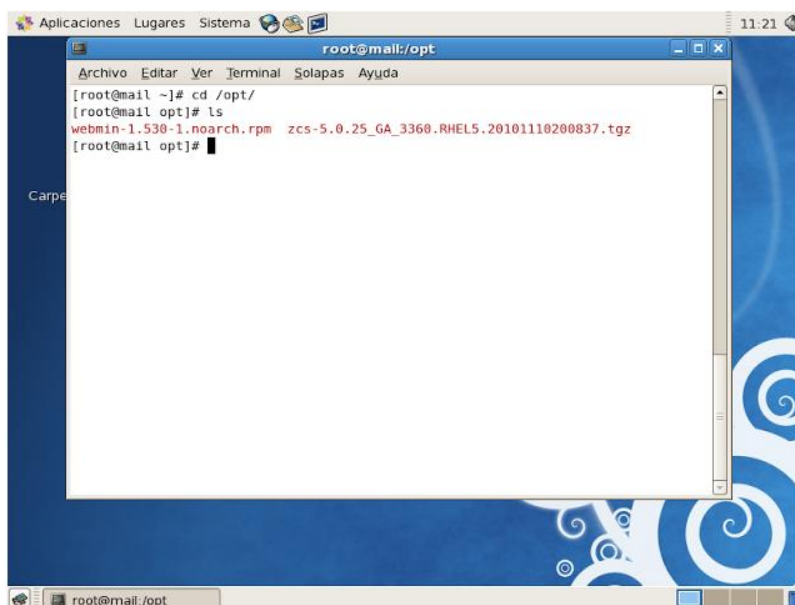
4. A continuación se preparan los servicios de sendmail, ver figura 46.



```
[root@mail ~]# chkconfig sendmail off
[root@mail ~]# chkconfig named on
[root@mail ~]# service sendmail stop
Desactivación de sm-client:           [ OK ]
Apagando sendmail:                    [ OK ]
[root@mail ~]#
```

Figura 46 Preparación de servicios de Sendmail

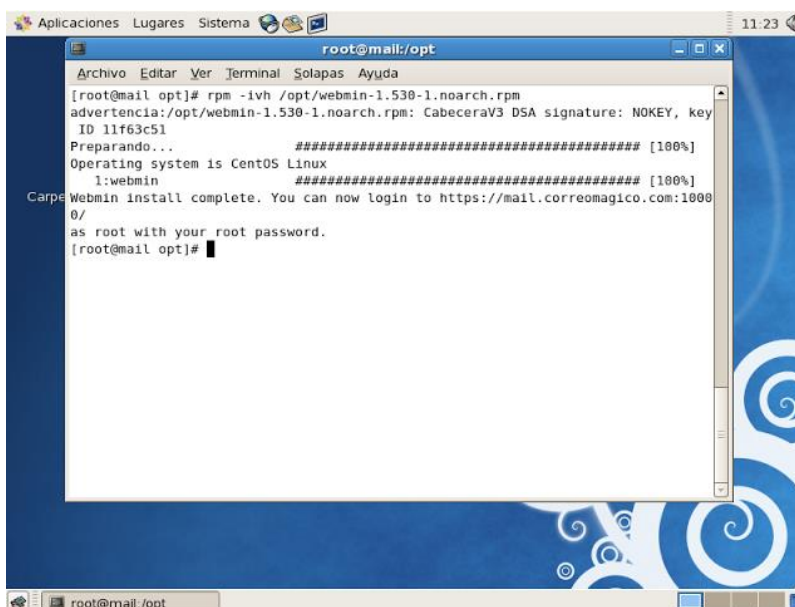
5. A continuación se debe copiar en la carpeta opt el webmin y el instalador de Zimbra que anteriormente fueron descargados, ver figura 47.

A terminal window titled 'root@mail:/opt' showing the execution of 'cd /opt/' and 'ls'. The 'ls' command lists two files: 'webmin-1.530-1.noarch.rpm' and 'zcs-5.0.25_GA_3360.RHEL5.20101110200837.tgz'.

```
root@mail:/opt
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@mail ~]# cd /opt/
[root@mail opt]# ls
webmin-1.530-1.noarch.rpm  zcs-5.0.25_GA_3360.RHEL5.20101110200837.tgz
[root@mail opt]#
```

Figura 47 Copia de archivos de instalación en OPT

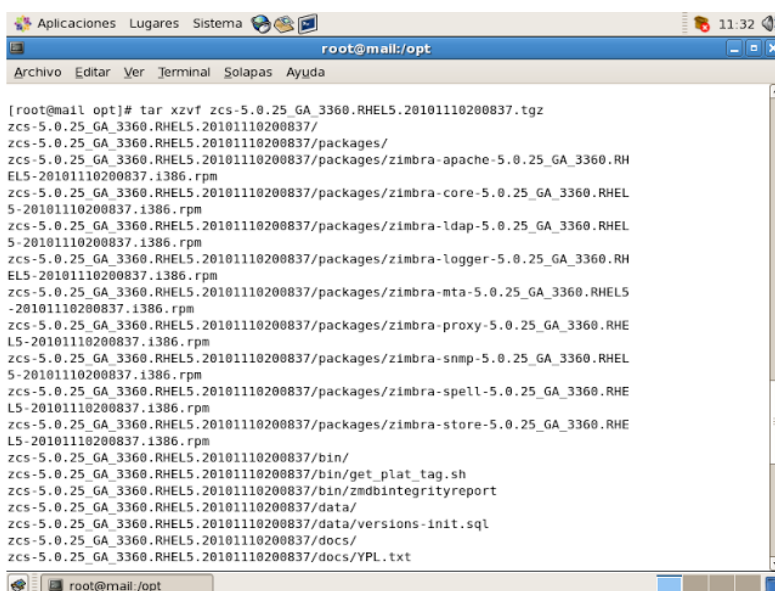
6. Se descomprime el webmin como se muestra, ver figura 48.

A terminal window titled 'root@mail:/opt' showing the execution of 'rpm -ivh /opt/webmin-1.530-1.noarch.rpm'. The output shows the installation progress, including a warning about a missing DSA signature, and the final message: 'Webmin install complete. You can now login to https://mail.correomagico.com:1000'.

```
root@mail:/opt
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@mail opt]# rpm -ivh /opt/webmin-1.530-1.noarch.rpm
advertencia:/opt/webmin-1.530-1.noarch.rpm: CabeceraV3 DSA signature: NOKEY, key
ID 11f63c51
Preparando... ##### [100%]
Operating system is CentOS Linux
1:webmin ##### [100%]
Webmin install complete. You can now login to https://mail.correomagico.com:1000
0/
as root with your root password.
[root@mail opt]#
```

Figura 48 Archivo webmin descomprimido

7. De la misma manera se descomprime el archivo instalador de zimbra, ver figura 49.



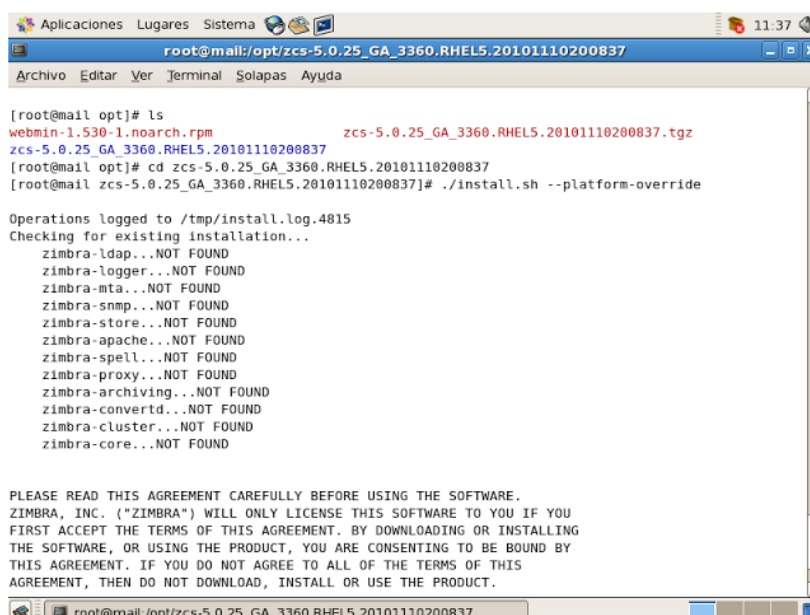
```

[root@mail opt]# tar xzvf zcs-5.0.25_GA_3360.RHEL5.20101110200837.tgz
zcs-5.0.25_GA_3360.RHEL5.20101110200837/
zcs-5.0.25_GA_3360.RHEL5.20101110200837/packages/
zcs-5.0.25_GA_3360.RHEL5.20101110200837/packages/zimbra-apache-5.0.25_GA_3360.RHEL5-20101110200837.1386.rpm
zcs-5.0.25_GA_3360.RHEL5.20101110200837/packages/zimbra-core-5.0.25_GA_3360.RHEL5-20101110200837.1386.rpm
zcs-5.0.25_GA_3360.RHEL5.20101110200837/packages/zimbra-ldap-5.0.25_GA_3360.RHEL5-20101110200837.1386.rpm
zcs-5.0.25_GA_3360.RHEL5.20101110200837/packages/zimbra-logger-5.0.25_GA_3360.RHEL5-20101110200837.1386.rpm
zcs-5.0.25_GA_3360.RHEL5.20101110200837/packages/zimbra-mta-5.0.25_GA_3360.RHEL5-20101110200837.1386.rpm
zcs-5.0.25_GA_3360.RHEL5.20101110200837/packages/zimbra-proxy-5.0.25_GA_3360.RHEL5-20101110200837.1386.rpm
zcs-5.0.25_GA_3360.RHEL5.20101110200837/packages/zimbra-snmp-5.0.25_GA_3360.RHEL5-20101110200837.1386.rpm
zcs-5.0.25_GA_3360.RHEL5.20101110200837/packages/zimbra-spell-5.0.25_GA_3360.RHEL5-20101110200837.1386.rpm
zcs-5.0.25_GA_3360.RHEL5.20101110200837/packages/zimbra-store-5.0.25_GA_3360.RHEL5-20101110200837.1386.rpm
zcs-5.0.25_GA_3360.RHEL5.20101110200837/bin/
zcs-5.0.25_GA_3360.RHEL5.20101110200837/bin/get_plat_tag.sh
zcs-5.0.25_GA_3360.RHEL5.20101110200837/bin/zmdbintegrityreport
zcs-5.0.25_GA_3360.RHEL5.20101110200837/data/
zcs-5.0.25_GA_3360.RHEL5.20101110200837/data/versions-init.sql
zcs-5.0.25_GA_3360.RHEL5.20101110200837/docs/
zcs-5.0.25_GA_3360.RHEL5.20101110200837/docs/YPL.txt

```

Figura 49 Archivo instalador de zimbra

8. Para la instalación se ingresa al directorio creando dentro de /opt/zcs y se selecciona ./install.sh --platform-override, obligando al sistema que omita la versión que se tiene instalado, como se puede visualizar en la figura 50.



```

[root@mail opt]# ls
webmin-1.530-1.noarch.rpm          zcs-5.0.25_GA_3360.RHEL5.20101110200837.tgz
zcs-5.0.25_GA_3360.RHEL5.20101110200837
[root@mail opt]# cd zcs-5.0.25_GA_3360.RHEL5.20101110200837
[root@mail zcs-5.0.25_GA_3360.RHEL5.20101110200837]# ./install.sh --platform-override

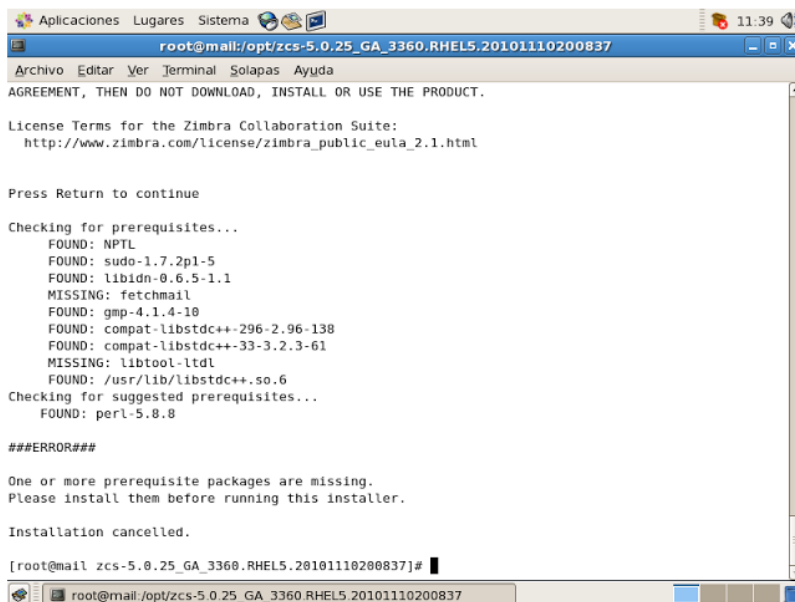
Operations logged to /tmp/install.log.4815
Checking for existing installation...
zimbra-ldap...NOT FOUND
zimbra-logger...NOT FOUND
zimbra-mta...NOT FOUND
zimbra-snmp...NOT FOUND
zimbra-store...NOT FOUND
zimbra-apache...NOT FOUND
zimbra-spell...NOT FOUND
zimbra-proxy...NOT FOUND
zimbra-archiving...NOT FOUND
zimbra-convertd...NOT FOUND
zimbra-cluster...NOT FOUND
zimbra-core...NOT FOUND

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.
ZIMBRA, INC. ("ZIMBRA") WILL ONLY LICENSE THIS SOFTWARE TO YOU IF YOU
FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY DOWNLOADING OR INSTALLING
THE SOFTWARE, OR USING THE PRODUCT, YOU ARE CONSENTING TO BE BOUND BY
THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS
AGREEMENT, THEN DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

```

Figura 50 Ingreso al directorio de Instalación

9. Luego se verifica los requisitos de las librerías para la instalación, en este caso indica que faltan librerías, ver figura 51.



```

Aplicaciones Lugares Sistema 11:39
root@mail:/opt/zcs-5.0.25_GA_3360.RHEL5.20101110200837
Archivo Editar Ver Terminal Solapas Ayuda
AGREEMENT, THEN DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

License Terms for the Zimbra Collaboration Suite:
http://www.zimbra.com/license/zimbra_public_eula_2.1.html

Press Return to continue

Checking for prerequisites...
FOUND: NPTL
FOUND: sudo-1.7.2p1-5
FOUND: libidn-0.6.5-1.1
MISSING: fetchmail
FOUND: gmp-4.1.4-10
FOUND: compat-libstdc++-296-2.96-138
FOUND: compat-libstdc++-33-3.2.3-61
MISSING: libtool-ltdl
FOUND: /usr/lib/libstdc++.so.6
Checking for suggested prerequisites...
FOUND: perl-5.8.8

###ERROR###

One or more prerequisite packages are missing.
Please install them before running this installer.

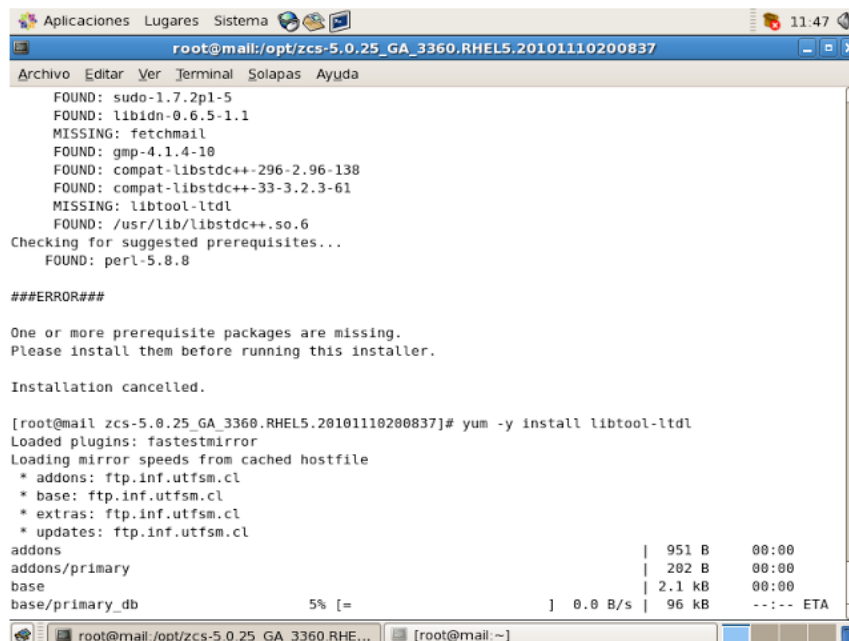
Installation cancelled.

[root@mail zcs-5.0.25_GA_3360.RHEL5.20101110200837]#

```

Figura 51 Verificación de librerías

10. A continuación serán instaladas con yum `-y install`, ver figura 52.



```

Aplicaciones Lugares Sistema 11:47
root@mail:/opt/zcs-5.0.25_GA_3360.RHEL5.20101110200837
Archivo Editar Ver Terminal Solapas Ayuda

FOUND: sudo-1.7.2p1-5
FOUND: libidn-0.6.5-1.1
MISSING: fetchmail
FOUND: gmp-4.1.4-10
FOUND: compat-libstdc++-296-2.96-138
FOUND: compat-libstdc++-33-3.2.3-61
MISSING: libtool-ltdl
FOUND: /usr/lib/libstdc++.so.6
Checking for suggested prerequisites...
FOUND: perl-5.8.8

###ERROR###

One or more prerequisite packages are missing.
Please install them before running this installer.

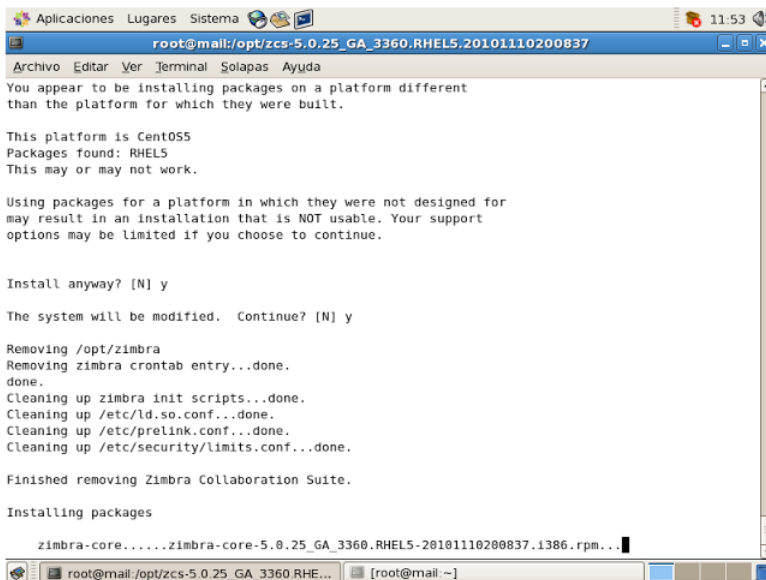
Installation cancelled.

[root@mail zcs-5.0.25_GA_3360.RHEL5.20101110200837]# yum -y install libtool-ltdl
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * addons: ftp.inf.utfsm.cl
 * base: ftp.inf.utfsm.cl
 * extras: ftp.inf.utfsm.cl
 * updates: ftp.inf.utfsm.cl
addons | 951 B | 00:00
addons/primary | 202 B | 00:00
base | 2.1 kB | 00:00
base/primary_db 5% [= ] 0.0 B/s | 96 kB --:-- ETA

```

Figura 52 Instalación de librerías con yum `-y install`

11. En el siguiente paso, el sistema preguntará si se desea seguir con la instalación de los paquetes que se han descargado, ver figura 53.



```

Aplicaciones Lugares Sistema 11:53
root@mail:/opt/zcs-5.0.25_GA_3360.RHEL5.20101110200837
Archivo Editar Ver Terminal Solapas Ayuda
You appear to be installing packages on a platform different
than the platform for which they were built.

This platform is CentOS5
Packages found: RHEL5
This may or may not work.

Using packages for a platform in which they were not designed for
may result in an installation that is NOT usable. Your support
options may be limited if you choose to continue.

Install anyway? [N] y

The system will be modified. Continue? [N] y

Removing /opt/zimbra
Removing zimbra crontab entry...done.
done.
Cleaning up zimbra init scripts...done.
Cleaning up /etc/ld.so.conf...done.
Cleaning up /etc/prelink.conf...done.
Cleaning up /etc/security/limits.conf...done.

Finished removing Zimbra Collaboration Suite.

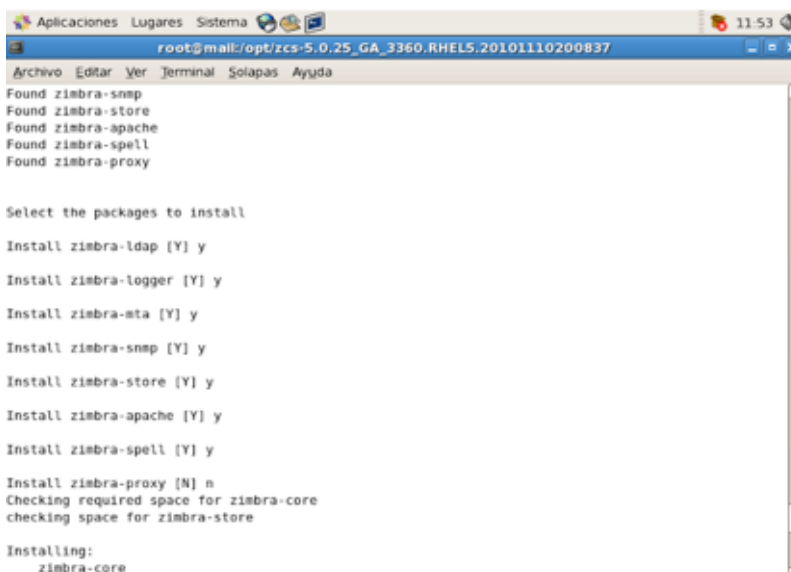
Installing packages

zimbra-core.....zimbra-core-5.0.25_GA_3360.RHEL5-20101110200837.1386.rpm...

```

Figura 53 Instalación de /install.sh --platform-override

12. A continuación se selecciona los paquetes a instalar, los cuales serán todos menos el zimbra proxy, ver figura 54.



```

Aplicaciones Lugares Sistema 11:53
root@mail:/opt/zcs-5.0.25_GA_3360.RHEL5.20101110200837
Archivo Editar Ver Terminal Solapas Ayuda
Found zimbra-snmp
Found zimbra-store
Found zimbra-apache
Found zimbra-spell
Found zimbra-proxy

Select the packages to install

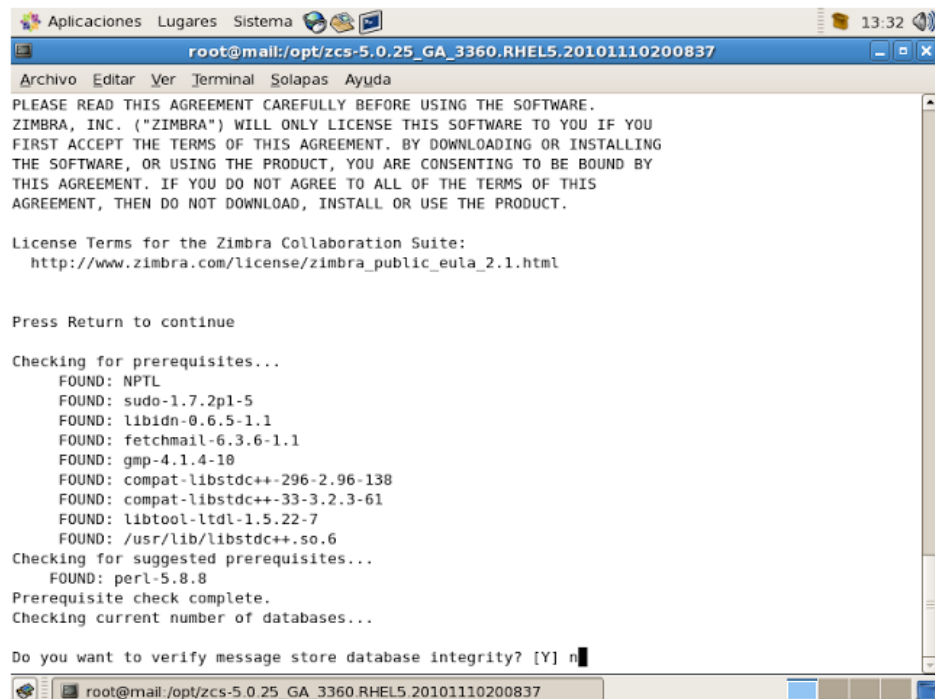
Install zimbra-ldap [Y] y
Install zimbra-logger [Y] y
Install zimbra-mta [Y] y
Install zimbra-snmp [Y] y
Install zimbra-store [Y] y
Install zimbra-apache [Y] y
Install zimbra-spell [Y] y
Install zimbra-proxy [N] n
Checking required space for zimbra-core
checking space for zimbra-store

Installing:
zimbra-core

```

Figura 54 Selección de paquetes a instalar

13. Luego el sistema pedirá verificar la integridad de la base de datos, responder con no (n), ver figura 55.



```

Aplicaciones Lugares Sistema 13:32
root@mail:/opt/zcs-5.0.25_GA_3360.RHEL5.20101110200837
Archivo Editar Ver Terminal Solapas Ayuda
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.
ZIMBRA, INC. ("ZIMBRA") WILL ONLY LICENSE THIS SOFTWARE TO YOU IF YOU
FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY DOWNLOADING OR INSTALLING
THE SOFTWARE, OR USING THE PRODUCT, YOU ARE CONSENTING TO BE BOUND BY
THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS
AGREEMENT, THEN DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

License Terms for the Zimbra Collaboration Suite:
http://www.zimbra.com/license/zimbra_public_eula_2.1.html

Press Return to continue

Checking for prerequisites...
FOUND: NPTL
FOUND: sudo-1.7.2p1-5
FOUND: libidn-0.6.5-1.1
FOUND: fetchmail-6.3.6-1.1
FOUND: gmp-4.1.4-10
FOUND: compat-libstdc+-296-2.96-138
FOUND: compat-libstdc+-33-3.2.3-61
FOUND: libtool-ltdl-1.5.22-7
FOUND: /usr/lib/libstdc++.so.6
Checking for suggested prerequisites...
FOUND: perl-5.8.8
Prerequisite check complete.
Checking current number of databases...

Do you want to verify message store database integrity? [Y] n

```

Figura 55 Verificación de la integridad de la base de datos

14. Continuando la instalación, se seguirán instalando paquetes, verificando las configuraciones, el menú de Zimbra se mostrará en el cual se seleccionará la opción tres (admin user to create), para crear un usuario de Zimbra, en este caso el administrador será admin@cemylub.com, en la opción diez y ocho se visualiza el Spell server URL que en este caso será: https://mail.cemylub.com:7071/zimbraAdmin/, como se puede visualizar en la figura 56.

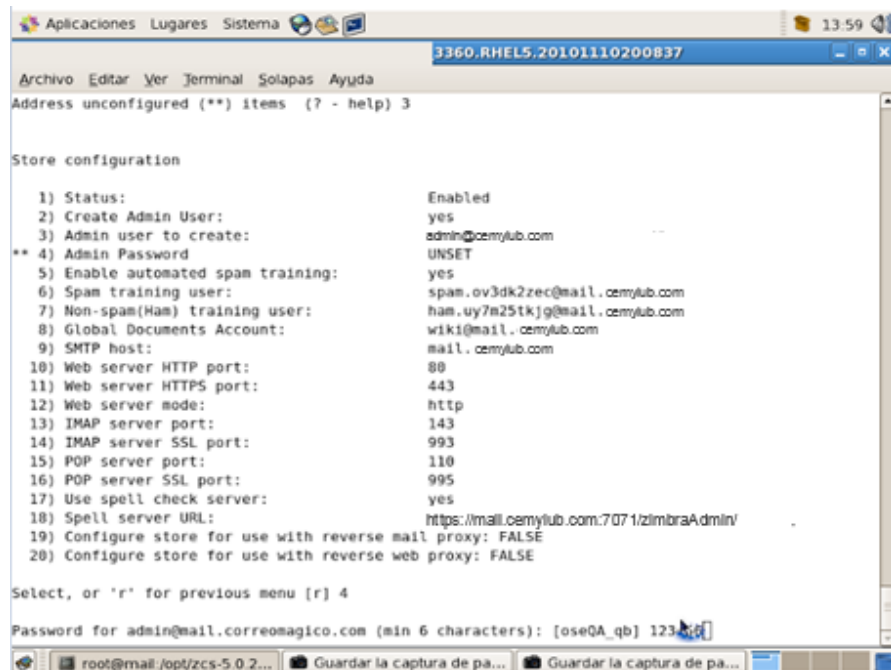


Figura 56 Creación de usuario de zimbra

15. Luego de finalizar con la instalación, se puede verificar que todos los servicios estén corriendo ejecutando la siguiente línea `zmcontrol status`, ver figura 57.

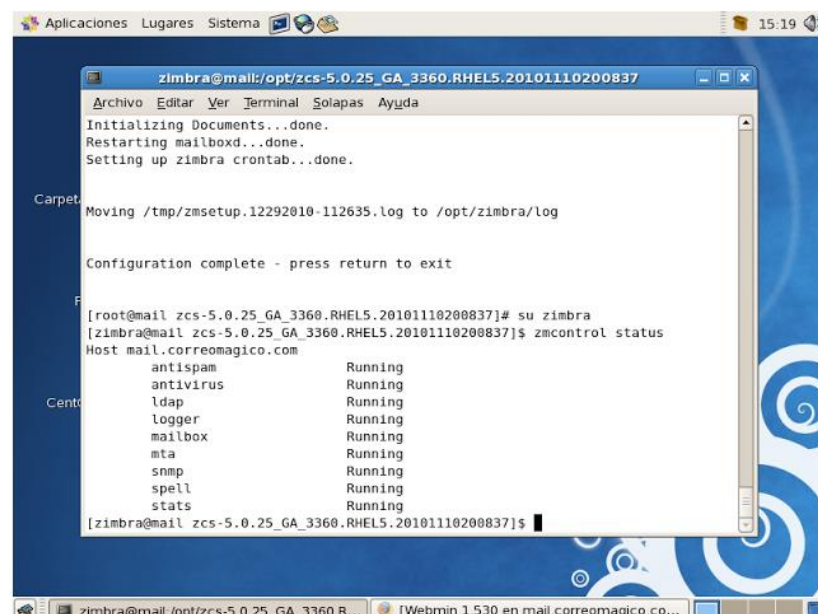
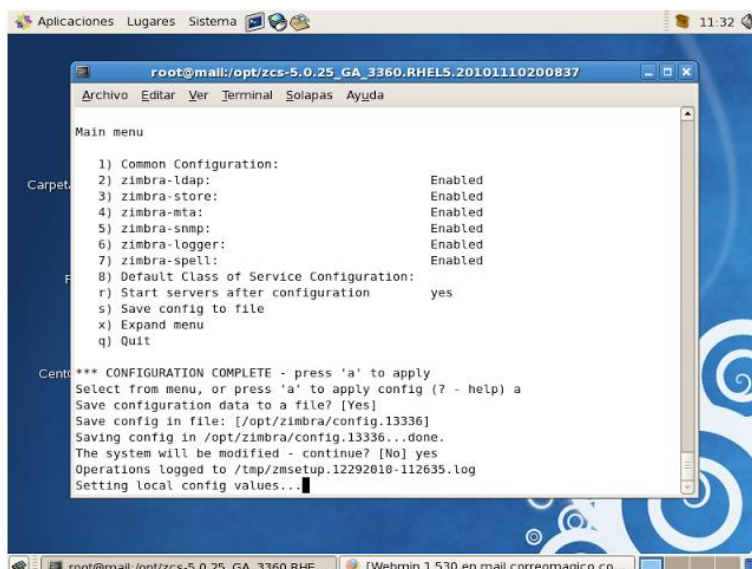


Figura 57 Verificación de funcionamiento de servicios

16. Para confirmar y aplicar las configuraciones se debe presionar la letra a, ver figura 58.



```

root@mail:/opt/zcs-5.0.25_GA_3360.RHEL5.20101110200837
Archivo Editar Ver Terminal Solapas Ayuda

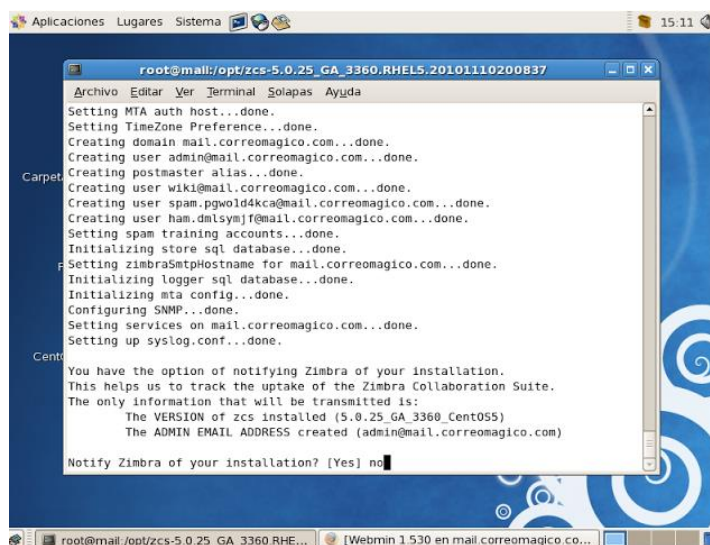
Main menu
1) Common Configuration:
2) zimbra-ldap: Enabled
3) zimbra-store: Enabled
4) zimbra-mta: Enabled
5) zimbra-snmp: Enabled
6) zimbra-logger: Enabled
7) zimbra-spell: Enabled
8) Default Class of Service Configuration:
r) Start servers after configuration yes
s) Save config to file
x) Expand menu
q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) a
Save configuration data to a file? [Yes]
Save config in file: [/opt/zimbra/config.13336]
Saving config in /opt/zimbra/config.13336..done.
The system will be modified - continue? [No] yes
Operations logged to /tmp/zmsetup.12292010-112635.log
Setting local config values...

```

Figura 58 Aplicando configuraciones en Zimbra

17. El sistema mostrará un mensaje en el cual dirá: notificar la instalación al cual se responderá con no (n), ver figura 59.



```

root@mail:/opt/zcs-5.0.25_GA_3360.RHEL5.20101110200837
Archivo Editar Ver Terminal Solapas Ayuda

Setting MTA auth host...done.
Setting TimeZone Preference...done.
Creating domain mail.correomagico.com...done.
Creating user admin@mail.correomagico.com...done.
Creating postmaster alias...done.
Creating user wiki@mail.correomagico.com...done.
Creating user spam.pgworld4kca@mail.correomagico.com...done.
Creating user ham.dmlsymjf@mail.correomagico.com...done.
Setting spam training accounts...done.
Initializing store sql database...done.
Setting zimbra5mtphostname for mail.correomagico.com...done.
Initializing logger sql database...done.
Initializing mta config...done.
Configuring SNMP...done.
Setting services on mail.correomagico.com...done.
Setting up syslog.conf...done.

You have the option of notifying Zimbra of your installation.
This helps us to track the uptake of the Zimbra Collaboration Suite.
The only information that will be transmitted is:
  The VERSION of zcs installed (5.0.25_GA_3360_Cent055)
  The ADMIN EMAIL ADDRESS created (admin@mail.correomagico.com)

Notify Zimbra of your installation? [Yes] no

```

Figura 59 Finalización de la instalación

18. Como se verificó anteriormente todos los servicios están corriendo, por lo tanto se puede ingresar desde otro equipo con la siguiente dirección: <https://mail.cemylub.com/>, ver figura 60.

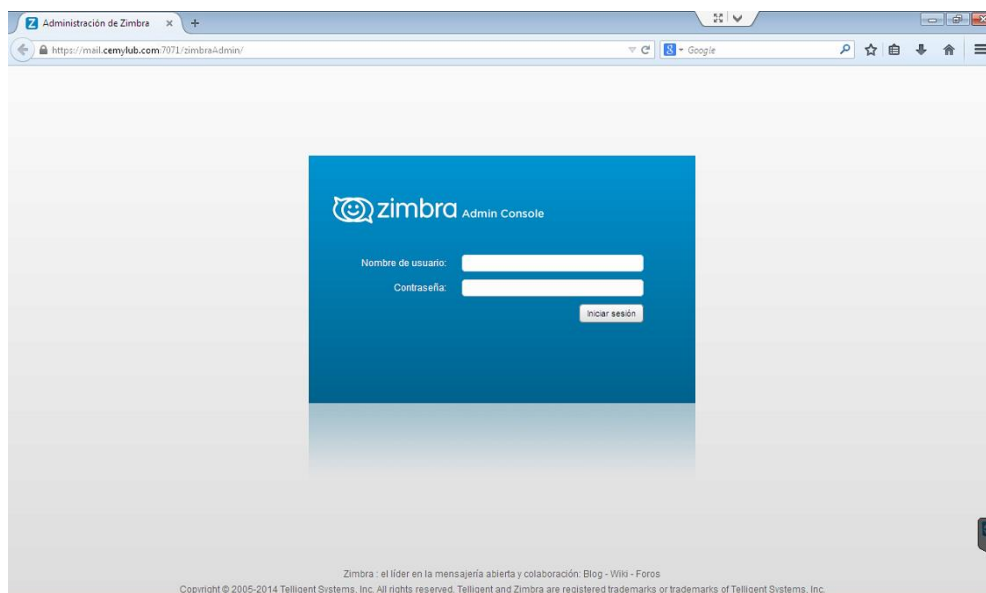


Figura 60 Ingreso a la consola de administración de zimbra

3.5 Instalación de nessus en Windows server 2008

En primer lugar antes de proceder a la instalación del servidor Nessus se realizará la instalación previa de Windows Server 2008.

3.5.1 Instalación de Windows server 2008

Antes de comenzar la instalación del sistema operativo se debe verificar que se cumplan los siguientes requisitos:

- Si se requiere configurar la unidad de arranque para RAID 1 (duplicación), se tiene que usar la utilidad de configuración del

controlador RAID integrado en LSI Logic previamente instalar el sistema operativo Windows.

- Para poder conocer el método de entrega multimedia de Windows que se tiene que seleccionar, se debe consultar la siguiente tabla 10 de requisitos.

Tabla 10

Métodos de entrega multimedia de Windows

MÉTODO	ACCIÓN O ELEMENTOS NECESARIOS
Windows local	Se debe tener el medio de instalación de Microsoft Windows Server 2008 R2 disponible para insertarlo en la unidad de CD/DVD-ROM física conectada cuando se le solicite.
Windows remoto	Se debe Insertar el medio de instalación de Microsoft Windows Server 2008 R2 en la unidad de CD/DVD-ROM del sistema JavaRConsole. Se debe asegurar de que ha seleccionado el CD-ROM en el menú de dispositivos JavaRConsole.
Imagen de Windows	Se debe asegurar de que se pueda acceder a la imagen ISO de instalación de Windows Server 2008 R2 desde el sistema JavaRConsole. Verifique de haber seleccionado la imagen del CD-ROM en el menú de dispositivos JavaRConsole.

(Parkway, 2010)

3.5.1.1 Pasos de instalación de Windows server

1. Apagar y volver a encender el servidor.

Si se usa el método remoto o de imagen de Windows, se puede realizar por medio de ILOM. En otras palabras empezar el proceso de BIOS POST.

2. Presionar la tecla F8 cuando aparezca el mensaje “press F8 for BBS POPUP”.

BBS POPUP es un menú que permitirá seleccionar un dispositivo de arranque, ver figura 61.

```
Initializing USB Controllers .. Done.  
Press F2 to run Setup (CTRL+E on Remote Keyboard)  
Press F8 for BBS POPUP (CTRL+P on Remote Keyboard)  
Press F12 to boot from the network (CTRL+N on Remote Keyboard)
```

Figura 61 Mensaje para acceder a BBS POPUP

3. A partir de que se haya completado el proceso BIOS POST, se mostrara el menú del dispositivo de arranque. Si se ha seleccionado el método local de instalación de Windows, se deberá insertar el DVD de Windows en la unidad de DVD disponible, ver figura 62.



Figura 62 Inserción de DVD

4. Selección de posibilidades

- Cuando se usa el método local de Windows, se debe seleccionar el CD/DVD desde el menú del dispositivo.

- Si se usa el método de Windows remoto o de imagen de Windows, se debe seleccionar el CD/DVD virtual desde el menú de dispositivo de arranque y pulsar intro.
5. A continuación aparecerá el asistente de instalación, continuar con los pasos que muestra hasta que aparezca el tipo de instalación en el cual se seleccionara personalizada avanzado “custom (advanced)”, ver figura 63.

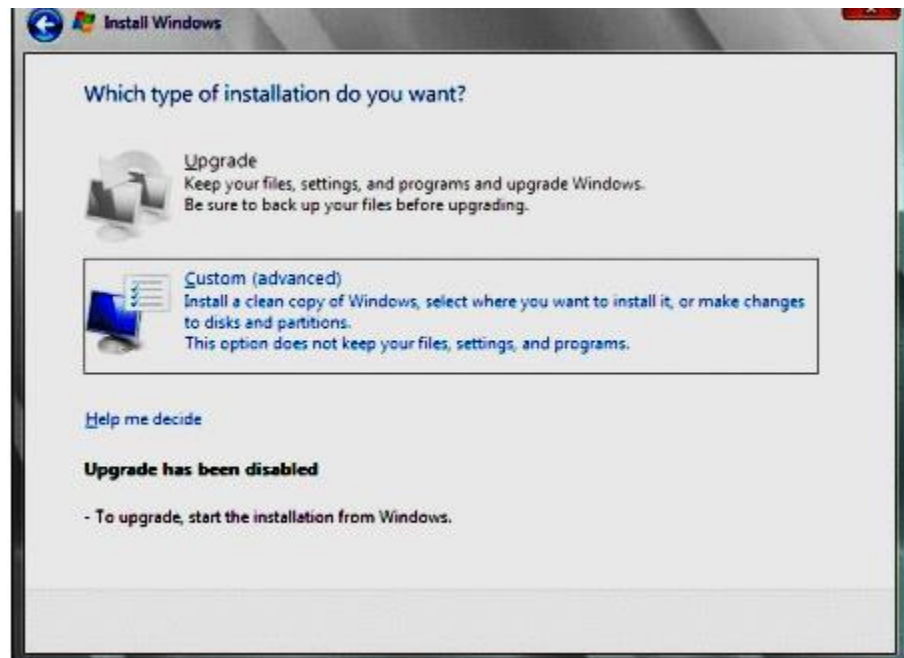


Figura 63 Selección del tipo de instalación

6. En el siguiente paso aparecerá la ventana “where to install windows” y se pulsara el botón “drive options (advanced)” como se muestra en la siguiente ilustración, ver figura 64.

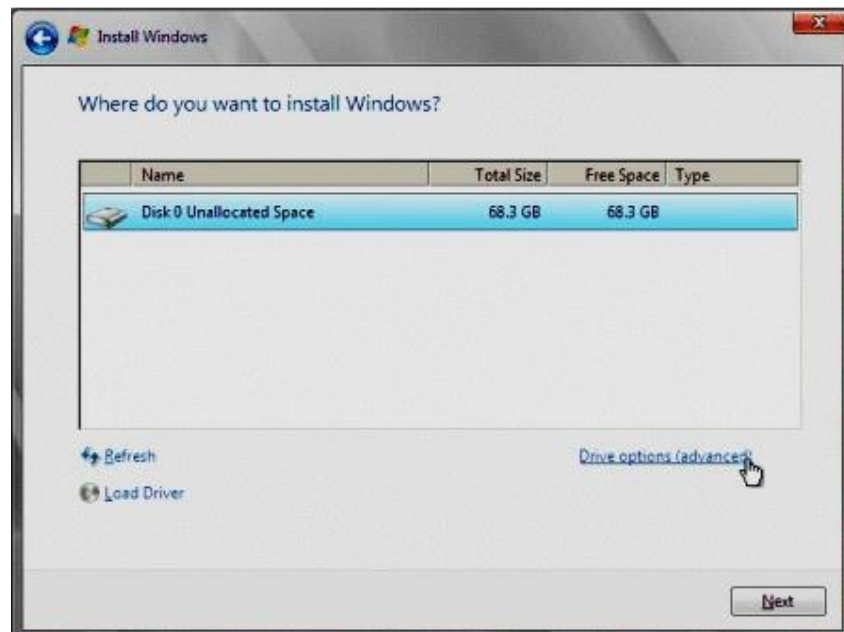


Figura 64 Dirección de instalación de Windows Server

7. A continuación, en la ventana de opciones de controlador avanzadas se deberá borrar la partición de disco existente, y crear un nuevo cambiando los valores de acuerdo a los requerimientos necesarios como se muestra en el figura 65.

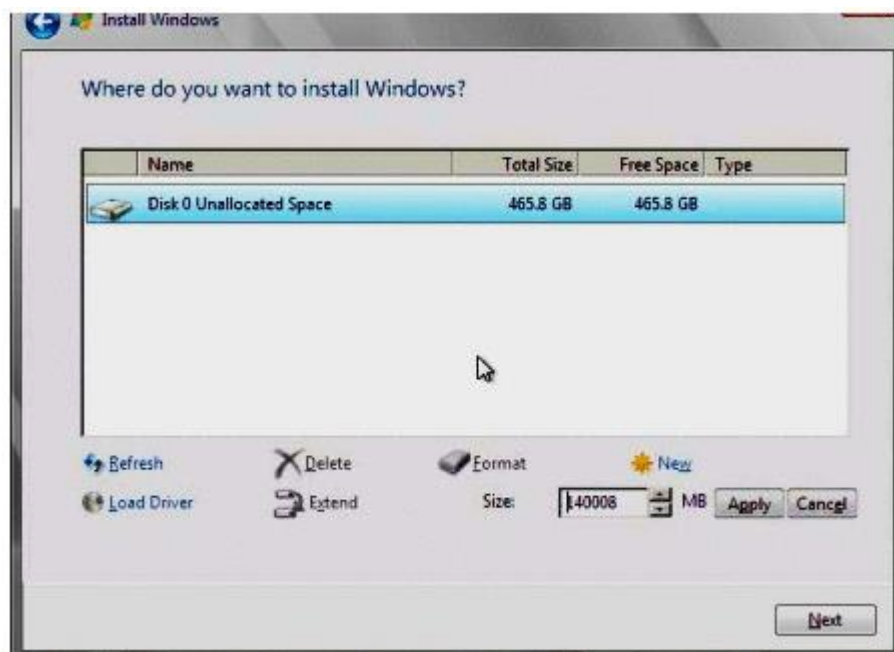


Figura 65 Creación de la nueva partición de disco

La instalación de Windows Server comenzara, por lo que el servidor se reiniciará varias veces durante el proceso de instalación. Una vez que la instalación de Windows Server se haya completado, Windows se iniciara y solicitara cambiar la contraseña de usuario. En este punto se deberá configurar la cuenta de acceso de usuario inicial.

Una vez que se haya configurado la cuenta inicial, aparecerá el escritorio de Windows Server 2008.

3.5.2 Instalación del servidor nessus

Nessus es distribuido como un archivo de instalación ejecutable, le cual es colocado en el sistema en el que debe ser instalado o en una unidad compartida a la que se tenga acceso el sistema.

Nessus debe ser instalado empleando una cuenta administrativa y no como usuario sin privilegios. Si ocurren errores que tengan relación con permisos, es decir que muestren "Access Denied" (Acceso denegado) o errores que muestren que una acción tuvo lugar debido a la falta de privilegios, se debe verificar que esta cuenta usada tenga privilegios administrativos. Si existen estos errores al seleccionar las utilidades de líneas de comandos, se debe ejecutar cmd.exe con los privilegios "Run as" (Ejecutar como) que son establecidos en "administrator" (administrador), ver figura 66.



Figura 66 Asistente de instalación de Nessus

En el proceso de instalación, el asistente le solicitará al usuario que introduzca algunos datos básicos. Antes de empezar, deberá el usuario aceptar el contrato de licencia, ver figura 67.

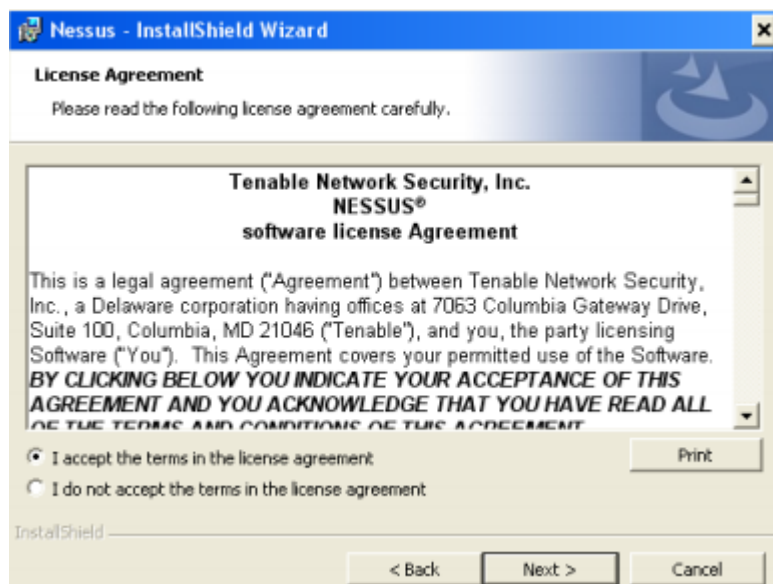


Figura 67 Contrato de licencia de Nessus

A continuación se puede configurar la ubicación en la que se instalará Nessus, ver figura 68.

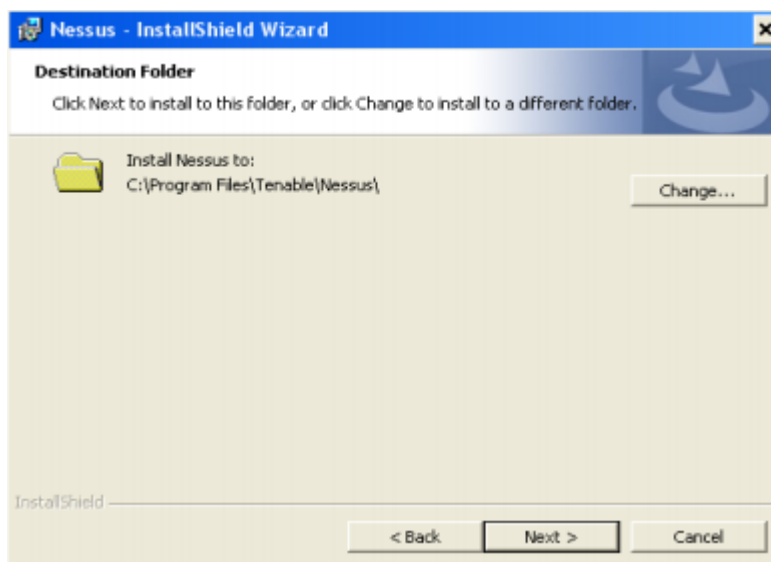


Figura 68 Ubicación de la instalación de Nessus

El asistente de instalación solicitará que se seleccione el "setup type", seleccionar "complete", ver figura 69.

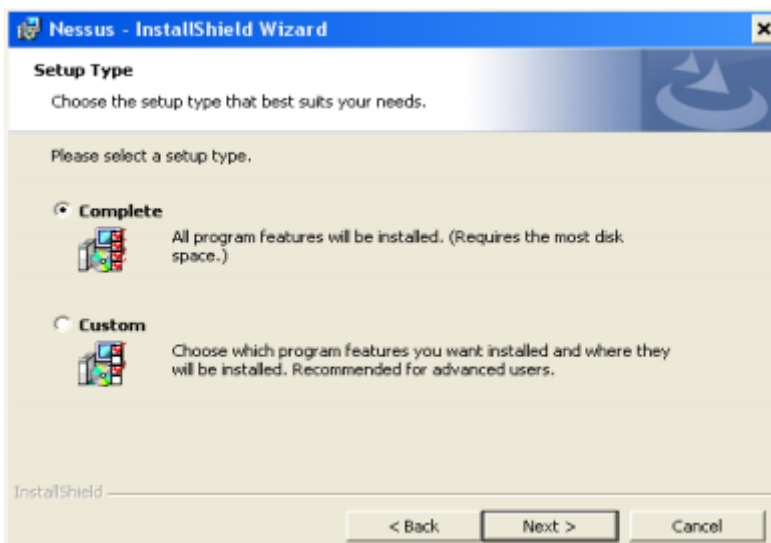


Figura 69 Selección del tipo de instalación

A continuación se solicitará que sea confirmada la instalación, ver figura 70.

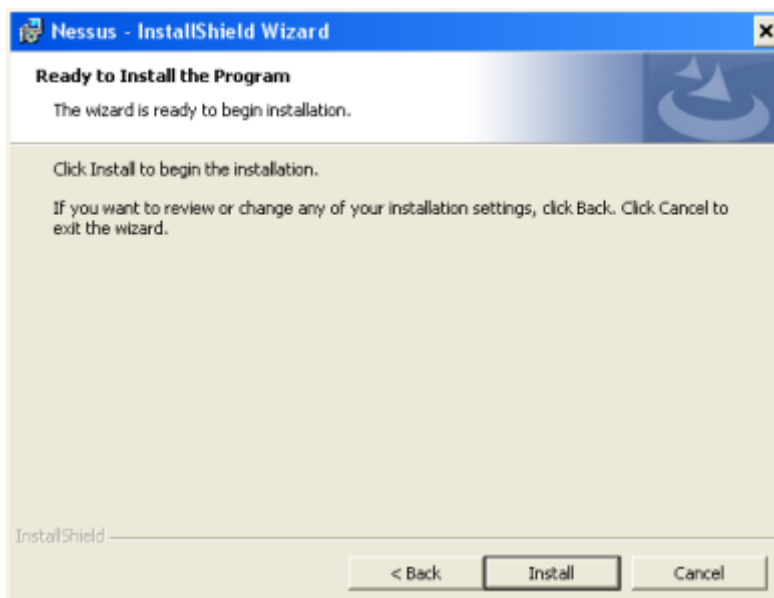


Figura 70 Confirmación de la instalación de nessus

Al cabo que haya terminado el proceso de instalación presionar el botón finish, ver figura 71.



Figura 71 Finalización de la instalación de nessus

A continuación se muestra en la tabla 11 los directorios principales de Nessus.

Tabla 11
Directorios principales de Nessus

DIRECTORIO PRINCIPAL DE NESSUS	SUBDIRECTORIOS DE NESSUS	OBJETIVO
\program file\teneable\nessus	\conf	Archivos de configuración
	\data	Platillas de hojas de estilo
	\plugins	Plugins de nessus
	\users\<>username>	Base de conocimiento del usuario guardada en el disco
	\kbs	
	\logs	Archivos de registro de Nessus

(Securit, 2011)

3.5.3 Configuración de nessus

Para iniciar y detener temporalmente el servidor Nessus, se lo puede realizar en el sistema de Windows abriendo el menú “Start” (Inicio) y haciendo clic en “Run” (Ejecutar). En el cuadro “Run” (Ejecutar), se escribe “service.mcs” para abrir el Windows Service Manager, ver figura 72.

Name ^	Description	Status	Startup Type	Log On As
Task Scheduler	Enables a user to configure and sc...	Started	Automatic	Local System
TCP/IP NetBIOS Helper	Provides support for the NetBIOS ...	Started	Automatic	Local Service
Telephony	Provides Telephony API (TAPI) sup...		Manual	Network Service
Tenable Nessus	Tenable Nessus Network Security ...	Started	Automatic	Local System
Tenable PVS Proxy Service	Tenable Passive Vulnerability Scan...		Automatic	Local System
Themes	Provides user experience theme m...	Started	Automatic	Local System
Thread Ordering Server	Provides ordered execution for a g...		Manual	Local Service

Figura 72 Servicio de tenable nessus iniciado

A partir de la versión 5.0 todas las configuraciones iniciales, opciones de proxy y código de activación se realizan mediante un proceso web. De esta manera se puede realizar las configuraciones siguientes:

- Registrar el servidor en la página oficial, de esta manera se recibirán plugins actualizados.
- Realizar actualizaciones de plugins.
- Configurar si se desea que el servidor Nessus se ejecute al iniciarse Windows.
- Asistente de instalación.
- Mejorado el sistema de filtros y creación de políticas
- Administrar usuarios de Nessus.
- Iniciar o detener el servidor Nessus.
- Reportes personalizados.
- Herramienta por excelencia de escaneo.

Una vez que se ingrese al servidor Nessus mediante la web se despliega la siguiente pantalla, ver figura 73.

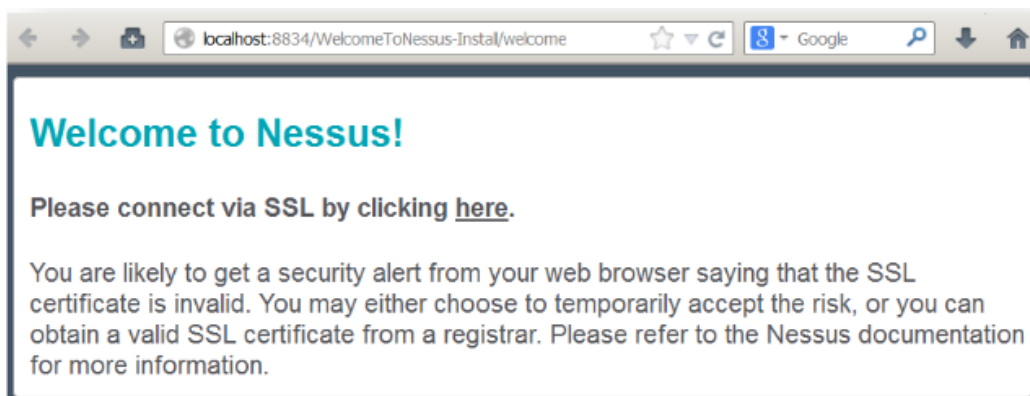


Figura 73 Interfaz de inicio de nessus

La primera vez que se conecta al servidor Nessus web, mostrará algún tipo de error que indica que la conexión no es confiable debido a un certificado SSL autofirmado. En la primera conexión, acepte el certificado para continuar la configuración, ver figura 74.

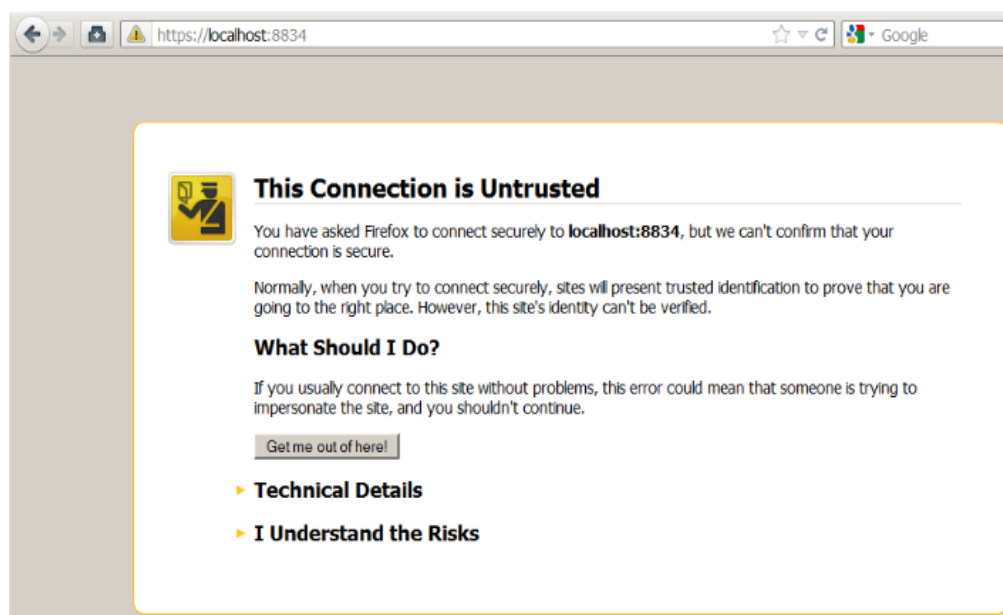


Figura 74 Interfaz de certificado de seguridad

A continuación se muestra un diálogo adicional que le permita aceptar el certificado, ver figura 75.



Figura 75 Certificado de seguridad

Una vez que lo aceptó, se le redirigirá a la pantalla inicial de registro que comienza las instrucciones paso a paso, ver figura 76.

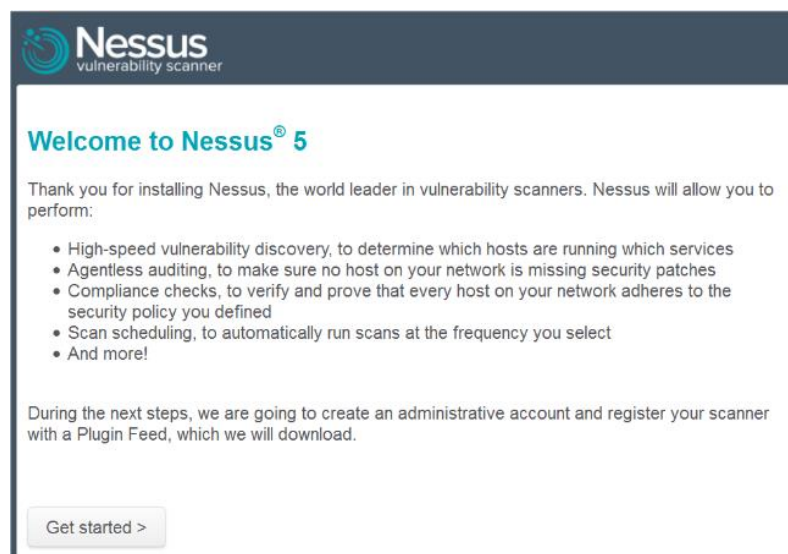
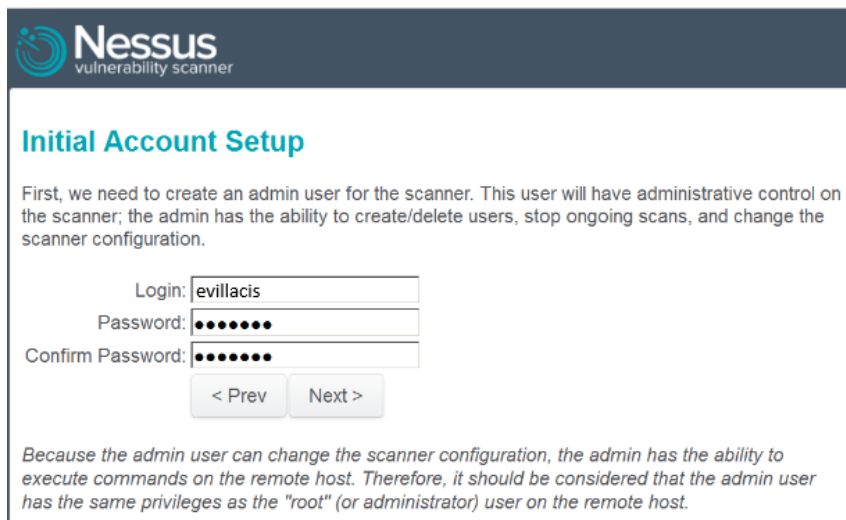


Figura 76 Interfaz de registro de nessus

El primer paso es crear una cuenta para el servidor Nessus. La cuenta inicial será de administrador; esta cuenta tiene acceso a la ejecución de comandos en el sistema operativo subyacente de la instalación de Nessus, por lo que se debe considerar de la misma manera que cualquier otra cuenta de administrador, ver figura 77.



Nessus
vulnerability scanner

Initial Account Setup

First, we need to create an admin user for the scanner. This user will have administrative control on the scanner; the admin has the ability to create/delete users, stop ongoing scans, and change the scanner configuration.

Login:

Password:

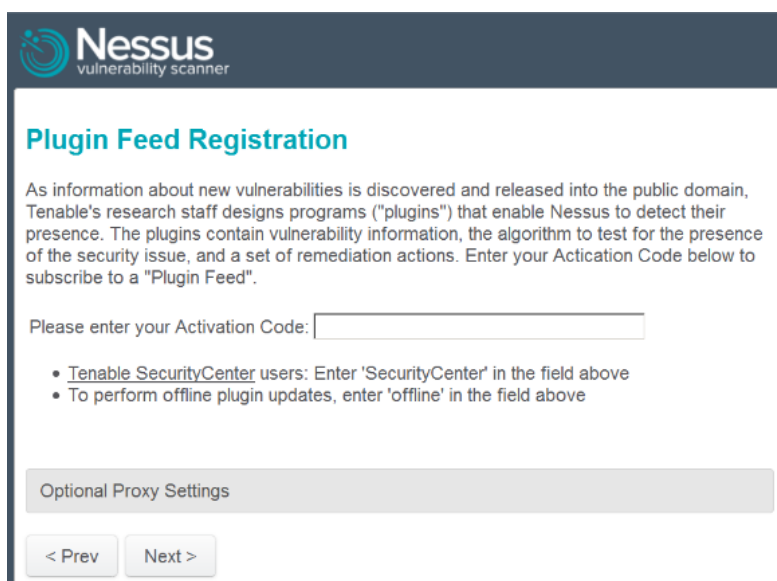
Confirm Password:

< Prev Next >

Because the admin user can change the scanner configuration, the admin has the ability to execute commands on the remote host. Therefore, it should be considered that the admin user has the same privileges as the "root" (or administrator) user on the remote host.

Figura 77 Interfaz de creación de usuario y contraseña

La siguiente pantalla solicita un Código de activación de plugins y le permite configurar parámetros de proxy opcionales. Si no tiene un código, puede obtener uno por medio del Tenable Support Portal (Portal de soporte de Tenable) o a través de su canal de ventas. Una vez que se registró, recibirá un correo electrónico con un enlace para activar el código, ver figura 78.



Nessus
vulnerability scanner

Plugin Feed Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, the algorithm to test for the presence of the security issue, and a set of remediation actions. Enter your Activation Code below to subscribe to a "Plugin Feed".

Please enter your Activation Code:

- [Tenable SecurityCenter](#) users: Enter 'SecurityCenter' in the field above
- To perform offline plugin updates, enter 'offline' in the field above

Optional Proxy Settings

< Prev Next >

Figura 78 Interfaz de activación mediante código

Una vez que se finalizó la configuración del Código de activación, el mismo se empezará a registrar, ver figura 79.

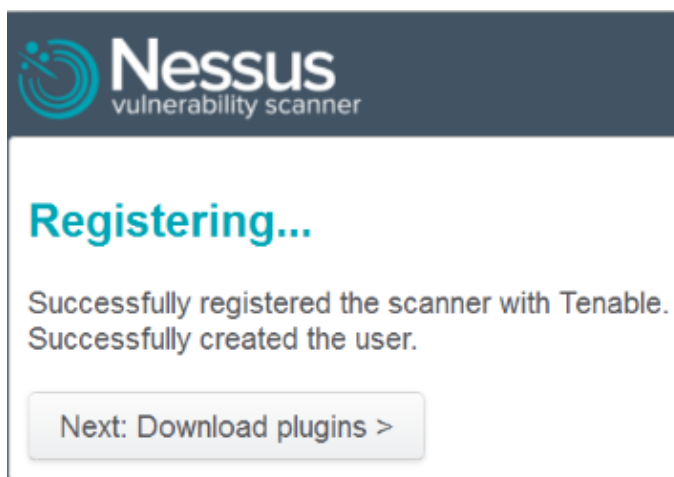


Figura 79 Registro con código de activación

Nessus actualizará y procesará los plugins, en su primera vez puede tardar unos minutos, ver figura 80.

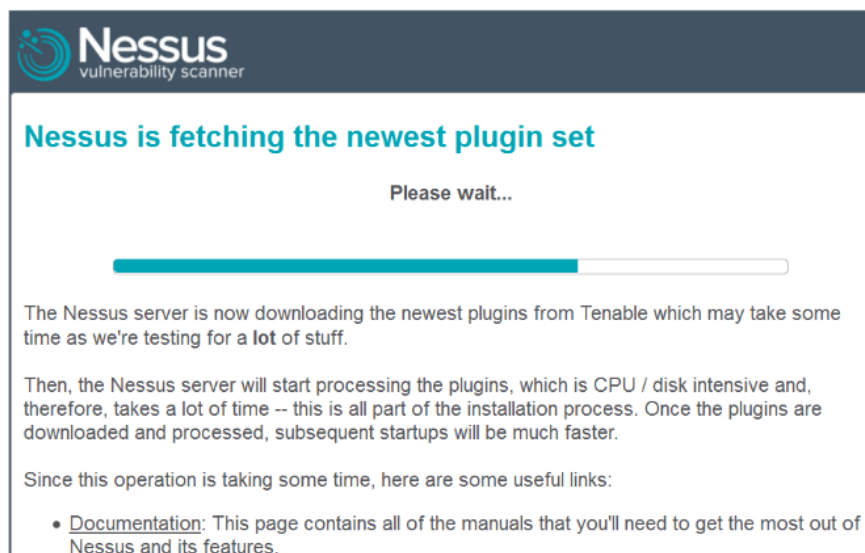


Figura 80 Actualización y descarga de plugins

El servidor web mostrará el mensaje “Nessus is initializing” y se volverá a cargar cuando esté listo, ver figura 81.

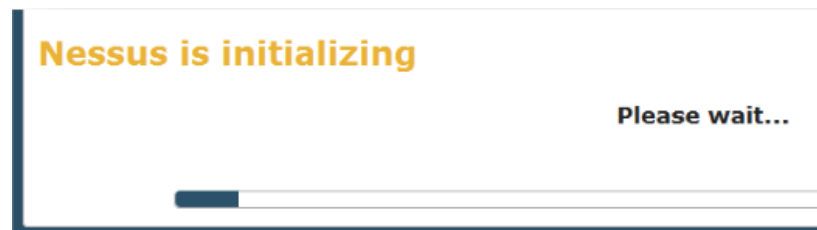


Figura 81 Primera actualización de nessus

Después de su inicialización, Nessus está listo para su uso, tal como se muestra en la figura 82.

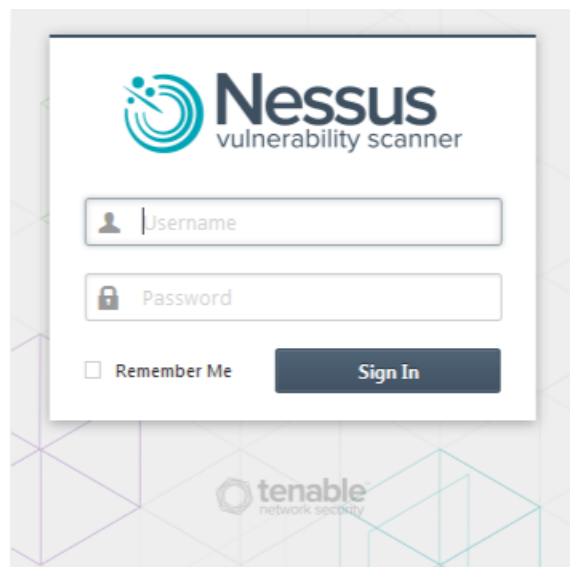


Figura 82 Autenticación de Nessus

3.5.3.4 Actualización de plugins de nessus

Nessus tiene infinidad de plugins o scripts (secuencias de comandos) los cuales realizan pruebas en busca de vulnerabilidades de red y host. Cada cierto tiempo se descubren nuevas vulnerabilidades y por lo que desarrollan nuevos plugins para detectarlas. Para que el analizador Nessus se encuentre actualizado con los plugins.

La opción “Perform a daily plugin update” configura el servidor Nessus para actualizar los plugins automáticamente desde Tenable cada 24 horas. Esto sucede aproximadamente en el momento del día en que inició Nessus, ver figura 83.

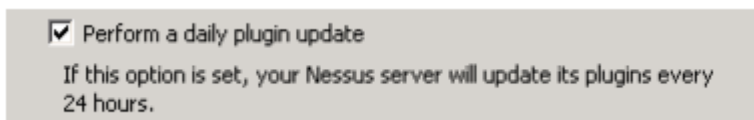


Figura 83 Actualización diaria de plugins

A continuación se puede ingresar al panel de configuración y visualizar las versiones y actualizaciones realizadas en Nessus, ver figura 84.

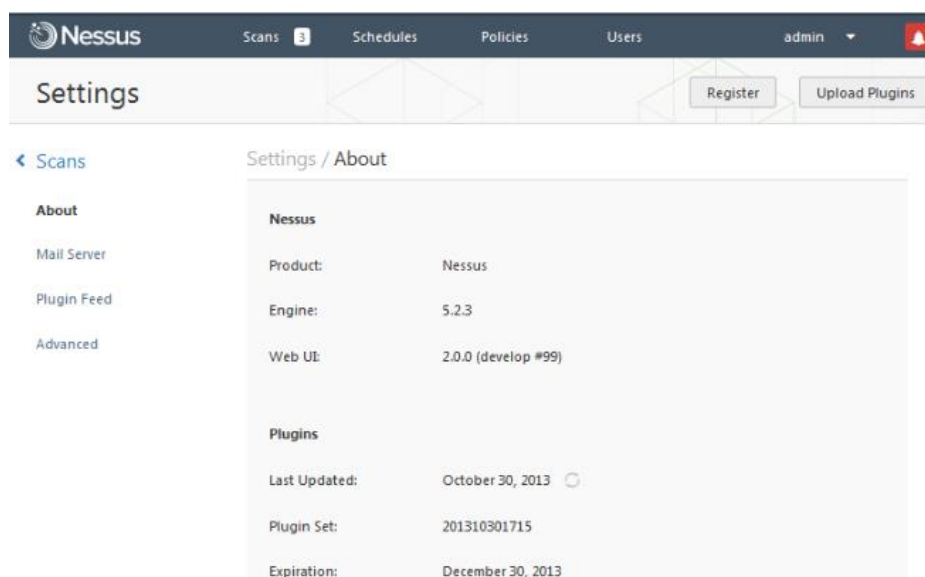


Figura 84 Interfaz web de la configuración

3.6 Instalación de EasyIDS en Centos 5.3

3.6.1 Instalación de easyids-snort

1. Una vez descargado EasyIDS se procederá con la instalación respectiva, se inicia el sistema operativo donde va a ser instalado, en este

caso es Centos, se ejecuta el instalador y se pulsa la tecla “ENTER” como se muestra a continuación en la figura 85.

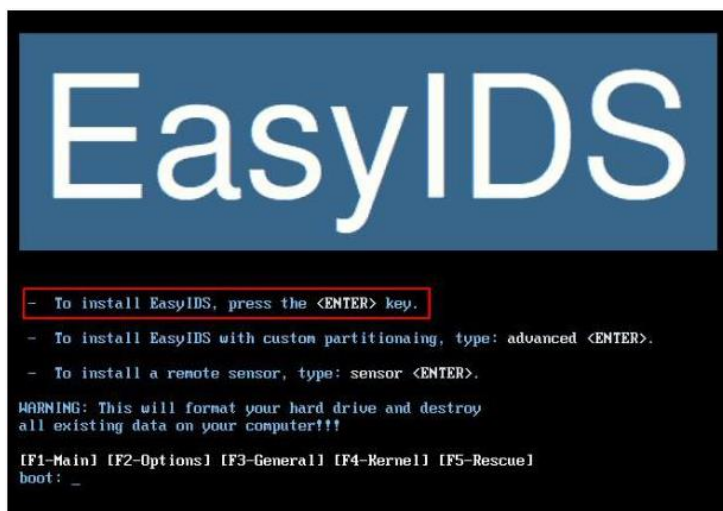


Figura 85 Ejecución del instalador de easyids

2. A continuación se debe seleccionar el idioma, y se presiona el botono “OK”, ver figura 86.

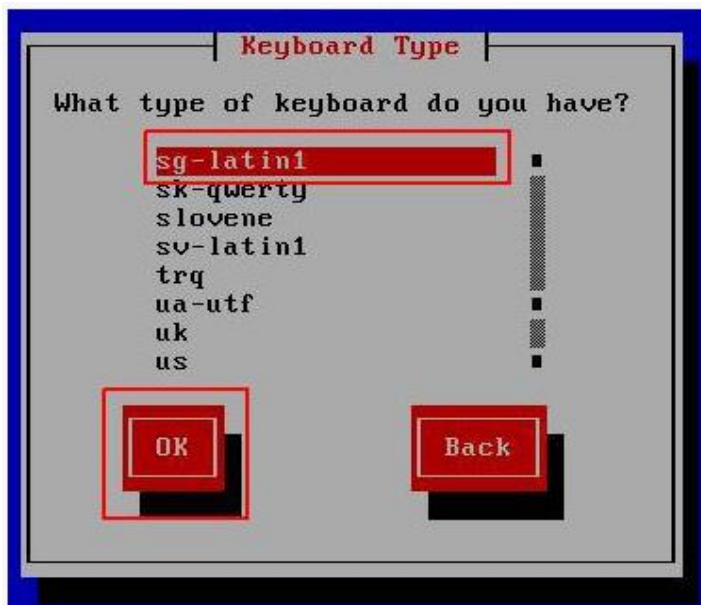


Figura 86 Selección del idioma

3. Como siguiente paso se seleccionará la zona horaria, este caso “Bogotá Lima Quito”, ver figura 87.



Figura 87 Selección de la zona horaria

4. A continuación el asistente de instalación pedirá que se ingrese una contraseña para el usuario root y se la confirme como se muestra en la siguiente ilustración, ver figura 88.

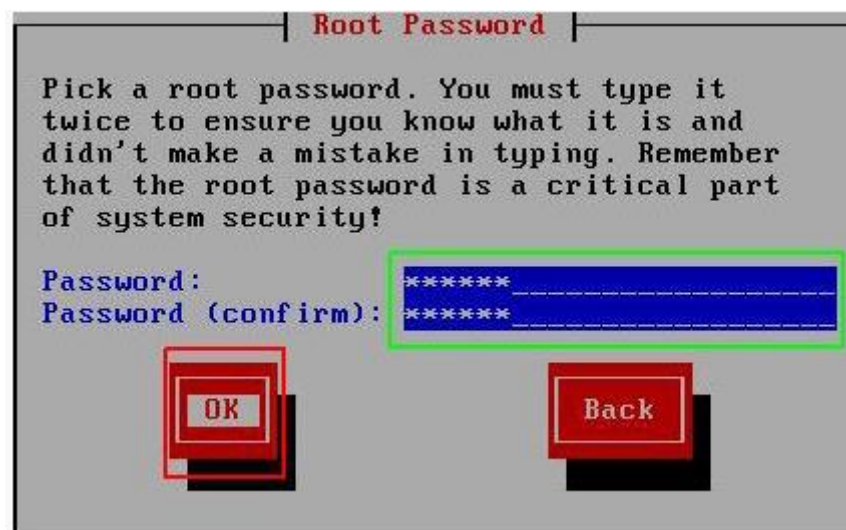


Figura 88 Selección de la contraseña del root

5. A continuación comenzará el proceso de instalación, al iniciarse los servicios se muestra el siguiente mensaje, ver figura 89.

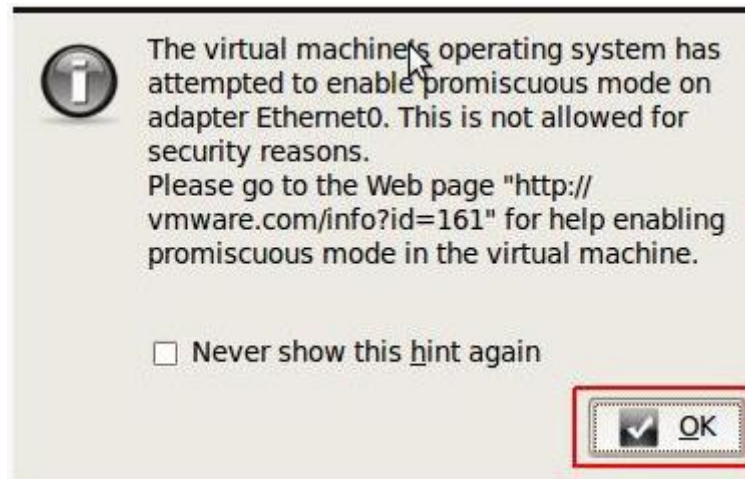


Figura 89 Mensaje de advertencia de instalación

6. Este mensaje indica que no es posible poner la tarjeta de red en modo promiscuo. Esto sucede en VMware por cuestiones de seguridad, para dar solución a este inconveniente ya que la tarjeta debe estar en modo promiscuo se debe abrir una terminal y digitar lo siguiente, ver figura 90.

```
chmod a+rw /dev/vmnet0
```

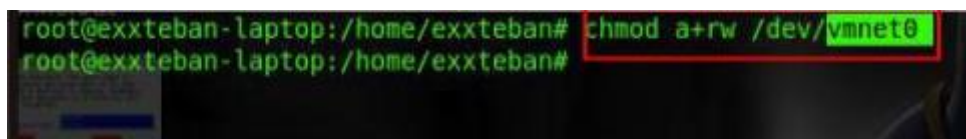


Figura 90 Permitir lectura y escritura a vmnet0

7. A continuación se realizará la configuración de red. Como se posee dos tarjetas, la eth0 y la eth1, la primera va a ser la tarjeta que estará en modo promiscuo vigilando la red y la otra tarjeta será la interfaz de administración, ver figura 91.

```

eth0 Link encap:Ethernet HWaddr 00:0C:29:6D:12:F1
      inet addr:192.168.0.100 Bcast:192.168.0.255 Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fe6d:12f1/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:40 errors:0 dropped:0 overruns:0 frame:0
      TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:11695 (11.4 KiB) TX bytes:19865 (19.3 KiB)
      Interrupt:67 Base address:0x2000

eth1 Link encap:Ethernet HWaddr 00:0C:29:6D:12:FB
      inet addr:192.168.0.102 Bcast:192.168.0.255 Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fe6d:12fb/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:14 errors:0 dropped:0 overruns:0 frame:0
      TX packets:55 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:4896 (4.7 KiB) TX bytes:11472 (11.2 KiB)

```

Figura 91 Configuración de redes en easyids

8. Al iniciar la máquina de EasyIDS, de forma predeterminada iptables viene con unas reglas que impiden el tráfico de entrada y por lo cual no se puede enviar un ping, y no almacena ataques simples como los de nmap. Para cual se deben deshabilitar las reglas de iptables de esta forma se podrán ver los reportes de ataques de barrido de puertos como nmap. Para poder visualizar las reglas se digita “iptables-L”, ver figura 92.

```

Chain INPUT (policy ACCEPT)
target     prot opt source                destination
RH-Firewall-1-INPUT all -- anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
RH-Firewall-1-INPUT all -- anywhere              anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source                destination
ACCEPT    all  -- anywhere              anywhere
ACCEPT    icmp -- localhost.localdomain anywhere      icmp any
ACCEPT    all  -- anywhere              anywhere      state RELATED,ESTAB
ACCEPT    tcp  -- anywhere              anywhere      state NEW tcp dpt:ssh
ACCEPT    tcp  -- anywhere              anywhere      state NEW tcp dpt:http
ACCEPT    tcp  -- anywhere              anywhere      state NEW tcp dpt:https
DROP      all  -- anywhere              anywhere

```

Figura 92 Observación de lista de reglas de iptables

9. Para borrar reglas se digita “iptables- F”. Para conocer un poco de la guía de administración de EasyIDS, desde una maquina externa que tenga

permisos para ingresar al server se debe iniciar un navegador y digitar la IP de la interfaz de administración. A continuación se mostrará un mensaje de error ya que no se puede validar el certificado ya que se está a nivel de LAN, de modo que se debe pulsar “continuar de todos modos”, ver figura 93.



Figura 93 Ingreso a la interfaz desde otra máquina

10. A continuación solicitará que se ingresen el usuario y contraseña, y posteriormente solicitara que dicha contraseña se cambie por cuestiones de seguridad, luego se observará la interfaz de EasyIDS, para ir a la configuración de los diferentes servicios que ofrece este sistema se ingresa en “settings”, ver figura 94.



Figura 94 Interfaz de easyids

11. A continuación se pueden crear reglas e incluirlas en Snort, de modo que se ingresa a “/etc/snot: cd/etc/snot”. Aquí se en listan los archivos disponibles con el comando “ls”, ver figura 95.

```
[root@easyids snort]# ls
attribute_table.dtd      gen-msg.map             reference.config        snortrules.md5
backlog                 Makefile                snort.rules            threshold.conf
barnyard.conf           Makefile.am             sid-msg.map            unicode.map
bylog.waldo             Makefile.in             snort.conf
classification.config   response.rules          snort_rules.conf
```

Figura 95 Inicio de creación de reglas en snort

12. Aquí se puede observar algunos ficheros y directorios “subrayados en rojo”. Para crear las reglas se debe dirigir a “/etc/snort/rules”, de este modo se listan los archivos, ver figura 96.

```
[root@easyids rules]# ls
attack-responses.rules  misc.rules              specific-threats.rules
backdoor.rules         multimedia.rules        spyware-put.rules
bad-traffic.rules      mysql.rules             sql.rules
cgi-bin.list           netbios.rules          telnet.rules
chat.rules             nntp.rules             tftp.rules
content-replace.rules  open-test.conf         virus.rules
ddos.rules             oracle.rules            voip.rules
deleted.rules          other-ids.rules        VRT-License.txt
dns.rules              p2p.rules              web-activex.rules
dos.rules              policy.rules            web-attacks.rules
experimental.rules     pop2.rules             web-cgi.rules
exploit.rules          pop3.rules             web-client.rules
finger.rules           porn.rules              web-coldfusion.rules
ftp.rules              rpc.rules               web-frontpage.rules
icmp-info.rules        rservices.rules        web-iis.rules
icmp.rules             scada.rules            web-misc.rules
imap.rules             scan.rules              web-php.rules
info.rules             shellcode.rules        x11.rules
local.rules            smtp.rules
Makefile.am           snmp.rules
```

Figura 96 Listas de archivos de reglas de snort en easyids

13. Una vez identificadas las extensiones que manejan las reglas, se crea un fichero llamado “ping.rules”. De este modo se ingresa una regla como se muestra a continuación, ver figura 97.



```

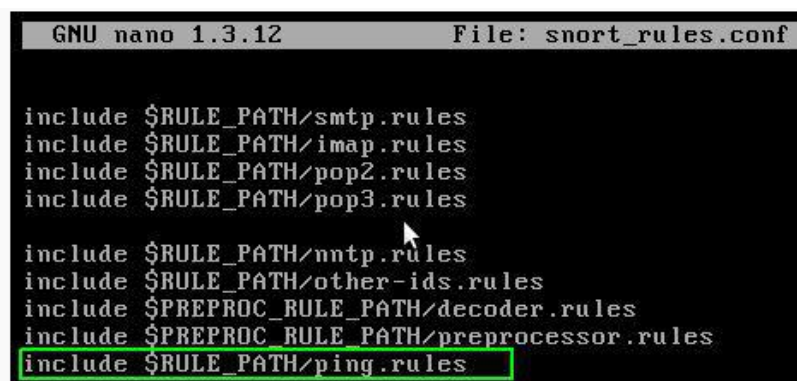
GNU nano 1.3.12      File: ping.rules      Modified
alert tcp 192.168.0.0/24 any -> any 1000:1024 (msg:"intento de acceso
tcp");
alert udp 192.168.0.0/24 any -> any 1000:1024 (msg:"intento de acceso
udp");

Get Help  WriteOut  Read File  Prev Page  Cut Text  Cur Pos
Exit      Justify    Where Is  Next Page  UnCut Text To Spell

```

Figura 97 Ingreso de regla con editor en el fichero ping.rules

14. Se guarda, de este modo se puede incluir una propia regla para lo cual se dirige a “/etc/snort/snort_rules”, y nuevamente “nano/etc/snort/snort_rules.conf” y se ingresará la ruta donde se encuentra el archivo “ping.rules”, ver figura 98.



```

GNU nano 1.3.12      File: snort_rules.conf

include $RULE_PATH/sntp.rules
include $RULE_PATH/imap.rules
include $RULE_PATH/pop2.rules
include $RULE_PATH/pop3.rules

include $RULE_PATH/mntp.rules
include $RULE_PATH/other-ids.rules
include $PREPROC_RULE_PATH/decoder.rules
include $PREPROC_RULE_PATH/preprocessor.rules
include $RULE_PATH/ping.rules

```

Figura 98 Inclusión de una propia regla snort

Se reinicia el Snort y de este modo está listo.

CAPÍTULO 4

PRUEBAS E IMPLEMENTACIÓN

4.1 Servicio de Proxy HTTP en Zentyal

Se define el servidor proxy HTTP, para disminuir el consumo de ancho de banda de la web en la red perimetral de la empresa Cemylub, incrementar la velocidad de navegación, determinar las políticas de acceso al internet y aumentar la seguridad bloqueando contenidos de alto riesgo.

4.1.1 Reglas de acceso

Después de haber realizado la configuración general, se tendrá que definir las reglas de acceso, por defecto Zentyal viene configurado con una regla de acceso la cual permite todo tipo de acceso, las políticas por omisión de regla siempre será la de denegar y la prioridad en el caso de que existan varias reglas será la que se encuentre más arriba como jerarquía, ver figura 99.

Proxy HTTP

Añadiendo un/a nuevo/a regla

Período de tiempo: De Para Días de la semana L M X J V S D

Período de tiempo en el cual se aplicará esta regla

Origen: Objeto de red Ventas

Decisión: Aplicar perfil de filtrado filtro_estricto

Figura 99 Creación de nueva regla

En el periodo de tiempo se puede determinar los días de la semana y el horario en cual se desea implementar la regla creada.

En el parámetro origen se fija a que elementos se aplicará la regla de acceso de un objeto de Zentyal a los usuarios de un determinado grupo. La tercera opción es aplicar la regla sobre cualquier tipo de tráfico que atraviese el proxy.

4.1.2 Filtrado de contenidos con Zentyal

Zentyal permite el filtrado de páginas web en base a su contenido. Se pueden definir múltiples perfiles de filtrado en Proxy HTTP y luego se selecciona perfiles de filtrado, ver figura 100.

Proxy HTTP
Perfiles de Filtrado

+ AÑADIR NUEVO/A

Nombre	Configuración	Acción
filtro_marketing		
filtro_general		
filtro_dev		

10 Página 1

Figura 100 Perfiles de filtrado

Accediendo a la configuración de estos perfiles, se podrá especificar diversos criterios para ajustar el filtro a nuestros certificados. En la primera pestaña podemos encontrar los Umbrales de contenido y el filtro del antivirus. Para que aparezca la opción de antivirus, el módulo Antivirus debe estar instalado y activado, ver figura 101.

Figura 101 Umbral de contenido

Estos dos filtros son dinámicos, es decir analizarán cualquier página en busca de palabras inapropiadas o virus. El umbral de contenidos puede ser ajustado para ser más o menos estricto, esto influirá en la cantidad de palabras inapropiadas que permitirá antes de rechazar una página.

En la siguiente pestaña Reglas de dominios y URL's se puede decidir de forma estática que dominios estarán permitidos en este perfil. Se decidirá bloquear sitios especificados sólo como IP, para evitar que alguien pueda evadir los filtros de dominios aprendiendo las direcciones IP asociadas. Así mismo con la opción Bloquear dominios y URL's no listados se mostrará si la lista de dominios más abajo se comporta como una blacklist o una whitelist, es decir, si el comportamiento por defecto será aceptar o denegar una página no listada, ver figura 102.

Dominio o URL	Decisión	Acción
facebook.com	Denegar	

Figura 102 Reglas de dominios y url

Finalmente, en la parte inferior, se tiene la lista de reglas, donde se puede especificar los dominios que se va a aceptar o denegar, como se muestra en la figura 103.

Para poder utilizar los filtros por categorías de dominios se debe crear y configurar una lista de dominios por categorías para el proxy HTTP – listas de categorías. Ahí se seleccionará el archivo que contiene la lista de URL's que se encuentran agrupadas en categorías destinada para el uso de filtros como Squidguardian o Dansguardian.



The image shows a web interface for configuring a Proxy HTTP. The main heading is 'Proxy HTTP' in green. Below it, the sub-heading is 'Añadiendo un/a nuevo/a listas por categorías'. The form contains the following elements:

- A 'Nombre:' label followed by a text input field containing 'shallalist'.
- An 'Archivo:' label with the word 'Opcional' in blue below it. To the right is a 'Choose File' button, followed by the text 'shallalist.tar.gz' and a checkmark icon.
- At the bottom, there are two buttons: a green button with a plus sign and the text 'AÑADIR', and a grey button with the text 'CANCELAR'.

Figura 103 Lista por categorías


Cuando se haya configurado la lista, se selecciona la determinada categoría que se va a permitir o no en la pestaña de categorías de dominio, en este caso como categorías en los dominios se tiene: sex/linguerie, shopping, solcialnet, spyware, tracker updatesites, urlshortener, violence, warez, weapons, antes de realizar todo este paso ya debían estar cargados la lista de dominios por categoría, ver figura 104.

Perfiles de Filtrado > shallalist

Configuración Reglas de dominios y URLs **Categorías de dominios** Tipos MIME Extensiones de archivo

Categorías de dominios



Categoría	Fichero de Listas	Lista Disponible	Decisión	Acción
sex/lingerie	shallalist	✓	Ninguno	
shopping	shallalist	✓	Ninguno	
socialnet	shallalist	✓	Ninguno	
spyware	shallalist	✓	Ninguno	
tracker	shallalist	✓	Ninguno	
updatesites	shallalist	✓	Ninguno	
urlshortener	shallalist	✓	Ninguno	
violence	shallalist	✓	Ninguno	
warez	shallalist	✓	Ninguno	
weapons	shallalist	✓	Ninguno	





















10  Página 7 de 8

Figura 104 Categorías de dominios

También se puede aceptar los diferentes tipos de contenidos y ficheros que van a ser aprobados por el perfil creado en la lista de categoría de dominios ya previamente cargada, este puede ser por MIME o por extensión de fichero, los de categoría MIME no es más que un identificador de formato en la web, en este caso se tiene: application/compress, application/futuresplash, application/gzip, application/java-vm, application/x-compress, application/x-gzip, application/x-shockwave-flash, application/zip, application/mpeg, ver figura 105.

Tipos MIME

+ AÑADIR NUEVO/A

Tipo MIME	Permitir <input checked="" type="checkbox"/>	Acción
application/compress	<input checked="" type="checkbox"/>	 
application/futuresplash	<input checked="" type="checkbox"/>	 
application/gzip	<input checked="" type="checkbox"/>	 
application/java-vm	<input checked="" type="checkbox"/>	 
application/x-compress	<input checked="" type="checkbox"/>	 
application/x-gzip	<input checked="" type="checkbox"/>	 
application/x-shockwave-flash	<input checked="" type="checkbox"/>	 
application/x-shockwave-flash2-preview	<input checked="" type="checkbox"/>	 
application/zip	<input checked="" type="checkbox"/>	 
audio/mpeg	<input checked="" type="checkbox"/>	 





10   Página 1 de 2  

Figura 105 Ficheros tipo mime

En la columna permitir se encuentra una casilla donde se va a seleccionar por defecto el denegar o aceptar todos los tipos enlistados. Además se cuenta con una interfaz para las extensiones de archivos descargados desde el proxy, ver figura 106.

Extensiones de archivo

+ AÑADIR NUEVO/A

Extensión	Permitir <input type="checkbox"/>	Acción
exe	<input type="checkbox"/>	 



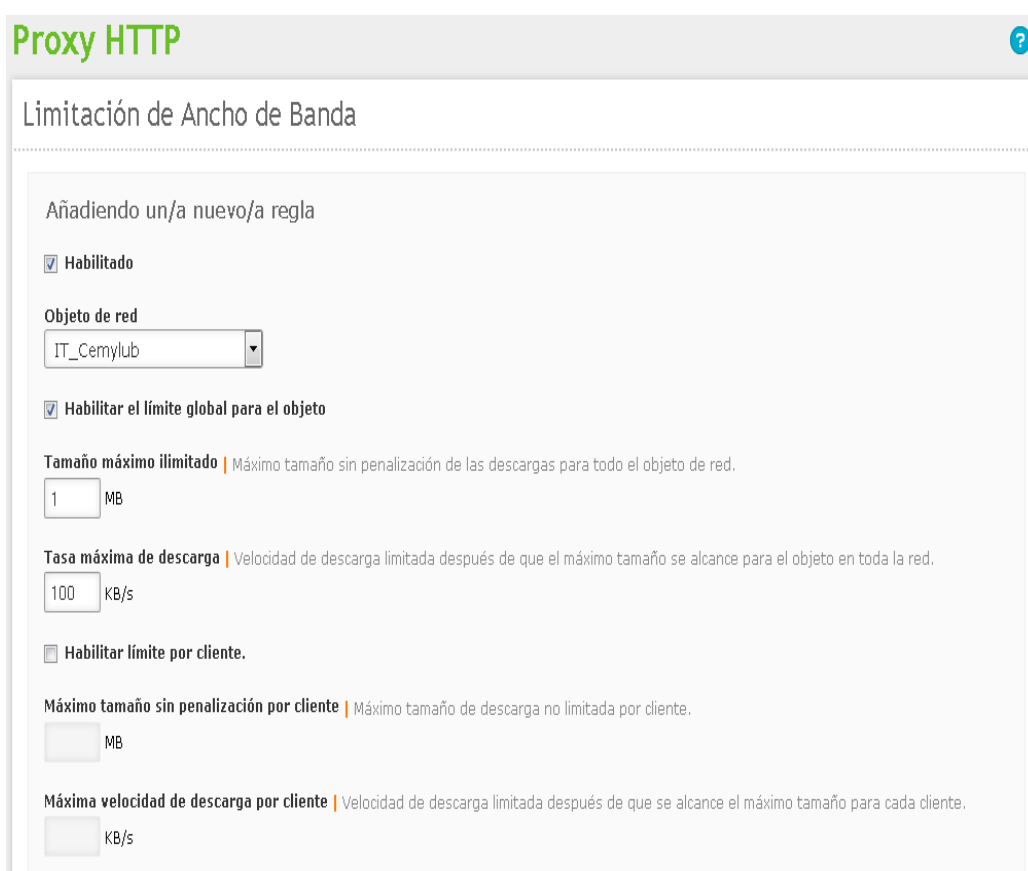
10   Página 1  

Figura 106 Extensiones de archivos

4.1.3 Limitación de ancho de banda

El proxy permite crear un límite para vigilar el ancho de banda que gasta cada usuario, el cual su funcionamiento consiste en el ancho de banda y la velocidad de descarga, este dependerá de las descargas del cliente, si el mismo hace un buen uso de la conexión se distribuirá correctamente su ancho de banda designado, ver figura 107 y 108.



Proxy HTTP ?

Limitación de Ancho de Banda

Añadiendo un/a nuevo/a regla

Habilitado

Objeto de red
IT_Cemylub

Habilitar el límite global para el objeto

Tamaño máximo ilimitado | Máximo tamaño sin penalización de las descargas para todo el objeto de red.
1 MB

Tasa máxima de descarga | Velocidad de descarga limitada después de que el máximo tamaño se alcance para el objeto en toda la red.
100 KB/s

Habilitar límite por cliente.

Máximo tamaño sin penalización por cliente | Máximo tamaño de descarga no limitada por cliente.
MB

Máxima velocidad de descarga por cliente | Velocidad de descarga limitada después de que se alcance el máximo tamaño para cada cliente.
KB/s

Figura 107 Creación de la regla de limitación de ancho de banda

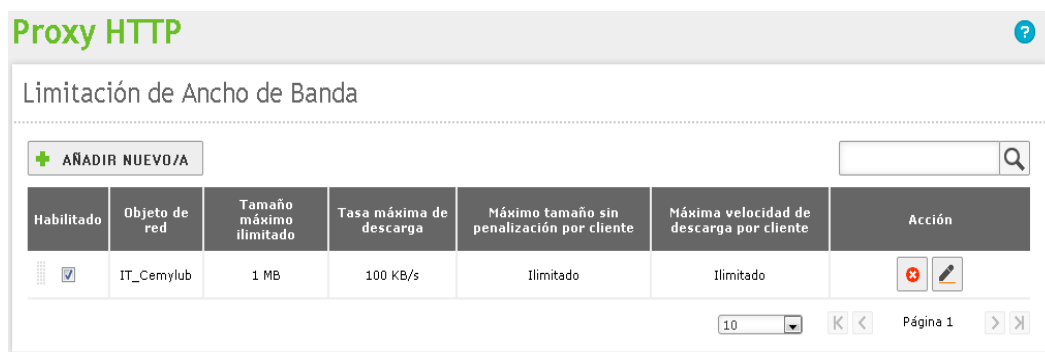


Figura 108 Regla creada de limitación de ancho de banda

4.2 Servicio de Firewall HTTP en Zentyal

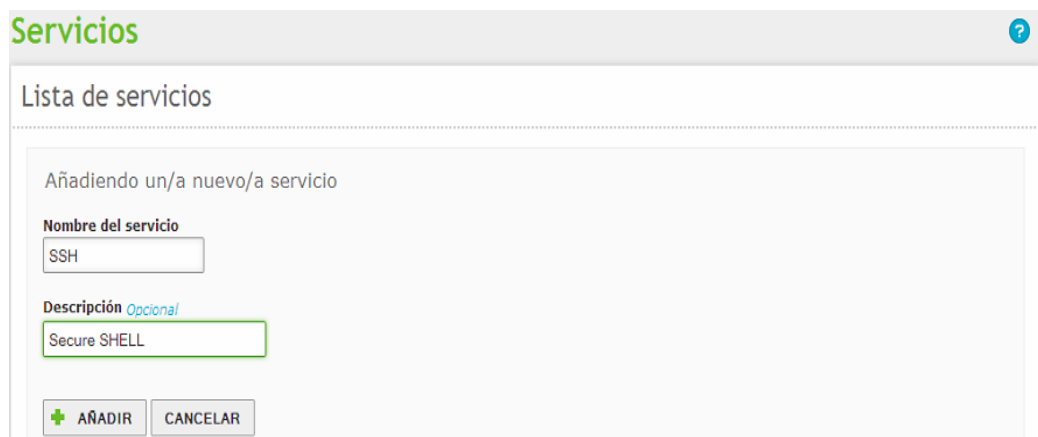
Las reglas para las interfaces externas es no permitir todo intento de una nueva conexión en Zentyal, así mismo para las interfaces internas es no permitir todos los intentos de conexión, a excepción de los servicios definidos por los módulos instalados, estos mencionados módulos son los que añaden las reglas al firewall, para luego permitir las conexiones y pueden ser modificadas por el administrador. Existe una excepción a esta norma que son conexiones al servidor LDAP, que adicionan la misma regla pero configurada para no permitir las conexiones por razones de seguridad. Se pueden determinar reglas en diferentes secciones, esto va a depender del flujo de tráfico que se desee aplicar como lo explica el gráfico 4.10.

4.2.1. Tráfico de redes internas a Zentyal

Tráfico entre redes internas y de redes internas a Internet (ejemplo: restringir el acceso a todo Internet o determinadas direcciones a unas direcciones internas o restringir las comunicaciones entre las subredes internas).

Para realizar el bloqueo mediante firewall de algunos puertos determinados, se debe crear el servicio con el puerto que se va habilitar o a

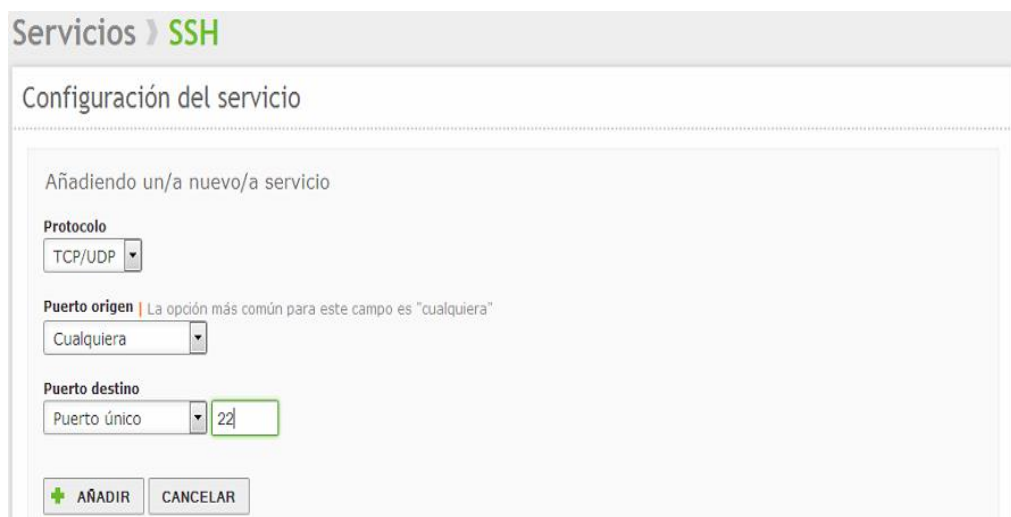
bloquear. En este caso se ha creado el servicio SSH en la pestaña de red para no poder tener acceso como se muestra en la figura 109.



The screenshot shows a web interface titled 'Servicios' with a sub-header 'Lista de servicios'. Below this, there is a section for adding a new service. The form includes a text input for 'Nombre del servicio' containing 'SSH' and a text input for 'Descripción Opcional' containing 'Secure SHELL'. At the bottom of the form are two buttons: 'AÑADIR' (Add) and 'CANCELAR' (Cancel).

Figura 109 Creación del servicio SSH

Una vez creada la regla, se indica que puerto único es el que se va a determinar para el mencionado servicio como lo muestra la figura 110.



The screenshot shows the 'Configuración del servicio' (Service Configuration) page for 'SSH'. The form includes a dropdown for 'Protocolo' set to 'TCP/UDP', a dropdown for 'Puerto origen' set to 'Cualquiera', and a dropdown for 'Puerto destino' set to 'Puerto único' with the value '22' entered in the adjacent text input. At the bottom are 'AÑADIR' and 'CANCELAR' buttons.

Figura 110 Puerto destino del servicio ssh

A continuación se muestra en la figura 111 ya creado el servicio SSH para poder utilizarlo en las reglas de filtrado de paquetes.



Figura 111 Servicio ssh creado

En el filtrado de paquetes se va a denegar el acceso al servicio SSH a todas las estaciones que pertenezcan al departamento IT_Bodega, tal como lo muestra la figura 112.

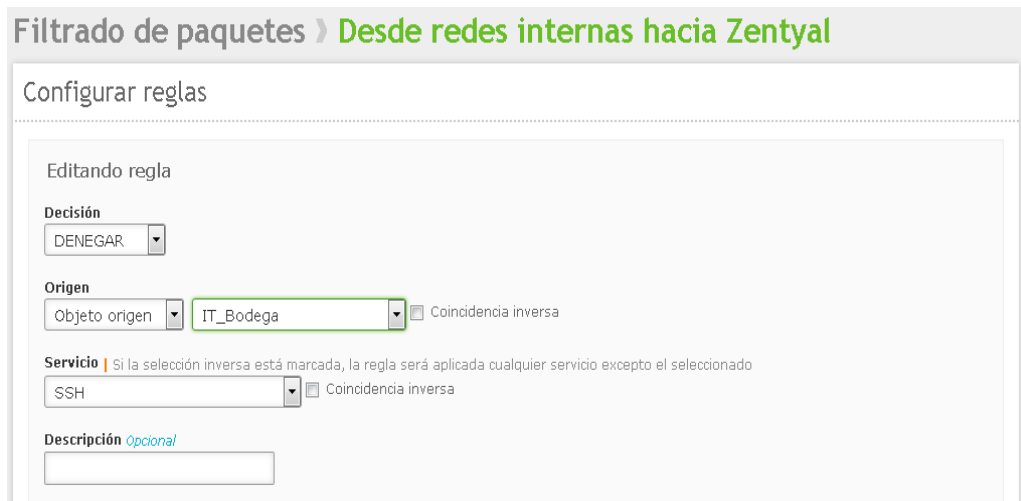


Figura 112 Creación de la regla de bloqueo con el servicio ssh

A continuación para comprobar que el puerto en mención se encuentre bloqueado, se abre un cliente SSH a través de la interfaz PUTTY para poder

acceder a la dirección IP del departamento IT_Bodega como se muestra en la figura 113.

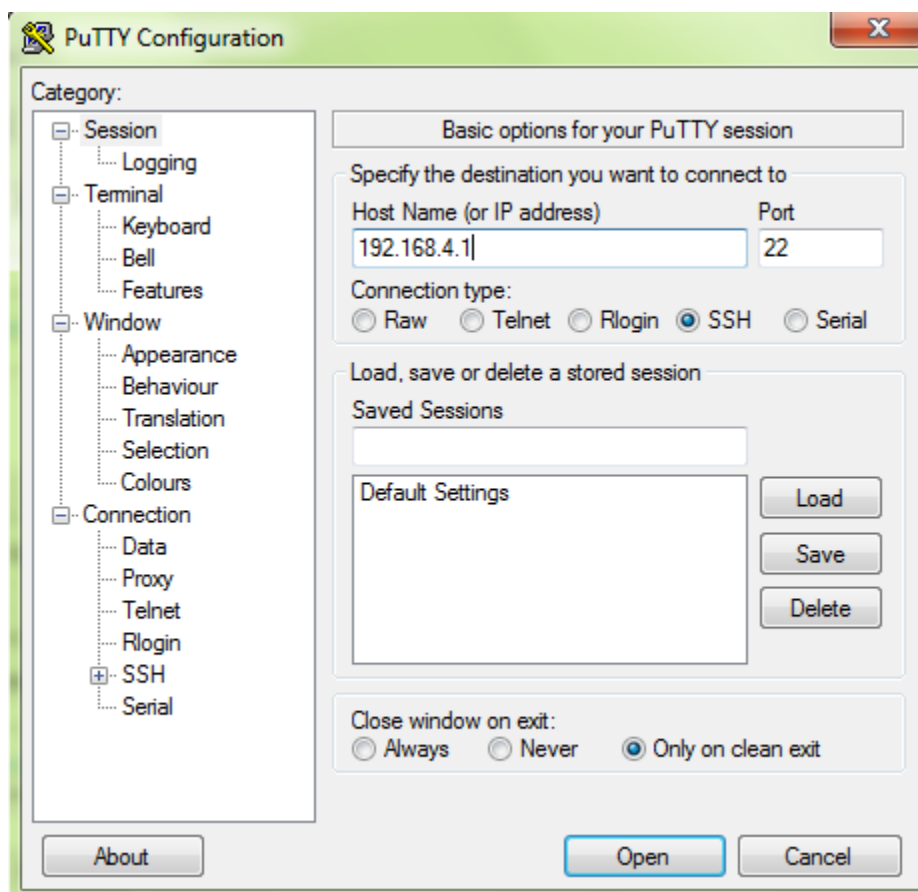


Figura 113 Accediendo a it_bodega desde putty

Una vez que se desea ingresar a la estación en mención muestra un mensaje de error de conexión, ya que mediante la regla de filtrado se ha bloqueado al puerto 22, tal como se muestra en la figura 114.

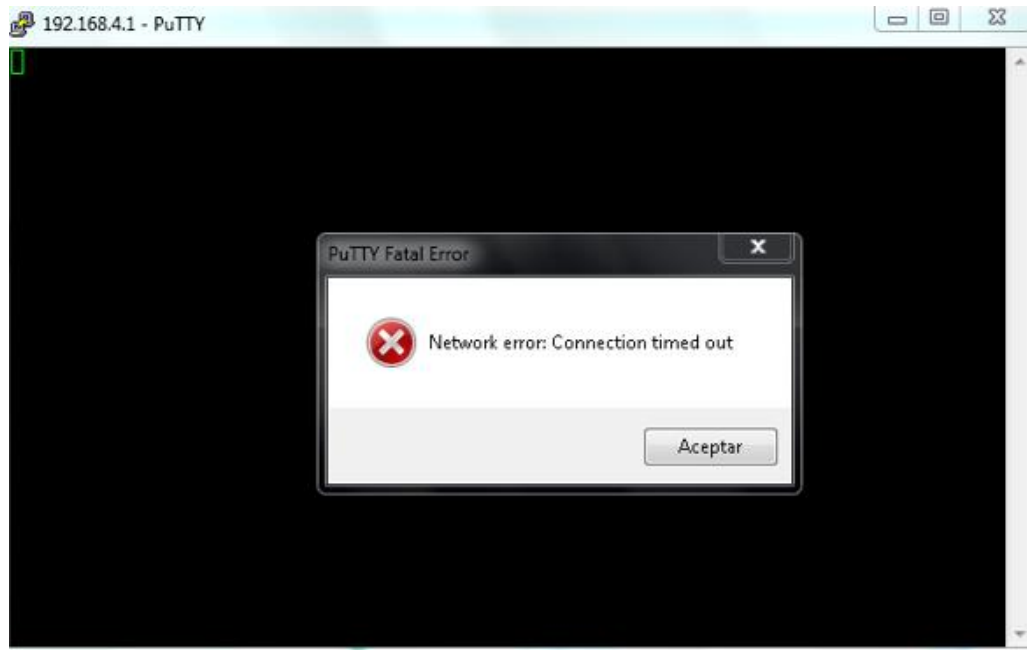


Figura 114 Pantalla de error de conexión en la interfaz Putty

Como segunda comprobación se abre una pantalla de cmd y se realiza un telnet a la dirección IP con el respectivo puerto, dando como resultado una pantalla que no accede a la petición que se ha realizado, como se muestra en la figura 115.

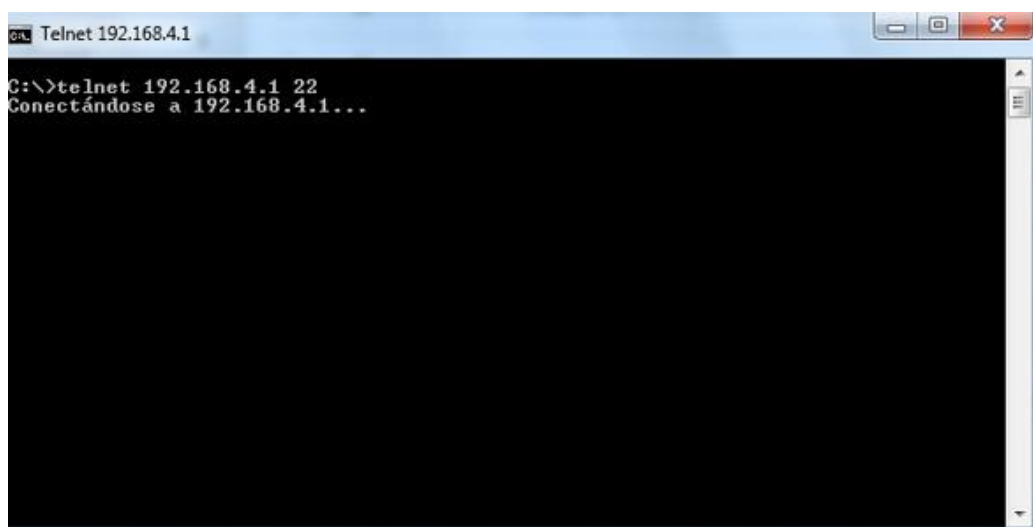


Figura 115 Pantalla de telnet

Esta vez se ha creado un servicio con nombre Zimbra para bloquear la administración a un departamento determinado. A continuación se crea el servicio como se muestra en la figura 116.

The screenshot shows a web interface titled 'Servicios' with a sub-header 'Lista de servicios'. Below this, there is a form for adding a new service. The form includes a text input for 'Nombre del servicio' containing 'Zimbra', and another text input for 'Descripción Opcional' containing 'Administracion Zimbra'. At the bottom of the form are two buttons: 'AÑADIR' (with a plus icon) and 'CANCELAR'.

Figura 116 Creación del servicio zimbra

Luego se determina el puerto con el cual se accede a la administración de Zimbra como se muestra en la figura 117.

The screenshot shows the configuration page for the 'Administracion Zimbra' service. The page title is 'Servicios > Administracion Zimbra' and the sub-header is 'Configuración del servicio'. The main content area is titled 'Editando servicio' and contains the following configuration options:

- Protocolo:** A dropdown menu set to 'TCP/UDP'.
- Puerto origen:** A dropdown menu set to 'Cualquiera', with a note: 'La opción más común para este campo es "cualquiera"'. Below the dropdown is a small text input field.
- Puerto destino:** A dropdown menu set to 'Puerto único' and a text input field containing '7071'.

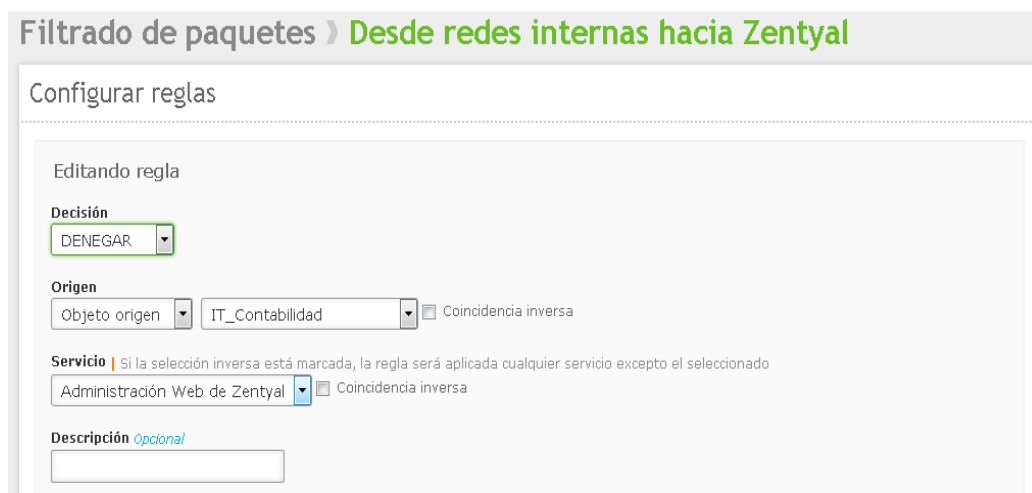
At the bottom of the configuration area are two buttons: 'CAMBIAR' and 'CANCELAR'. Below this is a table summarizing the service configuration:

Protocolo	Puerto origen	Puerto destino	Acción
TCP/UDP	cualquiera	7071	[Icons: delete, edit, refresh]

At the bottom right of the page, there is a pagination control showing '10' items per page, navigation arrows, and 'Página 1'.

Figura 117 Puerto destino del servicio zimbra

A continuación se crea la regla de filtrado de paquetes, donde el departamento de IT_contabilidad no va a poder acceder a la navegación de la administración de Zimbra, tal como se muestra en la figura 118.



The screenshot shows a web interface titled "Filtrado de paquetes" with a sub-header "Desde redes internas hacia Zentyal". Below this is a section "Configurar reglas" containing a form for editing a rule. The form includes the following fields:

- Editando regla**
- Decisión:** A dropdown menu set to "DENEGAR".
- Origen:** A dropdown menu set to "Objeto origen" and another dropdown menu set to "IT_Contabilidad". There is a checkbox for "Coincidencia inversa" which is unchecked.
- Servicio:** A dropdown menu set to "Administración Web de Zentyal". There is a checkbox for "Coincidencia inversa" which is unchecked. A note above the dropdown reads: "Si la selección inversa está marcada, la regla será aplicada cualquier servicio excepto el seleccionado".
- Descripción:** A text input field with the label "Descripción *opcional*".

Figura 118 Creación de la regla para el servicio zimbra

A continuación se intenta acceder a la dirección <https://mail.cemylub.com:7071> y muestra un mensaje en el cual indica que no se puede abrir la página de administración, como se muestra en la figura 119, donde en el navegador se encuentra totalmente bloqueado, mostrando un error al intentar recuperar el dominio escrito y da como acceso denegado, ya que está dentro de la regla creada.



Figura 119 Pantalla de bloqueo hacia el administrador de zimbra

4.3 Servicio de correo electrónico utilizando Zimbra Collaboration Suite 8.0.7.

4.3.1 Interfaz web de administrador

Para poder entrar al sistema se dirige a la dirección del administrador, se introduce el usuario y la contraseña, además de escoger el tipo de cliente que se desee usar estas opciones son: avanzado (Ajax), Normal (HTML) o móvil. Presionar el botón “log in”.

Para poder cambiar la contraseña se debe pulsar la pestaña “preferencias” y a continuación cambiar “contraseña” en la cual solicitara que se digite la contraseña actual y después las nueva contraseña dos veces una vez realizado esto pulsar “cambiar contraseña” de esta manera se guardarán los cambios realizados, ver figura 120.

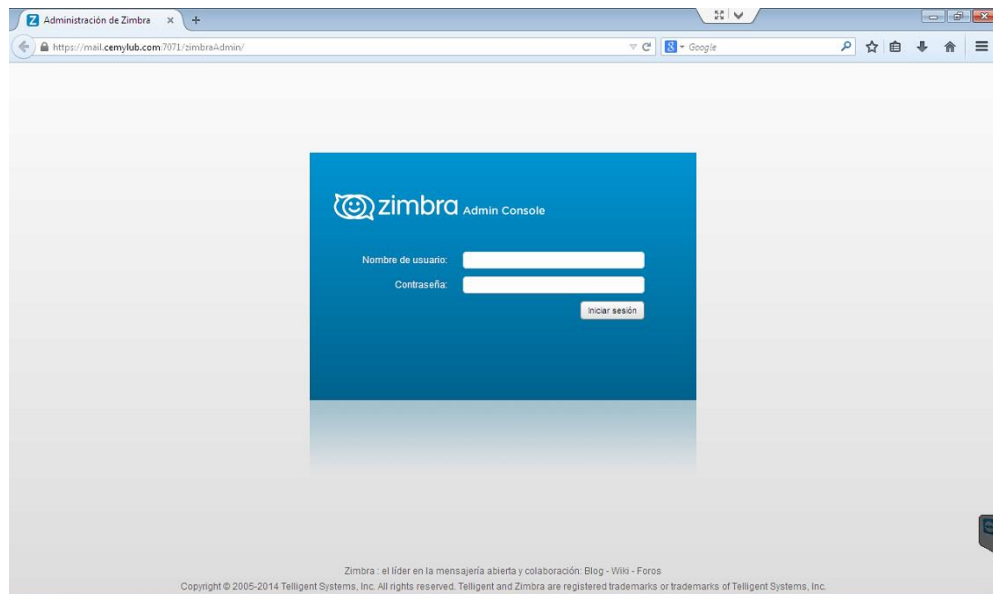


Figura 120 Ingreso al interfaz web de administrador

Una vez que se haya ingresado como administrador se va a encontrar tres frames correctamente delimitados, en la parte de la izquierda el menú de acciones, en la parte del centro el resultado del menú y en la parte derecha lo que son las tareas pendientes en el servidor, ver figura 121.

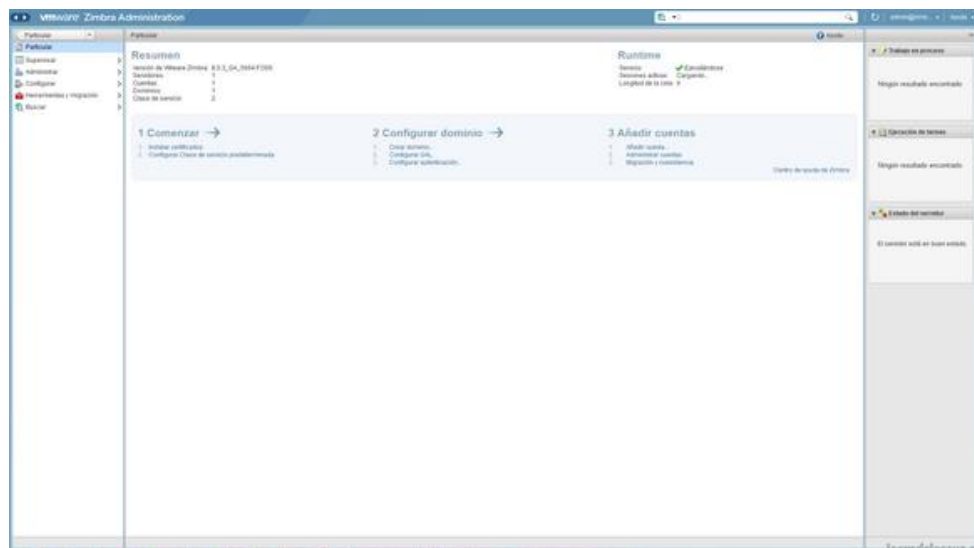


Figura 121 Interfaz web de administrador

En el menú “particular”, se encuentra toda la información con respecto al servidor de correo Zimbra, ya que muestra una lista donde se puede visualizar el número de cuentas existentes, la versión de Zimbra Collaboration Suite que se está ejecutando, el número de servidores en el que se está trabajando y los dominios que se están utilizando, además muestra la última copia de seguridad realizada. También existen unas opciones para la configuración del dominio y la creación y administración de cuentas, alias, migración y listas de correos como se puede visualizar en la figura 122.



Figura 122 Menú particular

Si se desea crea una nueva cuenta de correo electrónico, se da click en “añadir cuenta” y se abre una interfaz donde se debe llenar los campos: nombre de correo, nombre y apellido del usuario, así la contraseña (esta puede ser cambiada por el usuario una vez que ingrese por primera vez con la contraseña asignada temporalmente) como se muestra en la figura 123.

Figura 123 Creación de una nueva cuenta

En la opción “Supervisar” se encuentran datos estadísticos sobre lo que es: estado del servidor, estadísticas avanzadas, número de mensajes, volumen de mensajes, actividad antispam/antivirus, estadísticas móviles, estadísticas del servidor y colas de correo como se muestra en la figura 124.

Servidor	Servicio	Hora
mail.cemylub.com	spell	18 de Septiembre 2014 13:16
mail.cemylub.com	mailbox	18 de Septiembre 2014 13:16
mail.cemylub.com	logger	18 de Septiembre 2014 13:16
mail.cemylub.com	mta	18 de Septiembre 2014 13:16
mail.cemylub.com	stats	18 de Septiembre 2014 13:16
mail.cemylub.com	antispam	18 de Septiembre 2014 13:16
mail.cemylub.com	zmconfigd	18 de Septiembre 2014 13:16
mail.cemylub.com	ldap	18 de Septiembre 2014 13:16
mail.cemylub.com	opendkim	18 de Septiembre 2014 13:16
mail.cemylub.com	antivirus	18 de Septiembre 2014 13:16
mail.cemylub.com	snmp	18 de Septiembre 2014 13:16

Figura 124 Creación de una nueva cuenta

En la opción “Configurar” se encuentra la clase de servicio, en esta versión se incluye la opción de defaultExternal, la cual sirve para la administración de carpetas y calendarios compartidos para usuarios externos, además se encuentra la configuración general y los zimlests

disponibles que se encuentran para esta versión como se muestra en la figura 125.

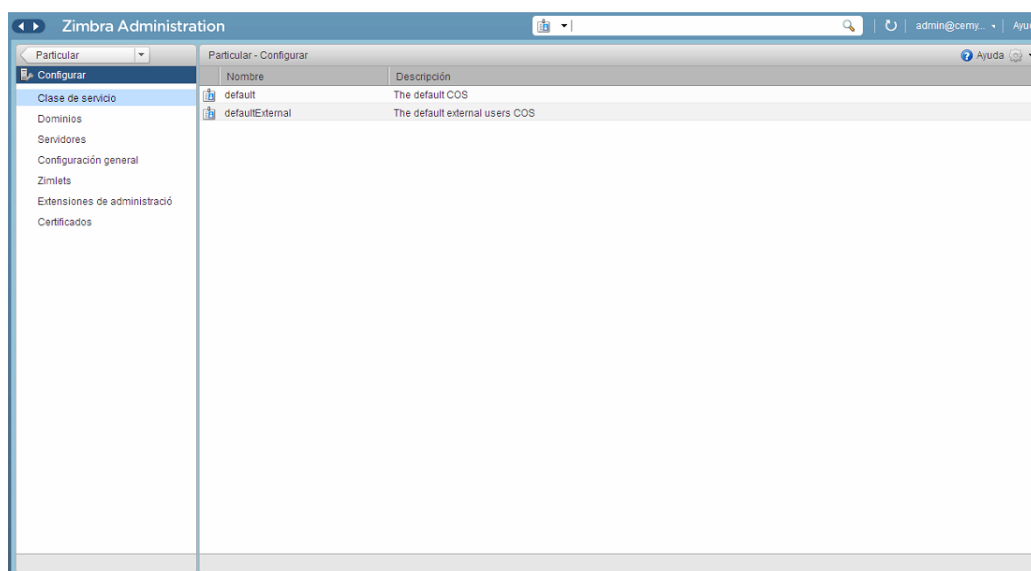


Figura 125 Configuración general

4.3.2 Interfaz web de usuario

4.3.2.1 Aplicaciones de Zimbra

Una vez que se ingresa al sistema se pueden observar las diferentes aplicaciones que ofrece zimbra las cuales son: correo, libreta de direcciones, agenda, tareas, mensajería instantánea (mi beta), bloc de notas, maletín y preferencias.

En la parte superior izquierda el sistema muestra el nombre del usuario además del espacio que se ocupa en el servidor, el administrador puede configurar cuotas de espacio y de ser el caso también se mostrará cuanto de espacio se encuentra ocupando. Debajo del nombre también se muestran las diferentes carpetas y subcarpetas en donde se almacenan y clasifican los correos. A continuación se encuentran las etiquetas y los Zimlets que son

aplicaciones que se utilizan para poder recibir información de diferentes sistemas y un calendario en el que se puede pulsar la fecha para ver la agenda del día, ver figura 126.

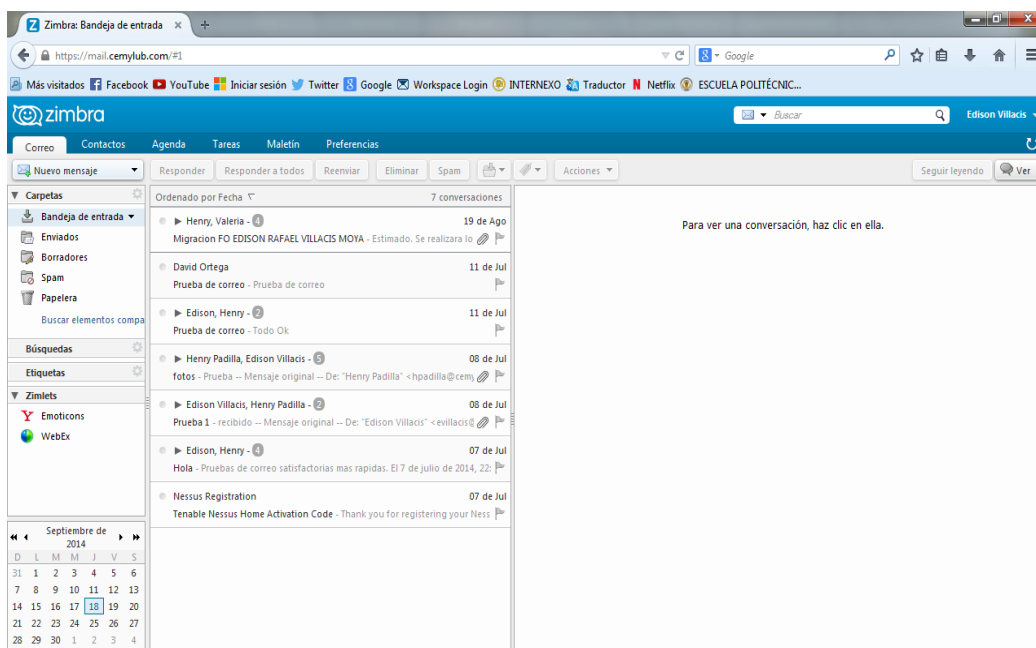


Figura 126 Interface de usuario en zimbra

4.3.2.2 Configuración de preferencias en zimbra

Por defecto zimbra ya viene configurado, pero se pueden realizar cambios ajustando las opciones mostradas en la pestaña “preferencias” en la cual se observa las opciones: general, correo, redactar, firmas, libreta de direcciones, cuentas, filtros de correo, agenda, mensajería instantánea, y accesos directos. Para asegurar los cambios realizados se debe pulsar el botón “guardar” el cual se encuentra a la izquierda, encima de la barra de herramientas.

Algunos detalles importantes de las opciones de configuración son los siguientes, ver figura 127.

- **Correo.** Se puede configurar cada cuanto se actualizará el buzón de entrada con correo nuevo. Se puede cargar el correo nuevo al buzón de entrada al tocar el botón “ver correo” cuando se encuentre en la aplicación de correo. En esta opción también se puede configurar el mensaje que se desplegara cuando el usuario este fuera de la oficina ya sea por un viaje o vacaciones, para hacerlo se debe marcar la casilla “enviar respuesta por ausencia” e introducir el texto que se quiera mostrar.
- **Redactar.** si se quiere redactar mensajes con diferentes tipos de letra, colores e imágenes, se debe seleccionar redactar mensajes en HTML.
- **Firmas.** En esta opción se puede crear múltiples firmas para los correos electrónicos, cada una con un nombre único.
- **Cuentas.** se puede definir aquí la firma por defecto a usar en todos los correos electrónicos. Cuando se cree un nuevo correo se podrá escoger otra firma o no firmar el correo.
- **Accesos directos.** Esta opción le permite al usuario configurar combinaciones de teclas para acceder rápidamente a diferentes opciones.

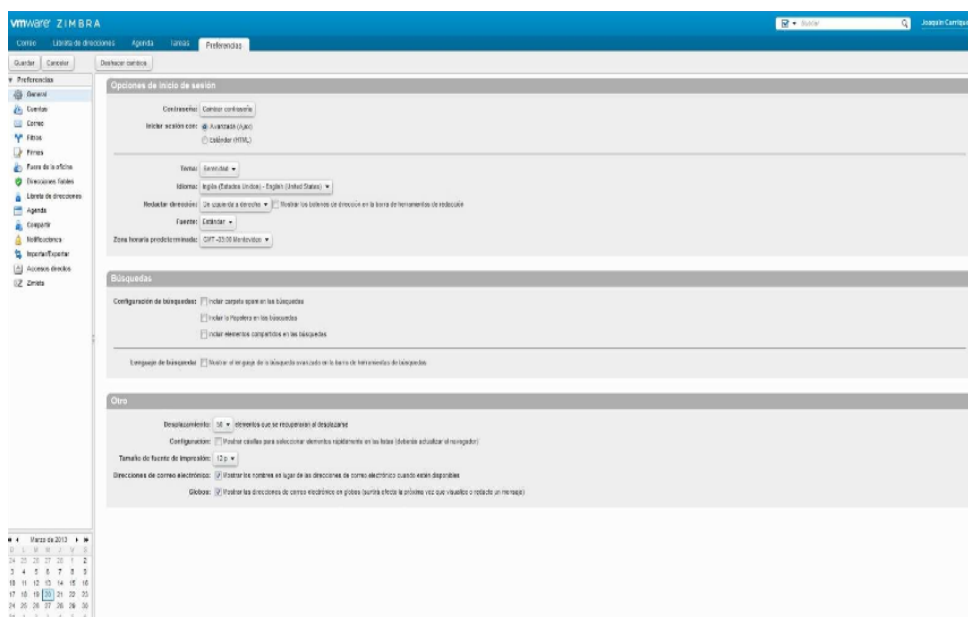


Figura 127 Ventana de preferencias en zimbra

4.3.2.3 Uso del correo electrónico

Para ordenar los correos electrónicos se debe tocar cualquier campo de la ventana para ver el correo. Por ejemplo, para ordenar los correos por fecha se puede tocar el campo “marcado como recibido”.

El número de mensajes desplegados en el buzón de entrada es controlado en la opción de preferencias. Si se tiene más mensajes que los que se muestran se debe usar las flechas que se encuentran en la parte derecha de la barra de herramientas para poder pasar al siguiente grupo de mensajes. Haciendo doble clic en algún mensaje, se podrá ver el mensaje en una ventana más grande o en una ventana separada esto se puede ajustar en la ventana de “preferencias”, la opción de “spam”, permitirá clasificar el mensaje como spam.

El uso del correo también permite imprimir, para realizarlos se debe presionar el icono de la impresora en la barra de herramientas y escoger la

opción “Imprimir”. El mensaje se abrirá en una gran ventana junto a una caja de dialogo de impresión.

Para poder crear un nuevo mensaje se debe presionar el botón de “nuevo” en la barra de herramientas. Se mostrará la página para crear un nuevo correo electrónico. Presionando las teclas “shif + c” se abrirá una nueva ventana para poder redactar los mensajes. En la creación del mensaje el usuario debe completar los campos de dirección como son: asunto, para, cc; conforme se inicie la digitación de la dirección, zimbra mostrara las direcciones de los correos de la lista global de los contactos “global address list (GAL)” y el usuario podrá seleccionar las direcciones electrónicas a las cuales quiera enviar el mensaje. Existen algunas herramientas que permiten realizar correcciones como por ejemplo “comprobar ortografía” otras que permiten enviar correo con archivos adjuntos y guardar mensajes que son interrumpidos como borradores también se puede añadir firma en la ventana de preferencias.

Zimbra también permite usar filtros de correo, los cuales se pueden crear, modificar o eliminar en la opción “preferencias-filtros de correo”, el uso de carpetas y etiquetas que permiten administrar mucho mejor los correos del usuario, un correo se puede guardar en una carpeta presionando el botón “mover elementos seleccionados” o con el botón derecho de ratón y escogiendo la opción “mover”. Para crear una carpeta presione el botón derecho del ratón sobre el título “carpetas”, además de que las carpetas pueden tener subcarpetas, ver figura 128.

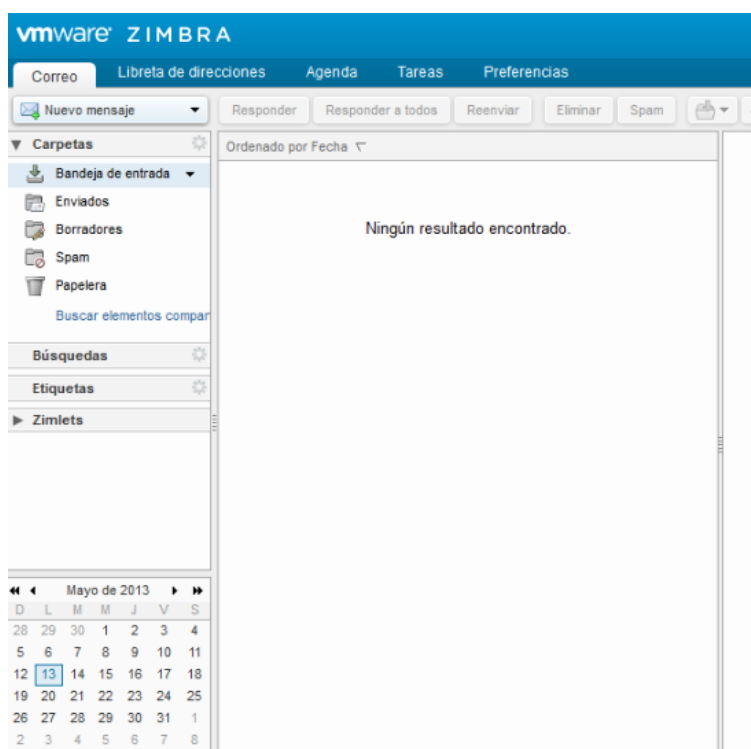


Figura 128 Partes de la ventana del correo

4.3.2.4 Librería de direcciones

Zimbra permite agregar contactos en la opción de contactos, existe una opción llamada “contactos profesionales” estos solo pueden ser agregados por el administrador, en la opción de contactos personales el usuario puede agregar sus propios contactos. Para ver los nombres y direcciones de la lista global, el usuario debe escribir el apellido o nombre que se quiere buscar como se muestra a continuación, ver figura 129.

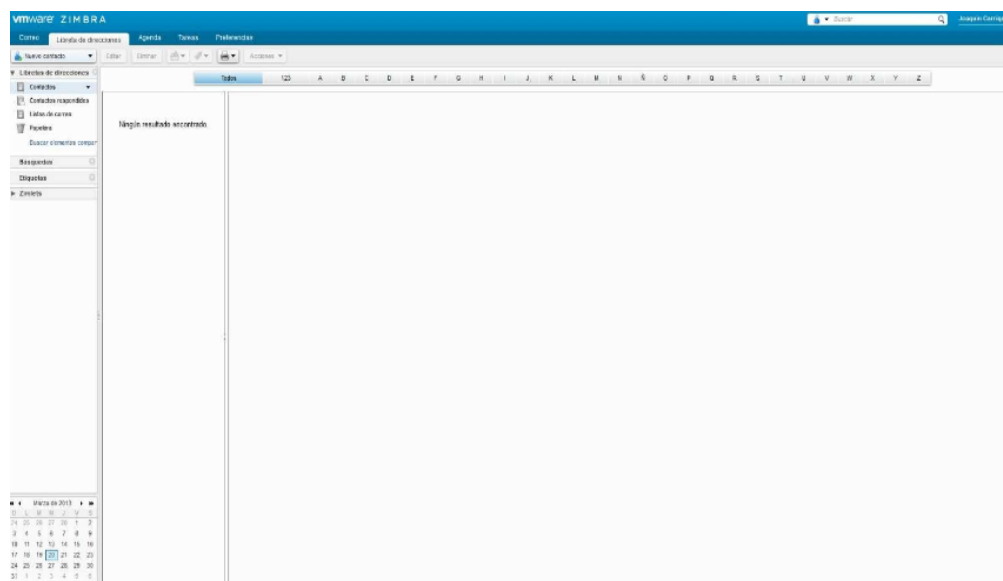


Figura 129 Búsqueda de un contacto en zimbra

4.3.2.5 Uso del calendario

En el calendario el usuario puede añadir citas, dirigiéndose a la barra de herramientas tocando la flecha hacia abajo que se encuentra a la derecha del botón “nuevo” seleccionar la opción de “nueva cita”. El campo de asunto es obligatorio llenarlo. La información digitada en este campo será la información que se desplegará luego en el calendario. Si se quiere usar alguno de los salones de la empresa se debe utilizar la opción de “buscar ubicaciones”, también se debe configurar la fecha y la hora de la cita.

Digitar la fecha y hora de inicio en “inicio” o también el usuario puede tocar la flecha para desplegar un calendario y escoger una fecha, seleccionar la fecha y hora que finalizara la cita en “fin”. Esta aplicación permite que el usuario tenga múltiples calendarios, tocando el botón “agenda”, puede escoger el usuario en que calendario quiere guardar una cita. En el campo de “asistentes” el usuario puede agregar los participantes, los nombres de estos pueden buscarse usando el botón “buscar asistentes” usando como fuente la “librería general de direcciones”. El usuario puede

también agregar recursos como: salones, proyectores, etc. que se necesitaran para dicha cita, en el campo de “recursos” se pueden digitar estos insumos, ver figura 130.

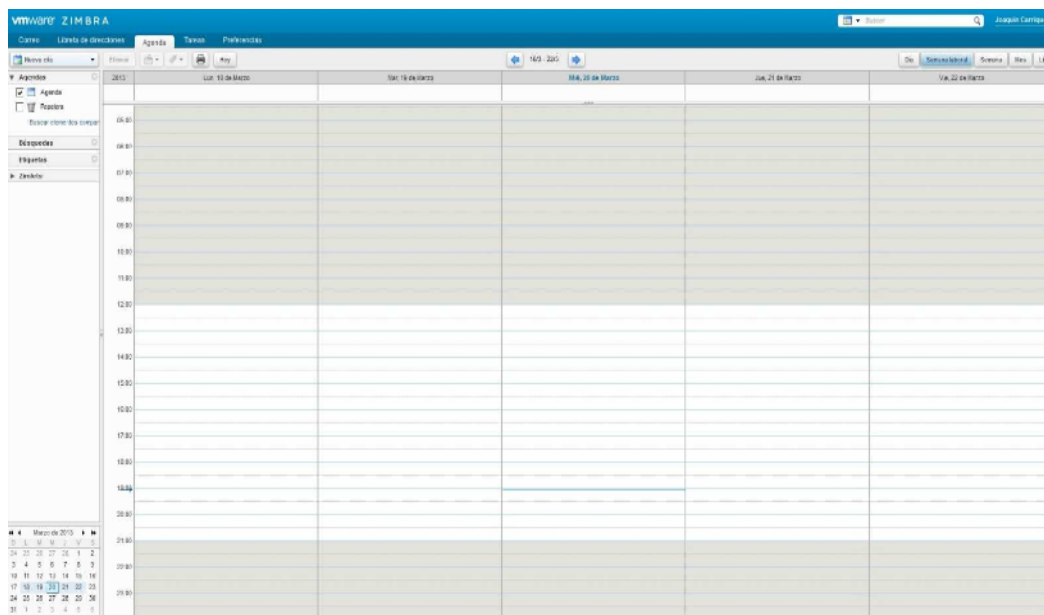


Figura 130 Uso del calendario en zimbra

4.3.2.6 Opción de tareas

En la opción de tareas se encuentra una barra de aplicaciones, donde muestra un botón “nuevo” y aparece una interfaz donde se anota la información de la tarea, para los cuales se tiene: asunto, ubicación, prioridad, fecha de inicio, fecha de entrega, descripción de la tarea, control de avance de la tarea y el espacio para la descripción.

La lista de tareas indicará el avance de cada uno en porcentaje y fecha de entrega, para poder ser visualizadas las tareas pendientes se tiene que ingresar al menú de tareas, ver figura 131.

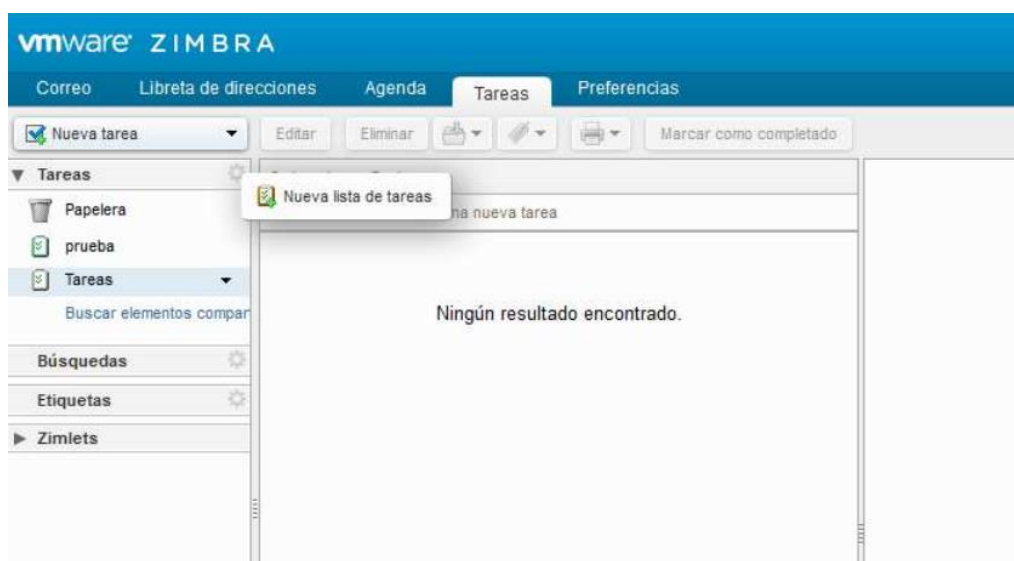


Figura 131 Opción de tareas

Una vez que se haya creado y determinada la tarea y ubicada en la lista, la misma se puede compartir con los demás usuarios. Estas tareas se mostraran en sus listas pertenecientes y se podrá visualizar su estado en % de realización y en fecha de entrega, ver figura 132.

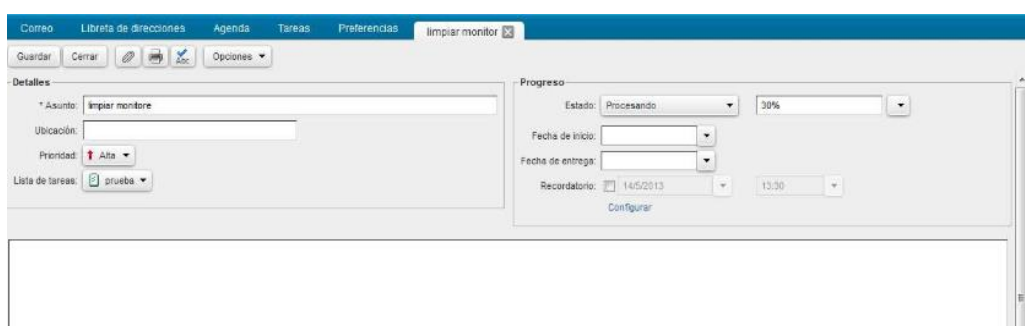


Figura 132 Detalles de la tarea

4.3.2.7 Etiquetas

En Zimbra existe la opción para realizar etiquetas que ayudan a clasificar y mantener el orden de los correos electrónicos, los componentes del calendario, contactos y tareas al momento de realizar una búsqueda. Existen

unas restricciones que se debe tomar en cuenta al momento de crear los nombres de etiqueta que pueden incluir cualquier carácter a excepción de los dos puntos (:), barra diagonal (/) o comillas (“). También al momento de suprimir una etiqueta, esta se va a eliminar de todo elemento que la tenga y no se elimina el artículo mismo, ver figura 133.

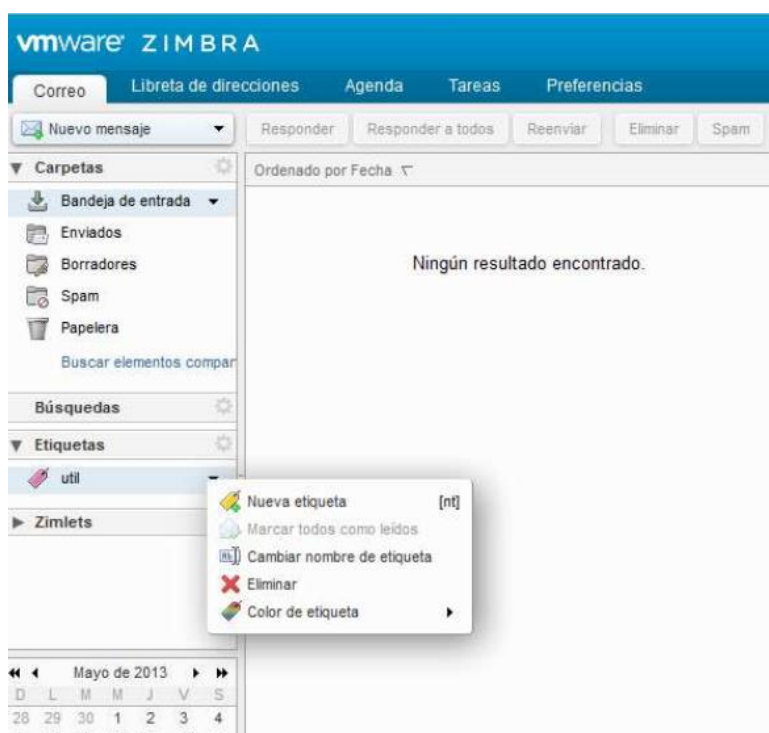


Figura 133 Creación de etiquetas

Zimbra pone a disposición la opción de almacenar cualquier archivo en el maletín de Zimbra, de igual manera se puede acceder desde cualquier lugar con conexión a internet, para guardar archivos en esta opción en la pestaña de maletín se debe crear en el botón “nuevo”, luego de desplegará la interfaz para almacenar el archivo en el maletín y se guardará en el servidor de correo.

4.4 Snort en EasyIDS

Una vez instalado y configurada la herramienta de EasyIDS, se la puede administrar de manera sencilla en su interfaz web, para lo cual se tiene unas opciones en el menú.

4.4.1 Menú de administración

- **Analysis:** Es una de las secciones más relevantes de EasyIDS, ya que permite analizar el comportamiento de Snort a través de su interfaz base, como se muestran en las figuras 134 y 135, y así poder mostrar la actividad del sistema, con sus respectivas alertas generadas.

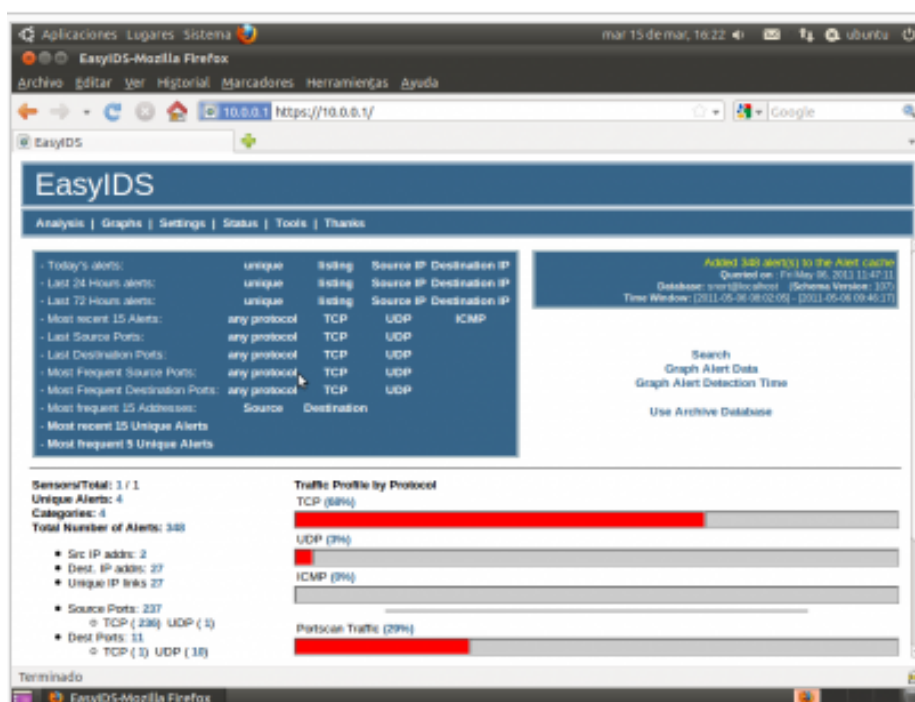


Figura 134 Interfaz base de snort

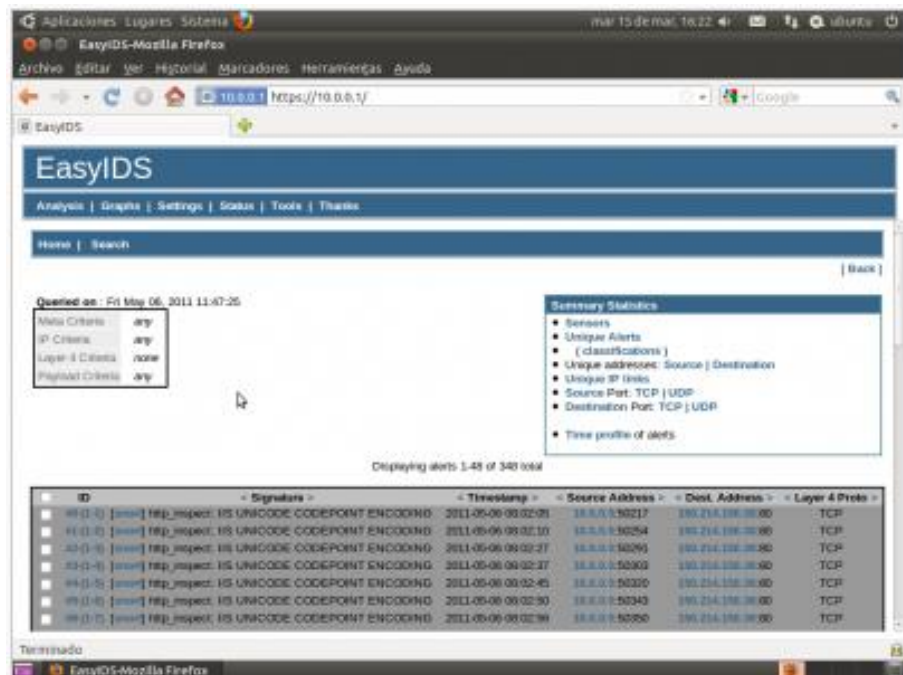


Figura 135 Alertas generadas

- **Graphs:** En esta opción se puede visualizar los gráficos de rendimiento con relación al tráfico de red como se muestra en el gráfico 4.38, el del sistema en la figura 136 y el de Snort en la figura 137.

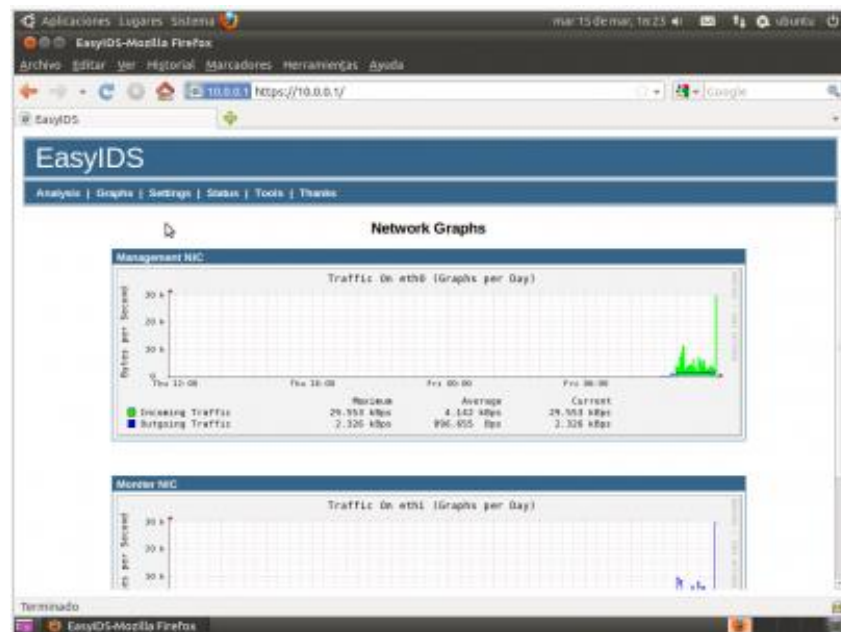


Figura 136 Tráfico de red

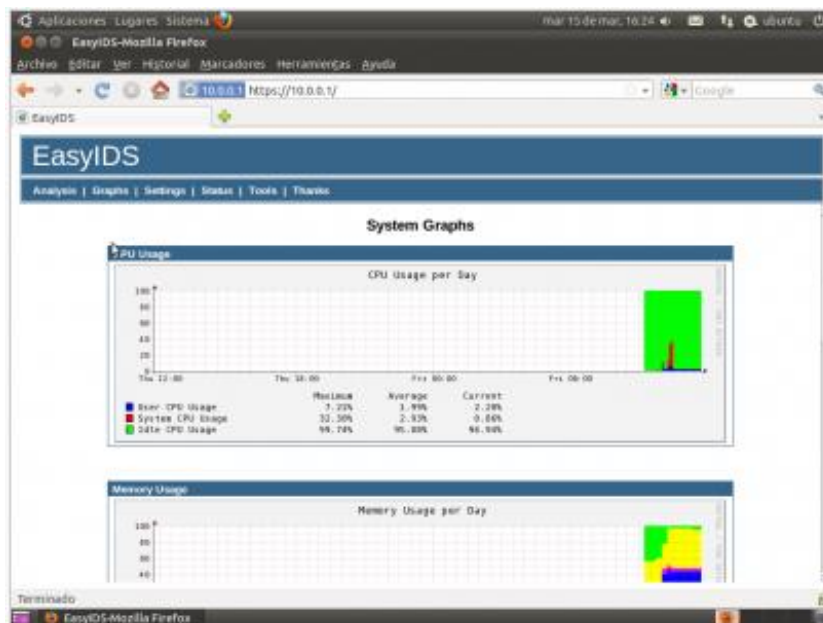


Figura 137 Rendimiento del sistema

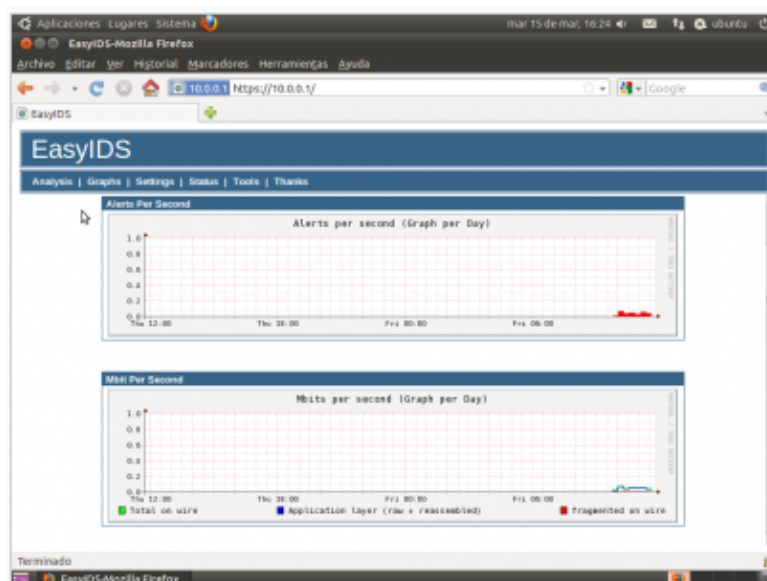


Figura 138 Rendimiento de Snort

- **Settings:** En esta opción se configura los elementos más importantes del sistema como arpwatc, barnyard, easyIDS, snort, stop y stunnel, ver figura 139.



Figura 139 Menú de ajustes

- **Status:** Comprueba el estado del sistema y de todos los servicios que se ejecutan dentro del mismo, ver figura 140.

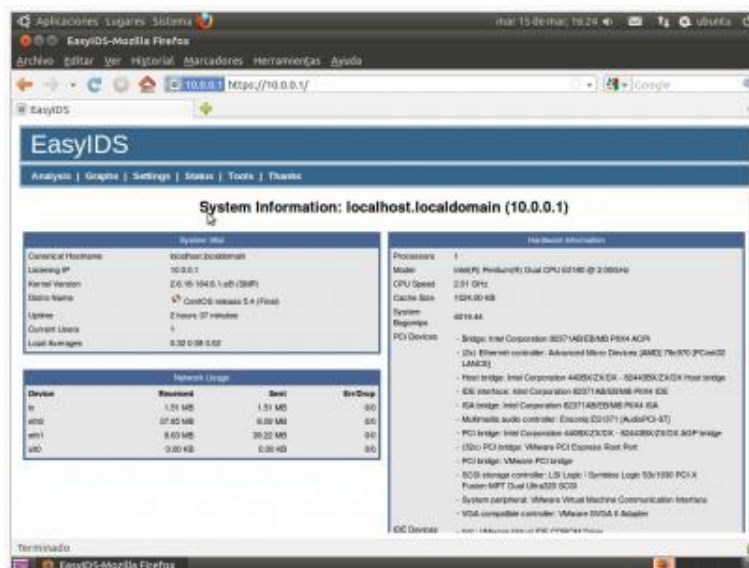


Figura 140 Estado del sistema

- **Tools:** Aquí se encuentra la herramienta nmap, el cuál escanea equipos y logviewer, para examinar los archivos del registro del sistema los cuales son conocidos como logs, ver figura 141.

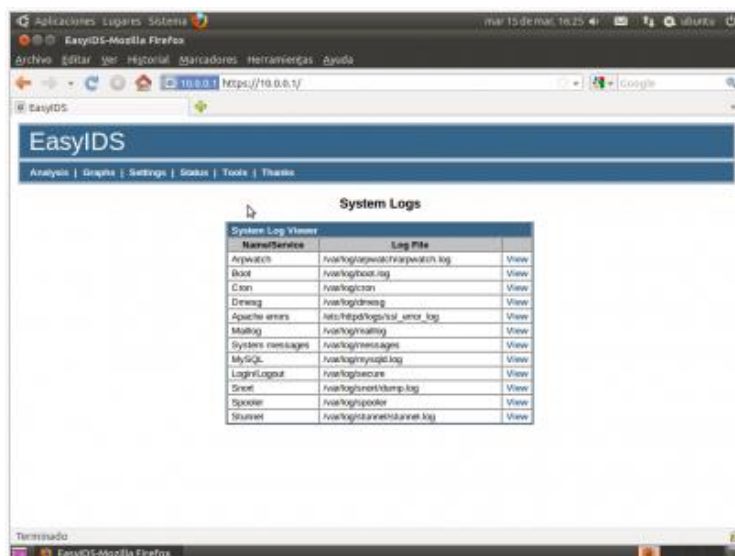


Figura 141 Menú de herramientas

4.5 Escaneo de vulnerabilidades utilizando Nessus

Una vez instalada y configurada la versión de Nessus 5.2.7 se procede al inicio de sesión del sistema con el nombre de usuario y contraseña creada durante la instalación como se muestra en la figura 142.

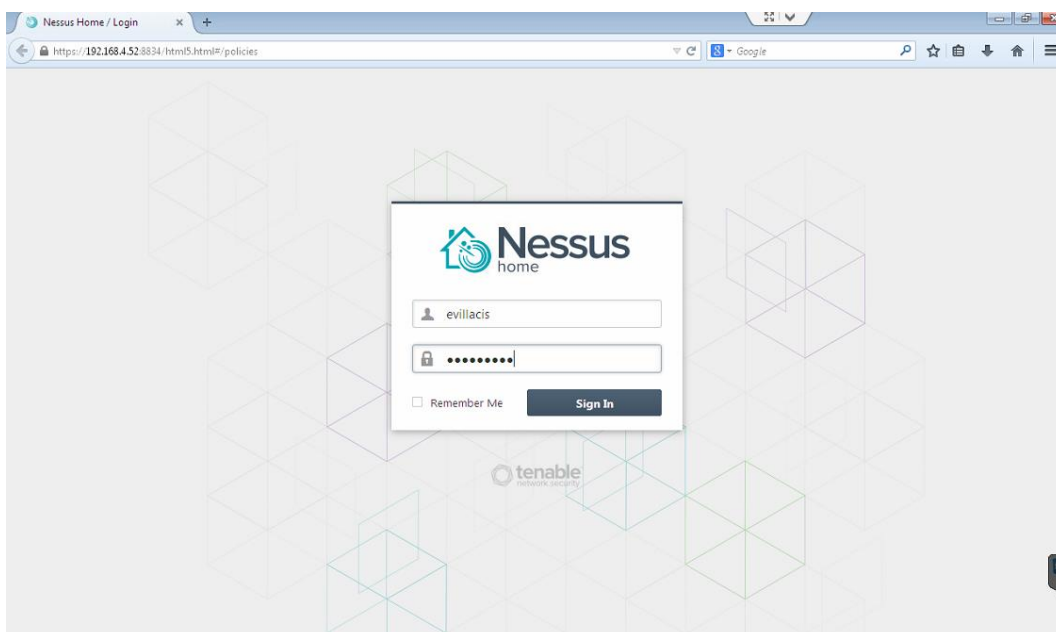


Figura 142 Interfaz de acceso

Cuando ya se haya autenticado correctamente el usuario, se abre la una interfaz con una serie de menús para consultar informes, realizar análisis y administrar directivas. El usuario administrador puede verificar la opción de administración de usuarios así como la configuración de Nessus.

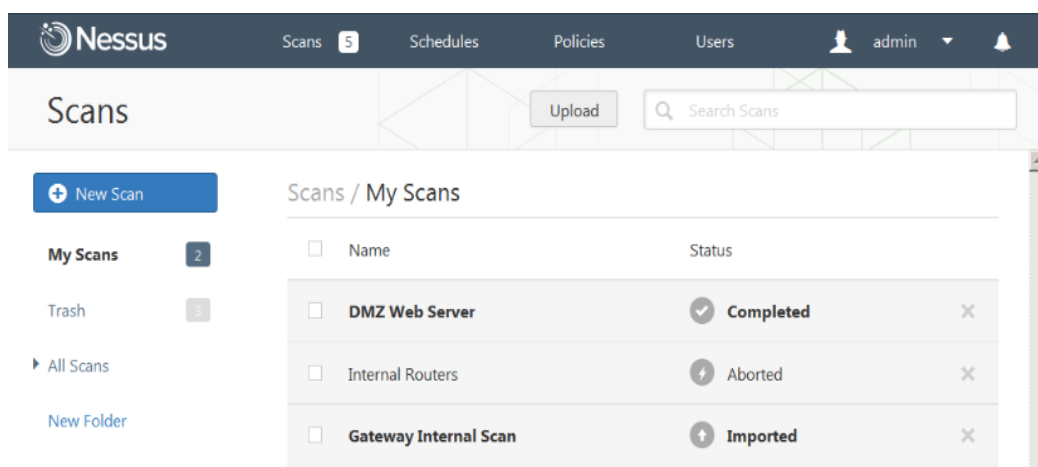


Figura 143 Menú inicio de nessus

En la zona superior izquierda se puede visualizar en todo momento las opciones del menú, el mensaje del usuario administrador como se muestra en la figura 143, el cual indica que actualmente se encuentra en sesión y al momento de abrir el menú mencionado se despliegan notificaciones relacionadas con la operación de Nessus, ver figura 144.

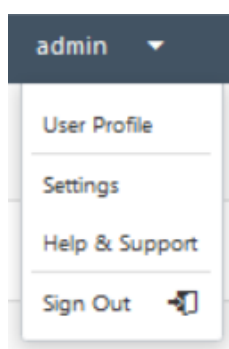


Figura 144 Opciones del menú

La opción “**User Profile**” muestra las opciones relacionadas con respecto a la cuenta del usuario, el cambio de contraseña, se puede administrar las carpetas y la página de las reglas de plugins.

La opción “**Settings**” muestra opciones de configuración, fuente de plugins y opciones avanzadas del analizador, ver figura 145.

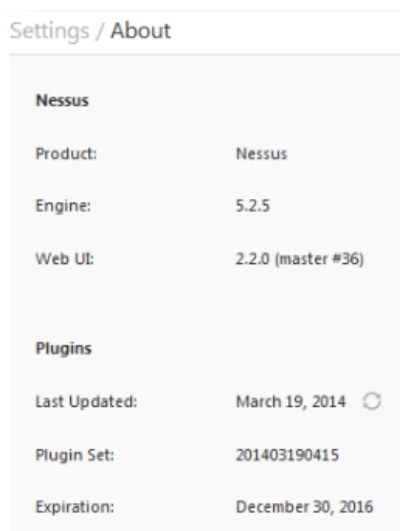


Figura 145 Opción de configuración

En la opción de “**Perfil de usuario**” concede modificar las opciones relacionadas con la cuenta, como se muestra en la figura 146.

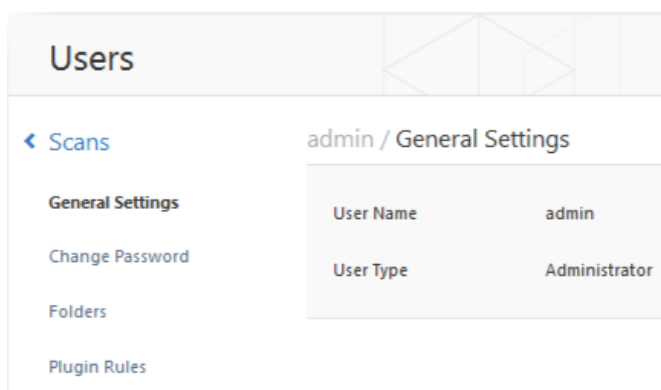


Figura 146 Perfil de usuario

Además se encuentra “**General Settings**”, mediante el cual se puede visualizar que usuario esta autenticado ya sea como administrador o como usuario. “**Change Password**” para cambiar nuestra contraseña, “**Folders**” mediante el cual se puede administrar las carpetas para salvar los resultados de los análisis a través de un método de organización para un mejor resultado de búsqueda, “**Plugin Rules**” brinda un método para crear reglas sobre los determinados plugins en relación con su respectivo análisis y se encuentra basado en el host; todas estas opciones arriba mencionadas.

4.5.1 Menú de configuración

En la opción “**About**” se muestra toda la información correspondiente sobre la instalación, versión de la UI Web, así como la fecha y versión del plugin.

La configuración “**Mail Server**” se refiere a la revisión de los parámetros relacionados con el servidor SMTP, la configuración “**Plugin Feed**” permite escoger un host de actualización de plugins personalizados así como un proxy para las actualizaciones de los plugins, ver figura 147.

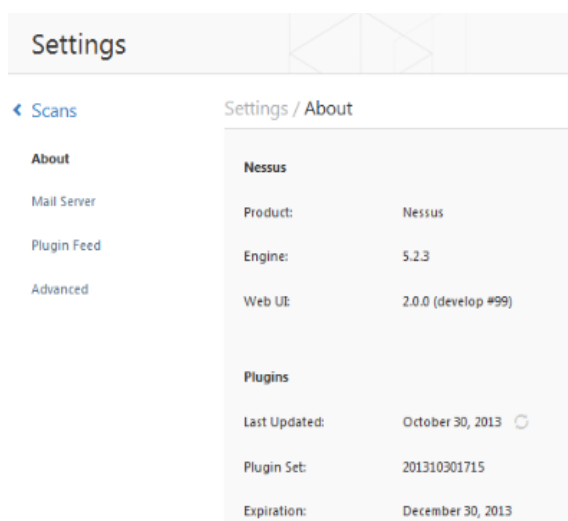


Figura 147 Menú de configuración

4.5.2 Teclas de acceso rápido de la interfaz

En la interfaz se puede encontrar una navegación de acceso rápido mediante el teclado, en las secciones más relevantes de la interfaz y la realización de las actividades comunes, las letras a utilizarse se muestran la tabla 11 y tabla 12.

Tabla 12

Teclas de acceso rápido al interfaz principal y listas

Interfaz principal	
R	Resultados
S	Análisis
T	Plantillas
P	Directivas
U	Usuarios
C	Configuración

(Security, Tenable Network, 2014)

Tabla 13**Teclas de acceso rápido de resultados y análisis**

Vista de resultados	
Shift + U	Cargar informe
Esc	Regresar a la lista de resultados
Flecha izquierda/derecha	Vulnerabilidad anterior/siguiente en modo Details (Detalles)
D	Eliminar resultado seleccionado
Vista de análisis	
N	Nuevo análisis
Vista de directivas	
Shift + U	Cargar nueva directiva
Vista de usuarios	
N	Nuevo usuario

(Security, 2014)

4.5.3 Políticas

Una política en Nessus se conforma por opciones de configuración que tienen relación con la creación de un análisis de vulnerabilidades, las cuales incluyen:

- Parámetros que supervisan los aspectos técnicos del análisis, como tiempo de espera, número de host y tipo de analizador de puertos.
- Credenciales para análisis locales, base de datos, certificación basada en HTTP, FTP, POP, IMAP o Kerberos.

- Definición de análisis en su totalidad con respecto a los plugins.
- Verificaciones de directivas de coincidencia de base de datos, nivel de ejecución de los informes, configuración de análisis para la localización de servicios.

4.5.3.1 Creación de una nueva política

Cuando exista conectividad en una UI del servidor Nessus, se puede realizar una nueva directiva personalizada haciendo click en “**Policies**” en la barra que se encuentra en la parte superior y se abre la interfaz del primer paso, el cual solicita que se defina el nombre de la directiva, la visibilidad, la cual puede ser privada o compartida y una descripción, ver figura 148.

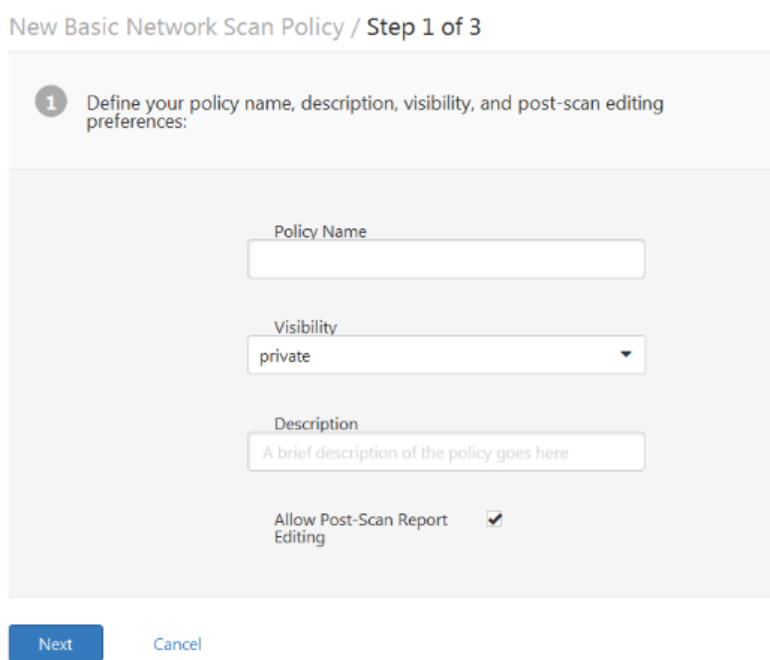
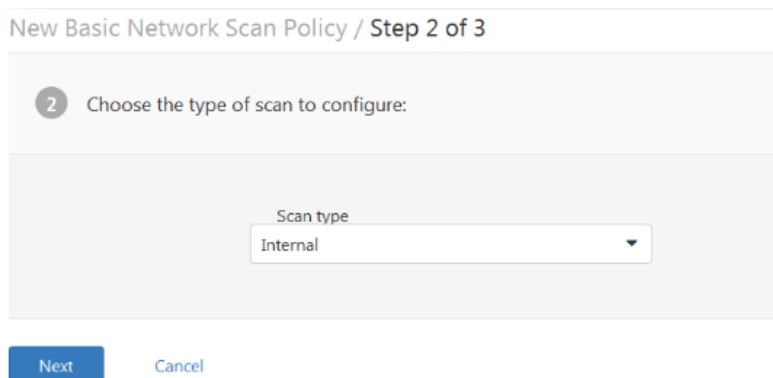


Figura 148 Paso para agregar una nueva política

En el siguiente paso se elige que host se empleará si interno o externo, las alternativas se transformarán de acuerdo a las respuestas, ver figura 149.



New Basic Network Scan Policy / Step 2 of 3

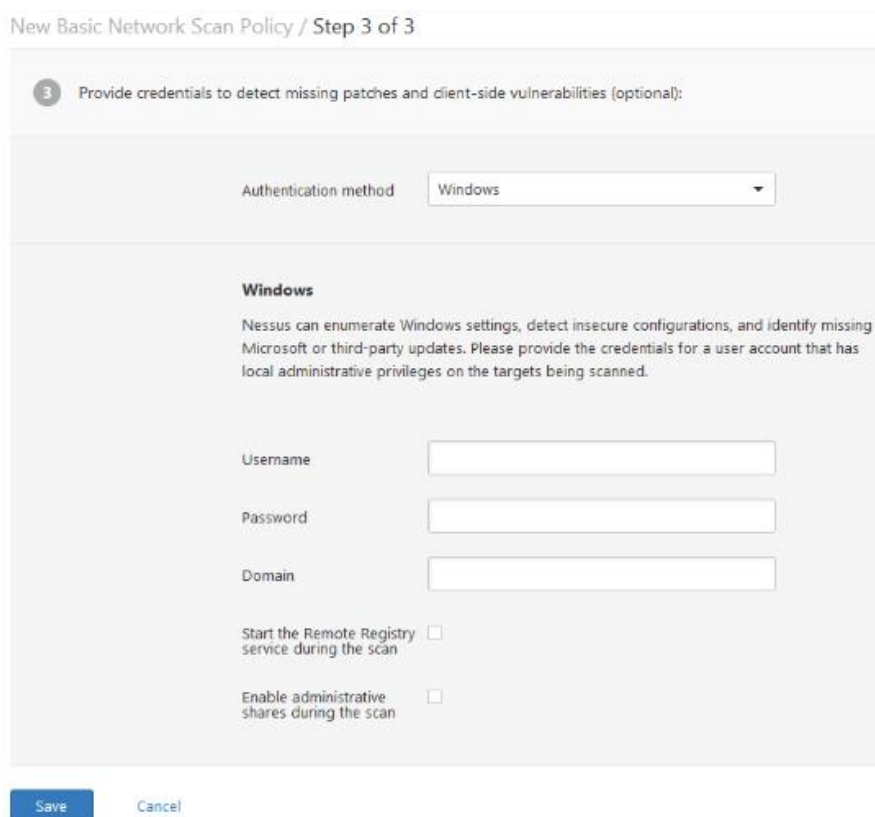
2 Choose the type of scan to configure:

Scan type
Internal

Next Cancel

Figura 149 Segundo paso para agregar una política

En el último paso se puede adicionar credenciales para realizar un mejor análisis, otros pasos del asistente de directivas pueden ser opcionales, cuando ya se crea la directiva se almacena con la configuración recomendada, ver figura 150.



New Basic Network Scan Policy / Step 3 of 3

3 Provide credentials to detect missing patches and client-side vulnerabilities (optional):

Authentication method Windows

Windows

Nessus can enumerate Windows settings, detect insecure configurations, and identify missing Microsoft or third-party updates. Please provide the credentials for a user account that has local administrative privileges on the targets being scanned.

Username

Password

Domain

Start the Remote Registry service during the scan

Enable administrative shares during the scan

Save Cancel

Figura 150 Tercer paso para agregar una nueva política

4.5.3.2 Creación de una política avanzada

Para no crear una política con el asistente se puede realizar de manera tradicional, configurando todas las opciones desde el inicio en la pestaña de “**Advanced**”, ver figura 151.

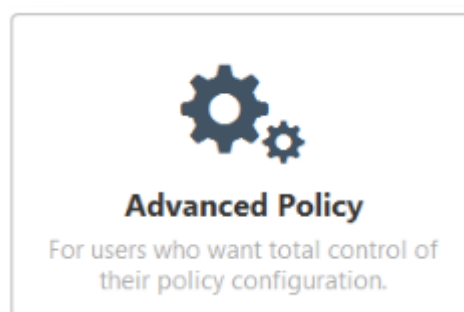


Figura 151 Política avanzada

4.5.4 Exportación, importación y copia de políticas

En el botón de “**Upload**”, en el menú de las políticas se pueden cargar políticas que ya hayan sido creadas anteriormente como se puede visualizar en la figura 152.

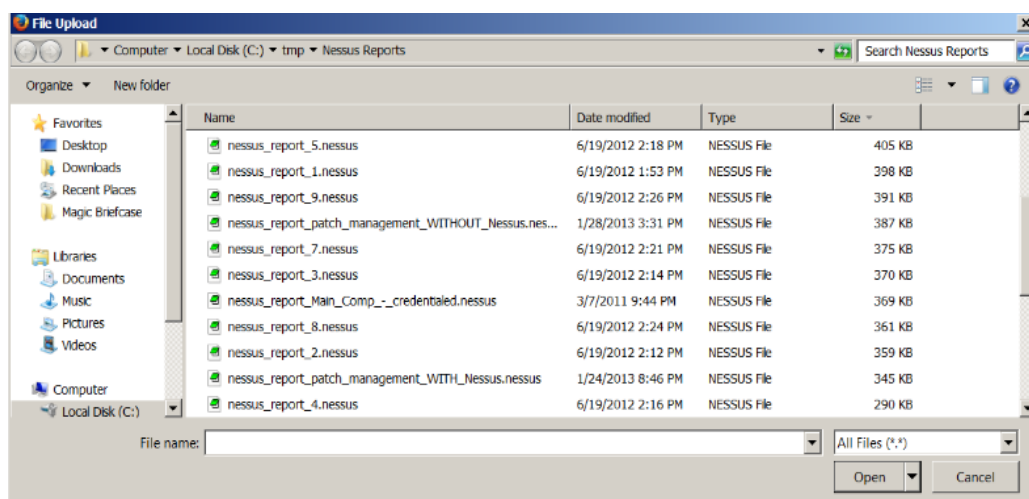


Figura 152 Exportación, importación y copia de políticas

4.5.5 Creación y programación de un análisis

El usuario puede realizar informes por capítulos: “**Vulnerability Centric**” (Enfocado en vulnerabilidades), “**Host Centric**” (Enfocado en hosts), “**Compliance**” (Compatibilidad) o “**Compliance Executive**” (Compatibilidad ejecutiva), además se puede exportar informes en pdf, cuando se utilizan los filtros de informes y las propiedades de exportación, ver figura 153.

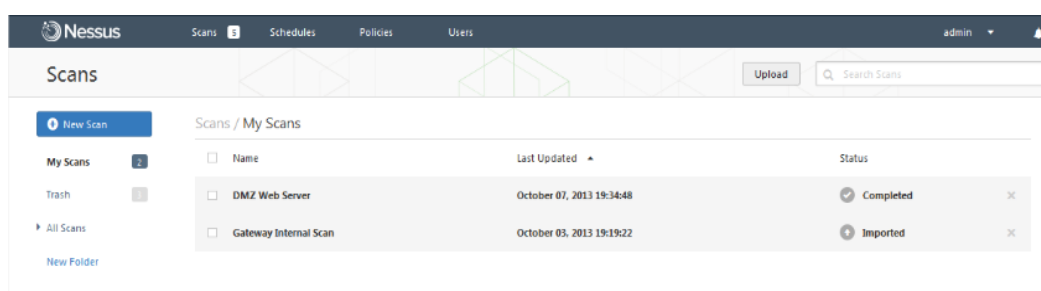


Figura 153 Programación de un análisis

También se puede encontrar los siguientes estados de análisis en la tabla 14.

Tabla 14

Estados de análisis

Estado de análisis	Descripción
Completed (Finalizado)	El análisis ha terminado.
Canceled (Cancelado)	El usuario detuvo el análisis antes de que haya finalizado.
Aborted (Interrumpido)	El análisis se ha interrumpido debido a una lista de objetivos inválida o a un error en el servidor (por ejemplo, reinicio o bloqueo).
Imported (Importado)	El análisis se ha importado mediante la función de cargar.

(Security, Tenable Network, 2014)

Una vez realizada la creación o selección de la política, se puede crear un nuevo análisis haciendo click en la opción “**Scans**” y luego aparecerá la opción de “**New Scan**” como se muestra a continuación en la figura 154.

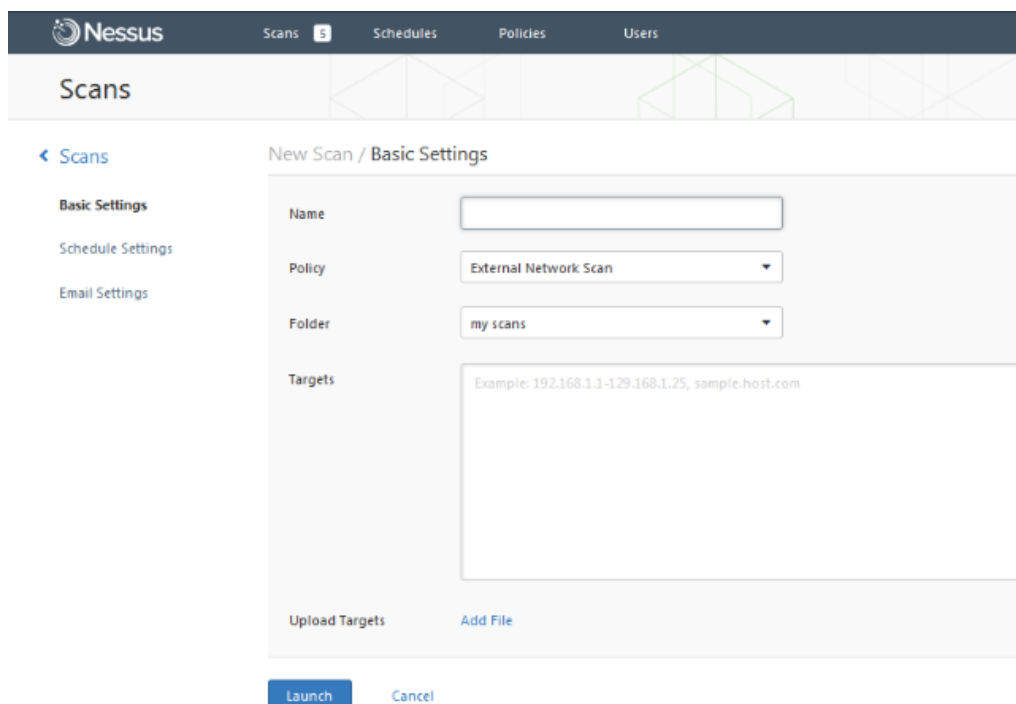


Figura 154 Creación de un nuevo scan

En la pestaña “**Basic Settings**” se puede ingresar cinco características para el destino del análisis:

- **Name:** nombre para reconocer el análisis.
- **Policy:** Selección de una nueva política ya creada, que utilizará el análisis para determinar las características en el comportamiento del servidor Nessus.
- **Folder:** Se almacena los resultados de los análisis.
- **Scan Targets:** Se introduce una dirección IP única, un intervalo de IP, una subred con notación CIDR o un host.
- **Upload Targets:** Se importa un texto con una lista de hosts ya almacenados.

En la pestaña de “**Schedule Settings**” se despliega un menú para controlar el inicio del análisis, ver figura 155.

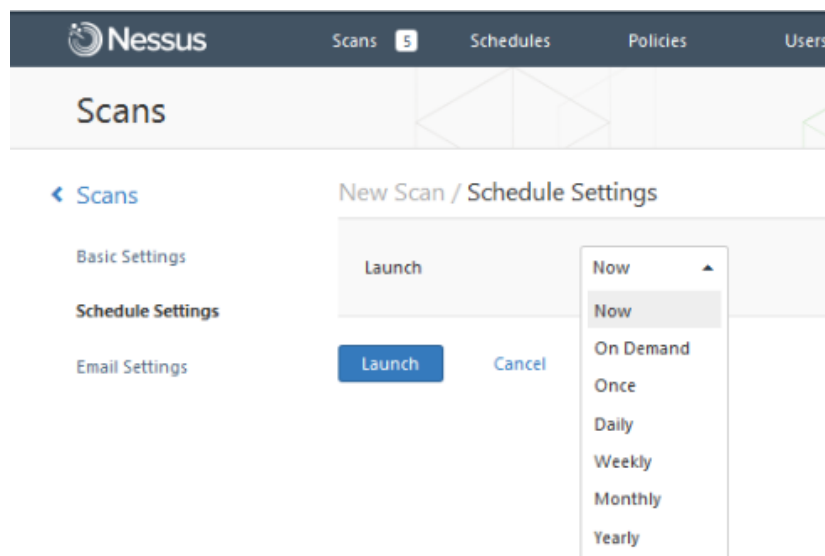


Figura 155 Pestaña de configuración del programa

Se ha realizado un análisis programado anteriormente y el mismo se lo puede exportar y modificarlo a la fecha que el usuario requiera, como se muestra en la figura 156.

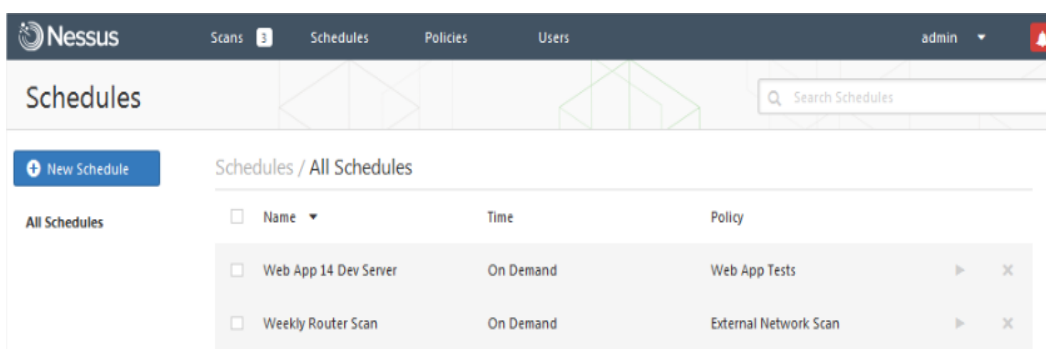


Figura 156 Análisis modificado

En la interfaz que aparecerá luego de programar la fecha, va a solicitar el sistema un mail para que pueda entregar el resultado de los análisis cuando este ya haya finalizado, ver en la figura 157.

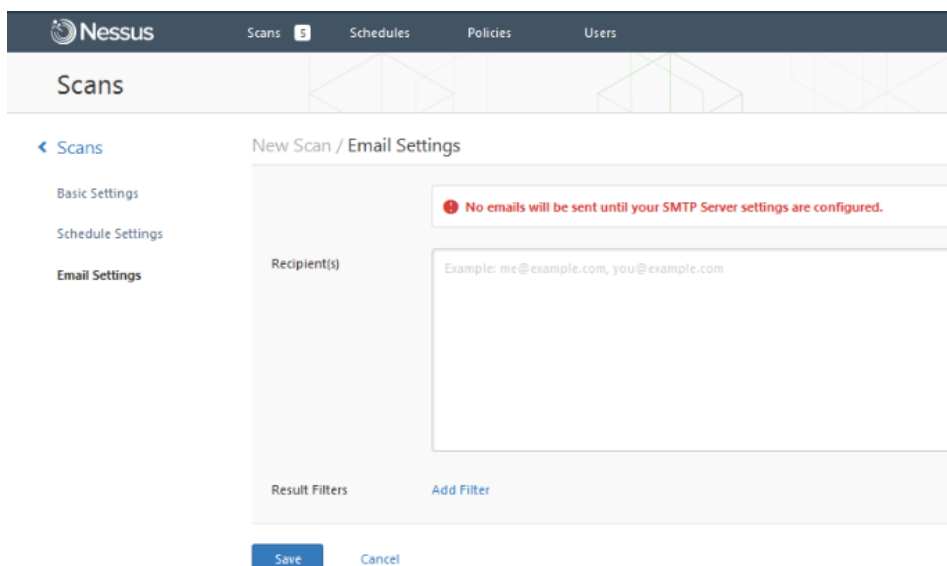


Figura 157 Petición de mail para entrega de resultados

Cuando ya se inicie el análisis, se despliega la lista de todos los análisis que se encuentren en pleno curso o su vez pausados, mostrando la información del análisis, a un lado de cada análisis existe la opción para pausar o interrumpir el análisis realizado en ese momento, ver figura 158.

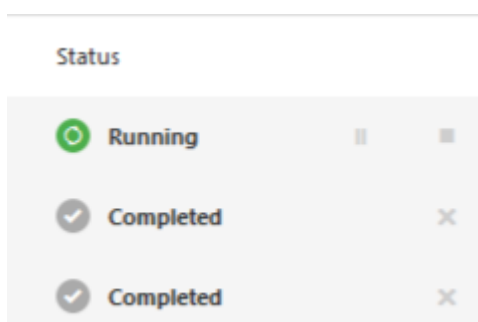


Figura 158 Estado del análisis

Para poder visualizar el resultado de los análisis, se debe escoger un informe de la lista, aquí se muestra todas las vulnerabilidades o hosts,

además se puede encontrar puertos o información de vulnerabilidades determinadas, ver figura 159.

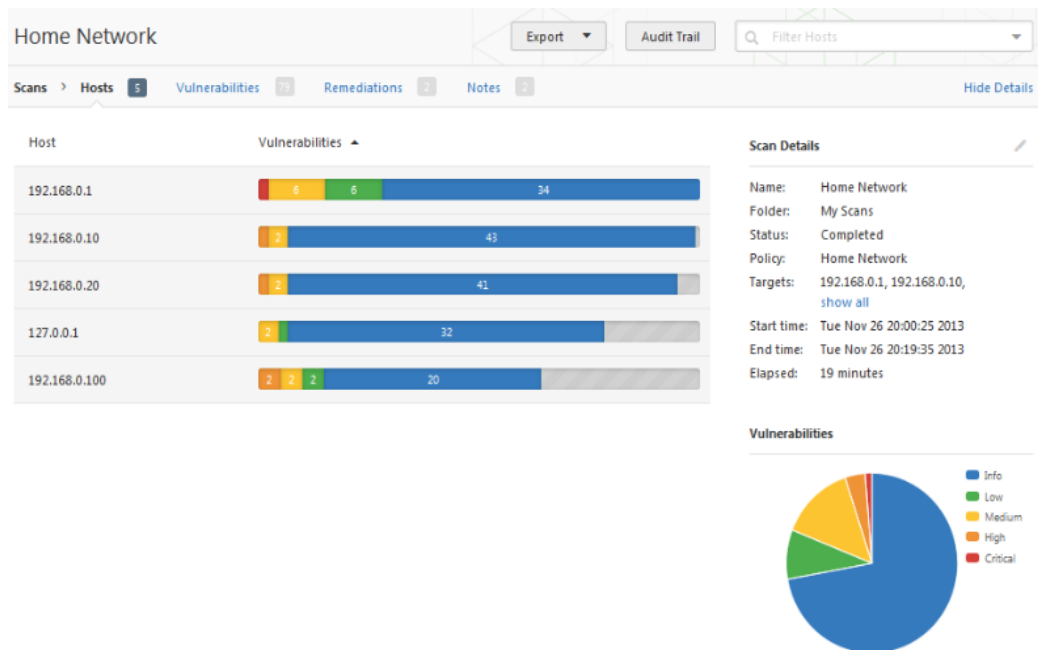


Figura 159 Informe de resultados de un análisis

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Se implementó los servicios de red utilizando herramientas de software libre para mantener la confidencialidad, integridad y disponibilidad de la información, en la empresa CEMYLUB.
- Se instaló un servicio de correo electrónico funcional y de alto rendimiento que permite ofrecer herramientas necesarias aprovechando los recursos en la red.
- Se definió las políticas de red mediante la implementación de un servidor firewall, brindado seguridad y control de la comunicación a la red local, impidiendo ataques malintencionados internos o externos.
- Como resultado del trabajo se ha logrado configurar un servidor proxy con autenticación de usuarios controlando el acceso a los recursos usando diferentes criterios de acceso, analizando el tráfico generador mediante la herramienta de Squid, identificando las vulnerabilidades a equipos de nuestra red, permitiendo que el sistema brinde seguridad y eficiencia para el servicio de CEMYLUB.
- Después de la instalación de un servidor Nessus se ha podido escanear e identificar vulnerabilidades a las estaciones y protocolos dentro de la red perimetral, disminuyendo los riesgos que afectan a las redes de datos.

- Mediante la creación e interpretación de reglas en el IDS Snort, se analizan los sistemas de información que circulan por la red de datos, protegiendo en tiempo real ante posibles intrusiones.
- Se garantizó el correcto acceso a los recursos de forma segura y eficiente, de manera que se cree un ambiente de confianza con el servicio tecnológico.

5.2 Recomendaciones

- Las medidas de seguridad tanto como las intrusiones y ataques a la información van creciendo paralelamente al avance tecnológico de las comunicaciones, por lo cual se recomienda un constante monitoreo y actualización de los sistemas actualmente implementados.
- Cada vez existe más personal dentro de la empresa, por lo que a un futuro se recomienda un rediseño de la red, para aumentar el número de equipos que cubran una mayor afluencia tanto de usuarios como de información.
- Cuando se vayan a modificar las políticas de seguridad creadas, se debe tomar en cuenta la responsabilidad y el poder que se le va a entregar a cada usuario, ya que a pesar de que se le ha brindado un conocimiento de las nuevas reglas de la empresa no queda exento de nuevos ataques, por lo que esto causaría un gran problema para todo el trabajo que se ha realizado.

5.3 Bibliografía

- Bogotá, A. M. (n.d.). *Montaje de la solución a Nivel Distrital Zimbra*.
- Dueñas, J. B. (2013, Diciembre). *Alcance Libre*.
- Erick Cruz, D. R. (2010). *Modelo de seguridad para la medición de vulnerabilidades y reducción de riesgos en redes de datos*.
- Gladys Bravo, N. G. (2010). *Arquitectura de monitoreo en tiempo real de una red*.
- Kleinerman, J. E. (2011). *Manual de Uso de IPTables*.
- León, L. (2012). *Diseño e implementación de una infraestructura de servicios de red y resguardo de servidores linux a través de open source en la empresa proteco coasin s.a*.
- López, E. (2006, Noviembre 13). *Servidor Proxy Squid*.
- López, J. G. (2009). *Optimización de sistemas de detección de intrusos de red utilizando técnicas computaciones avanzadas*.
- Medina, J. A. (2012, Junio). *Tuxjm*. Retrieved from http://tuxjm.net/docs/Manual_de_Instalacion_de_Servidor_Proxy_Web_con_Ubuntu_Server_y_Squid/html-multiples/ch01s02.html
- Mireya, S. (2008). *Estudio e implementacion de qos mediante las herramientas iproute2 y netfilter de linux*.
- Parkway, O. (2010, Junio). *Instalación de Windows server 2008*.
- *Quer System Informática*. (2010).
- Rice, C. (2010, Mayo 11). *Anandtech*. Retrieved from <http://www.anandtech.com/show/3715/family-proxy>
- S.L., Z. (2014, Julio 23). *Zentyal Wiki*.
- Sabater, J. (2008, Octubre 10). *Zimbra 5, suite de mensajería y colaboración*.
- Securit, T. N. (2011, Junio 14). Retrieved from Nessus 4.4 Guía de instalación.
- Security, T. N. (2014). *Guía del usuario de Nessus 5.2 HT*.

- *Security, Tenable Network.* (2014, Enero 16). Retrieved from Guía del usuario de Nessus 5.2 HTML5.
- *Tesis GNU/Linux.* (2010, Octubre 2010).
- Zwicky Elizabeth, D. C. (2000). *Building Internet FIREWALS.*