ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE DMZ Y LA INTERCONEXIÓN SEGURA MEDIANTE VPN UTILIZANDO EL FIREWALL FORTIGATE 60

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ANÁLISIS DE SISTEMAS INFORMÁTICOS

ANDREA ELIZABETH CONZA GONSÁLEZ
liz_cg2712@hotmail.com

DIRECTOR: ING. CÉSAR GALLARDO
cesar.gallardo@epn.edu.ec

Quito, Septiembre de 2009

DECLARACIÓN

Yo Andrea Elizabeth Conza Gonsález, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Andrea Elizabeth Conza Gonsález

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Andrea Elizabeth Conza Gonsález, bajo mi supervisión.

Ing. Cesar Gallardo
DIRECTOR DE PROYECTO

AGRADECIMIENTO

Agradezco a Dios por su gran amor y ser el motor que mueve mi vida, por enseñarme a descubrir su infinita grandeza. Además por permitirme culminar una etapa de mi vida y por el comienzo de otra que apenas comienza.

A mis padres que han sabido guiarme de la mejor manera, con su amor y paciencia me han ofrecido sus valiosos consejos; siendo el soporte para mí en todo momento. A mis hermanos que me apoyaron, y creyeron en mí.

De manera especial a la personita que forma parte de mi vida; siendo el apoyo en la finalización de este proyecto.

A los amigos que están y a los que se fueron gracias por formar parte de mi vida, siempre los llevare en mi corazón

A todas las personas que me ayudaron de una u otra forma a convertir en realidad este hermoso sueño.

DEDICATORIA

Este proyecto esta dedicado a Dios, por brindarme la oportunidad de estudiar y saber que aun cuando las cosas no salen como uno las desea, es porque él siempre nos tiene reservado algo mucho mejor.

A mis padres que con cariño han sabido brindarme lo mejor de sí y ser el mejor regalo de Dios. Mi madre, amiga y confidente, lista para escucharme en cualquier momento, con su gran ternura. Mi padre, el soporte que me motiva a seguir luchando incansablemente por lograr mis metas.

A mis queridos hermanos que siempre creyeron en mí, y por aprender de ellos lo mejor de sí; su fuerza y persistencia en la vida.

A Leito por forma parte de mi vida, que llegó en el mejor momento con su ternura, amor, y cariño me impulsó alcanzar este sueño.

A mis amigos con los que iniciamos un sueño, y en el camino fuimos aprendiendo juntos; fortaleciendo nuestra amistad

ÍNDICE DE CONTENIDO

CAPÍTULO 1: INTRODUCCIÓN 1

1.1 ASPECTOS GENERALES 1

1.1.1 ÁMBITO 1

1.1.2 PROBLEMA 1

1.2 ALCANCE 1

1.3 OBJETIVOS 2

1.3.1 GENERAL 2

1.3.2 ESPECÍFICOS 2

1.4 JUSTIFICACIÓN 2

CAPÍTULO 2: MARCO TEÓRICO 3

2.1 REDES DE COMPUTADORAS 3

2.1.1 RED DE COMPUTADORAS 3

2.1.2 CLASIFICACIÓN DE LAS REDES 3

2.1.2.1 Por su tecnología de transmisión (difusión) 3

2.1.2.2 Por su tamaño 3

2.1.2.3 Por método de conexión 5

2.1.2.4 Por relación funcional 6

2.1.2.5 Por topología de red 7

2.1.2.6 Por el tipo de transmisión 11

2.2 MODELO OSI 12

2.2.1 INTRODUCCIÓN 12

2.2.2 CONCEPTO DE MODELO OSI 13

2.2.3 CAPAS DEL MODELO OSI 13

2.2.3.1 Capa de Aplicación 13

2.2.3.2 Capa de Presentación 14

2.2.3.3 Capa de Sesión 14

2.2.3.4 Capa de Transporte 14

2.2.3.5 Capa de Red 15

2.2.3.6 Capa de Enlace de datos 16

2.2.3.7 Capa Física 16

2.3 MODELO TCP/IP 17

2.3.1 INTRODUCCIÓN 17

2.3.2 CONCEPTO MODELO TCP /IP 18

2.3.2.1 Capa de Aplicación 18

2.3.2.2 Capa de Transporte 19

2.3.2.3 Capa de Internet 19

2.3.2.4 Capa de Acceso de Red 19

2.4 DIRECCIONAMIENTO IP 20

2.4.1 DIRECCIONAMIENTO IPV4 20

2.4.1.1 Componentes de una dirección IP 21
2.4.1.2 Clases de direcciones de Internet IPV4 21
2.4.1.3 Cabecera IPV4 22
2.4.2 DIRECCIONAMIENTO IPV6 24
2.4.2.1 Tipos de direcciones en IPV6 25
2.4.2.2 Representación de las direcciones 25
2.4.2.3 Cabecera IPv6 26
2.5 COMPARACIÓN ENTRE MODELOS OSI Y TCP/IP 27
2.5.1 SIMILITUD ENTRE EL MODELO OSI Y EL MODELO TCPIP 27
2.5.2 DIFERENCIA ENTRE EL MODELO OSI Y EL MODELO TCPI 28
2.6 PROTOCOLOS DE TCP /IP 28
2.7 SEGURIDAD INFORMÁTICA 29
2.7.1 INTRODUCCIÓN 29
2.7.2 CONCEPTO DE SEGURIDAD INFORMÁTICA 30
2.7.3 GENERALIDADES 30
2.7.3.1 Alias 30
2.7.3.2 Cracker 30
2.7.3.3 Hacker 30
2.7.3.4 Pirata Informático 31
2.7.4 VIRUS INFORMÁTICOS 31
2.7.4.1 Tipos de Virus de Informáticos 31
2.7.5 TIPOS DE ATAQUES 32
2.7.5.1 Shoulder Surfing 32
2.7.5.2 Eavesdropping–Packet Sniffing 32
2.7.5.3 Snooping–Downloading 33
2.7.5.4 Spoofing 33
2.7.5.5 Barrido de puertos 33
2.7.5.6 Detección de Proxies 33
2.7.5.7 Ataques Smurf/Fraggle 34
2.7.6 MÉTODOS DE HACKING 34
2.7.6.1 Caballo de Troya 34
2.7.6.2 Superzapping 34
2.7.6.3 Puertas Falsas 35
2.7.6.4 Bombas lógicas 35
2.7.7 VULNERABILIDADES 35
2.7.7.1 Negación de servicio (denial of service) 35
2.7.7.2 Cracking de password 35
2.7.7.3 E-mail bombing y spamming 35
2.7.7.4 Consideraciones de software 36
2.7.7.5 Consideraciones de una red 36
2.7.8 SISTEMAS OPERATIVOS 36
2.7.8.1 Software Libre (Open Source) 36

2.7.8.2 Software bajo licenciamiento ... 37
2.8 SERVIDORES ... 39
2.8.1 SERVIDOR DE CORREO ... 39
2.8.1.1 Protocolo de transporte de correo ... 39
2.8.1.2 Protocolos de acceso a correo ... 39
2.8.1.3 Clasificación de los programas de correo ... 40
2.8.2 SERVIDOR WEB ... 42
2.8.2.1 Apache ... 43
2.8.2.2 Internet Information Servers (IIS) ... 43
2.8.3 SERVIDOR BASE DE DATOS ... 44
2.8.3.1 MySQL ... 44
2.9 MECANISMOS DE SEGURIDAD EN REDES ... 45
2.9.1 RED PRIVADA VIRTUAL (VPN) ... 45
2.9.1.1 Características ... 46
2.9.1.2 Elementos de una VPN ... 46
2.9.1.3 Requerimientos Básicos ... 47
2.9.1.4 Funcionamiento de una VPN ... 47
2.9.1.5 Tipos de VPN ... 48
2.9.1.6 Protocolos de túnel ... 49
2.9.2 ZONA DESMILITARIZADA (DMZ) ... 51
2.9.2.1 Arquitectura para una DMZ ... 52
2.9.3 FIREWALL ... 54
2.9.3.1 Tipos de cortafuegos ... 55
2.9.3.2 Tipos de Cortafuegos según su implementación ... 58
2.9.4 ANÁLISIS COMPARATIVO ... 81
2.9.4.1 Costos de Software ... 81
2.9.4.2 Comparativa con Servidores ... 82
2.9.4.3 Costos de los Dispositivos (Firewall) ... 82
2.9.5 SELECCIÓN Y DETERMINACIÓN DE LA ALTERNATIVA DE SOLUCIÓN ... 83
2.9.6 PRESUPUESTO ... 83

CAPÍTULO 3: DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PARA EL LTI ... 85

3.1 ANÁLISIS DE LA SITUACIÓN ACTUAL ... 85
3.2 ESTRUCTURA FÍSICA DE RED DEL LABORATORIO LTI ANTES DE LA IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD ... 86
3.3 ESTRUCTURA FÍSICA DE LOS SERVIDORES DEL LABORATORIO LTI ANTES DE LA IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD ... 87
3.4 DISEÑO DE SOLUCIÓN DEL SISTEMA DE SEGURIDAD CON EL FIREWALL FORTIGATE 60 ... 88
3.5 CONFIGURACIÓN DE LOS SERVICIOS ... 88
3.5.1 SERVIDOR CORREO ... 88

3.5.2 SERVIDOR WEB ... *91*
3.5.3 SERVIDOR BASE DE DATOS ... *93*
3.6 CONFIGURACIÓN DEL FIREWALL FORTIGATE 60 ... 97
3.6.1 CONFIGURACIÓN INICIAL ... *97*
3.6.1.1 Configuración mediante CLI (interfaz de Línea de Comandos) ... 98
3.6.1.2 Configuración mediante la Interfaz de Administración basada en Web ... 98
3.6.2 CONFIGURACIÓN DE INTERFACES ... *100*
3.6.2.1 Configuración de DHCP ... 100
3.6.2.2 Configuración de interfaz Internal ... 101
3.6.2.3 Configuración de interfaz WAN1 ... 102
3.6.2.4 Configuración de interfaz DMZ ... 103
3.6.2.5 Configuración Static Route ... 103
3.6.2.6 Configuración de DNS ... 104
3.6.3 MODO DE OPERACIÓN ... *105*
3.6.4 FIREWALL ... *106*
3.6.4.1 Políticas de firewall ... 106
3.6.4.2 Registro de Direcciones ... 106
3.6.4.3 Grupo de Direcciones ... 107
3.6.5 SCHEDULES (INTERVALOS DE TIEMPO) ... *108*
3.6.5.1 Recurring Schedules ... 108
3.6.6 SERVICIOS ... *109*
3.6.6.1 Grupos de Servicios ... 109
3.6.7 WEB URL FILTERING Y CATEGORY BLOCK ... *109*
3.6.7.1 Content Blocking ... 109
3.6.7.2 URL Blocking ... 110
3.6.8 PROTECTION PROFILES (PERFILES DE PROTECCIÓN) ... *111*
3.6.9 POLÍTICAS DE FIREWALL ... *112*
3.6.9.1 Configuración de Políticas usuarios ... 112
3.6.10 SERVICIOS PROTEGIDOS DMZ ... *113*
3.6.10.1 Servidor Web ... 113
3.6.10.2 Servidor Correo ... 116
3.6.11 VPN (VIRTUAL PRIVATE NETWORK) ... *120*
3.6.11.1 Configuración Dial-up VPN en Firewall FortiGate ... 121
3.6.11.2 Instalación de FortiClient en el cliente VPN ... 125
3.6.11.3 Configuración de FortiClient ... 127
3.6.11.4 Instalación de MySQL Tools en el cliente VPN ... 131
3.6.11.5 Configuración del cliente SSH MySQL ... 134
3.7 PRUEBA DE ACTIVIDAD DE LA DMZ ... 135
3.7.1 SERVICIO WEB ... *135*
3.7.2 SERVICIO DE CORREO ... *136*
3.8 PRUEBA DE SEGURIDAD DMZ ... 137
3.9 PRUEBA DE ACTIVIDAD DE VPN ... 140

3.9.1 CONEXIÓN DEL HOST 140

CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES 144

4.1 CONCLUSIONES 144

4.2 RECOMENDACIONES 145

GLOSARIO ……. 146

BIBLIOGRAFÍA … 157

ÍNDICE DE FIGURAS

FIGURA 2.1.- TOPOLOGÍA DE BUS 8
FIGURA 2.2.- TOPOLOGÍA EN ESTRELLA 9
FIGURA 2.3.- TOPOLOGÍA EN ANILLO 10
FIGURA 2.4.- TOPOLOGÍA EN MALLA 10
FIGURA 2.5.- TOPOLOGÍA EN ÁRBOL 11
FIGURA 2.6.- MODELO OSI 13
FIGURA 2.7.- CAPA DE ENLACE DE DATOS 16
FIGURA 2.8.- MODELO TCP/IP 18
FIGURA 2.9.- CLASES ASIGNADAS DE DIRECCIONES DE INTERNET 22
FIGURA 2.10.- CABECERA IPV4 23
FIGURA 2.11.- CABECERA FIJA IPV6 26
FIGURA 2.12.- COMPARACIÓN MODELOS TCP/IP OSI 27
FIGURA 2.13.- REPRESENTACIÓN ESQUEMÁTICA DEL SERVICIO DE CORREO ELECTRÓNICO 41
FIGURA 2.14.- ELEMENTOS DE UNA VPN 47
FIGURA 2.15.- FUNCIONAMIENTO DE UNA VPN 47
FIGURA 2.16.- DATAGRAMA IP 49
FIGURA 2.17.- ZONA DESMILITARIZADA 52
FIGURA 2.18.- ARQUITECTURA SCREENED SUBSET 53
FIGURA 2.19.- PROXY DE APLICACIONES 56
FIGURA 2.20.- DUAL COMED HOST 57
FIGURA 2.21.- FORTIGATE 60 63
FIGURA 3.1.- ESTRUCTURA DE RED DEL LTI ANTES DE LA IMPLEMENTACIÓN DE DMZ Y VPN 86
FIGURA 3.2.- ESTRUCTURA DE SERVIDORES DEL LABORATORIO LTI EN LA POLIRED ANTES DE LA IMPLEMENTACIÓN DE DMZ Y VPN 87
FIGURA 3.3.- TOPOLOGÍA DE RED DEL LTI CON LA IMPLEMENTACIÓN DE FIREWALL 88
FIGURA 3.4.- CONFIGURACIÓN DE LA TARJETA DE RED SERVIDOR DE CORREO 89
FIGURA 3.5.- ARCHIVO DE CONFIGURACIÓN DE DOVECOT 90
FIGURA 3.6.- INGRESO AL NAVEGADOR DE CORREO 90
FIGURA 3.7.- CREACIÓN DE CUENTA DE USUARIO 91
FIGURA 3.8.- CONFIGURACIÓN DE LA TARJETA DE RED SERVIDOR WEB. 91
FIGURA 3.9.- UBICACIÓN DEL DIRECTORIO INDEX.HTML 92
FIGURA 3.10.- PÁGINA DE INICIO SITIO WEB 92
FIGURA 3.11.- CONFIGURACIÓN DE LA TARJETA DE RED SERVIDOR DE BASE DE DATOS 93
FIGURA 3.12.- INGRESAR LA CLAVE DE MYSQL 94
FIGURA 3.13.- VERIFICAR LA EXISTENCIA DE LOS ARCHIVOS 95
FIGURA 3.14.- EDICIÓN DE LA PALABRA SECRETA 95
FIGURA 3.15.- INGRESAR A LA PÁGINA DE INICIO DE PHPMYADMIN 95
FIGURA 3.16.- SELECCIONAR PRIVILEGIOS EN LA PÁGINA PRINCIPAL DE PHPMYADMIN 96

FIGURA 3.17.- AGREGAR UN USUARIO NUEVO 96
FIGURA 3.18.- CONFIGURACIÓN DE PRIVILEGIOS PARA EL NUEVO USUARIO 97
FIGURA 3.19.- INTERFAZ INICIAL DE ADMINISTRADOR BASADA EN WEB 99
FIGURA 3.20.- MENÚ PRINCIPAL 99
FIGURA 3.21.- CONFIGURACIÓN DHCP 101
FIGURA 3.22.- CONFIGURACIÓN INTERFAZ INTERNAL 102
FIGURA 3.23.- CONFIGURACIÓN INTERFAZ WAN1 102
FIGURA 3.24.- CONFIGURACIÓN INTERFAZ DMZ 103
FIGURA 3.25.- CONFIGURACIÓN STATIC ROUTE 104
FIGURA 3.26.- CONFIGURACIÓN DNS 105
FIGURA 3.27.- EJEMPLO DE CONFIGURACIÓN DE RED CON MODO NAT/ROUTE 106
FIGURA 3.28.- REGISTRO DE DIRECCIONES USUARIOS 107
FIGURA 3.29.- REGISTRO GRUPO DE USUARIOS 108
FIGURA 3.30.- CREACIÓN RECURRING SCHEDULES 108
FIGURA 3.31.- CREACIÓN DE UN SERVICIO 109
FIGURA 3.32.- CONTENIDO BLOQUEADO 110
FIGURA 3.33.- LISTA DE URL'S BLOQUEADAS 111
FIGURA 3.34.- CREACIÓN DE UN PERFIL NUEVO 111
FIGURA 3.35.- CONFIGURACIÓN VIP SERVIDOR WEB 113
FIGURA 3.36.- REGISTRO DE DIRECCIÓN DEL SERVIDOR CORREO 114
FIGURA 3.37.- REGISTRO DE DIRECCIÓN DEL WEB MASTER 114
FIGURA 3.38.- REGISTRO DE DIRECCIÓN DEL WEB MASTER 115
FIGURA 3.39.- POLÍTICAS DE ACCESO DEL WEB MASTER 116
FIGURA 3.40.- CONFIGURACIÓN VIP DEL SERVIDOR CORREO 117
FIGURA 3.41.- REGISTRO DE DIRECCIÓN DEL SERVIDOR DE CORREO 117
FIGURA 3.42.- POLÍTICA PARA ENVIÓ DE MENSAJES 118
FIGURA 3.43.- POLÍTICA PARA PERMITIR CORREOS DESDE SERVIDORES EXTERNOS 119
FIGURA 3.44.- POLÍTICAS PARA PERMITIR CORREOS INTERNOS 120
FIGURA 3.45.- REGISTRO DE UN RANGO DE DIRECCIONES 121
FIGURA 3.46.- REGISTRO DE NUEVO USUARIO LOCAL DE FORIGATE 122
FIGURA 3.47.- REGISTRO DEL USUARIO EN UN GRUPO 122
FIGURA 3.48.- CONFIGURACIÓN PHASE1 123
FIGURA 3.49.- CONFIGURACIÓN PHASE2 123
FIGURA 3.50.- CONFIGURACIÓN DE RANGO DE DIRECCIONES PARA USUARIOS DIAL UP 124
FIGURA 3.51.- POLÍTICA PARA VPN 125
FIGURA 3.52.- EJECUCIÓN DEL PROGRAMA FORTICLIENT 125
FIGURA 3.53.- LICENCIA Y TÉRMINOS DE USO PARA EL USUARIO FORTICLIENT 126
FIGURA 3.54.- TIPO DE INSTALACIÓN DE IPSEC VPN Y FIREWALL 126
FIGURA 3.55.- INICIO DE LA INSTALACIÓN 127
FIGURA 3.56.- FINALIZACIÓN DEL PROGRAMA 127

FIGURA 3.57.- PÁGINA PRINCIPAL DE FORTICLIENT 128
FIGURA 3.58.- CONFIGURACIÓN USUARIO EN FORTICLIENT 129
FIGURA 3.59.- MENÚ DE CONFIGURACIÓN AVANZADAS FORTICLIENT 129
FIGURA 3.60.- CONFIGURACIÓN AVANZADA DE FORTICLIENT 130
FIGURA 3.61.- CONFIGURACIÓN MANUAL DE VIRTUAL IP 130
FIGURA 3.62.- CONFIGURACIÓN DE INICIO DE SESIÓN DEL CLIENTE VPN 131
FIGURA 3.63.- COMPROBACIÓN DE CONECTIVIDAD CON LA INTERFAZ INTERNAL 131
FIGURA 3.64.- SETUP DE MYSQL TOOLS 132
FIGURA 3.65.- LICENCIA Y TÉRMINOS DE USO DE MYSQL TOOLS 132
FIGURA 3.66.- DESTINO DE LA CARPETA DE INSTALACIÓN DE MYSQL TOOLS 133
FIGURA 3.67.- TIPO DE INSTALACIÓN SEGÚN LAS NECESIDADES 133
FIGURA 3.68.- INICIO DE LA INSTALACIÓN MYSQL TOOLS 134
FIGURA 3.69.- CONEXIÓN DESDE EL CLIENTE VPN HACIA EL SERVIDOR BASE DE DATOS 135
FIGURA 3.70.- INGRESO A LA PÁGINA DE INICIO 136
FIGURA 3.71.- INGRESO A CUENTA DE CORREO 136
FIGURA 3.72.- ENVÍO DE MENSAJE DE CORREO 137
FIGURA 3.73.- RECEPCIÓN DE MENSAJES 137
FIGURA 3.74.- TELNET AL FIREWALL POR EL PUERTO 80 138
FIGURA 3.75.- DIRECCIÓN IP DEL USUARIO1 DE LA RED INTERNAL 138
FIGURA 3.76.- TELNET DESDE UN USUARIO AL PUERTO 21 AL SERVIDOR DE CORREO 138
FIGURA 3.77.- TELNET DESDE UN USUARIO AL PUERTO 21 AL SERVIDOR WEB 138
FIGURA 3.78.- TELNET DESDE UN USUARIO AL PUERTO 3306 AL SERVIDOR BASE DE DATOS 139
FIGURA 3.79.- DIRECCIÓN IP DEL USUARIO1 DE LA RED INTERNAL 139
FIGURA 3.80.- TELNET AL SERVIDOR DE CORREO Y AL SERVIDOR WEB POR EL PUERTO 21 139
FIGURA 3.81.- TELNET AL SERVIDOR DE BASE DE DATOS AL PUERTO 21 140
FIGURA 3.82.- TELNET AL SERVIDOR DE CORREO Y WEB AL PUERTO 80 140
FIGURA 3.83.- MONITOREO DE LA CONEXIÓN DESDE PC FORTICLIENT 141
FIGURA 3.84.- PING HACIA LA INTERFAZ INTERNAL 141
FIGURA 3.85.- MONITOREO DE LA CONEXIÓN DESDE EL FIREWALL FORTIGATE 141
FIGURA 3.86.- SELECCIÓN DE BASE DE DATOS A MODIFICAR EN EL CLIENTE 142
FIGURA 3.87.- INSERCIÓN DE NUEVO CAMPO EN LA BASE DE DATOS PRUEBA 142
FIGURA 3.88.- REVISIÓN DE LOS CAMBIOS EN EL SERVIDOR 143

ÍNDICE DE TABLAS

TABLA 2.1.- CARACTERÍSTICAS TÉCNICAS D-LINK DFL-800 60
TABLA 2.2.- CARACTERÍSTICAS TÉCNICAS D-LINK DFL-860 62
TABLA 2.3.- CARACTERÍSTICAS TÉCNICAS FORTIGATE 60 64
TABLA 2.4.- CARACTERÍSTICAS TÉCNICAS FORTIGATE 60B 66
TABLA 2.5.- CARACTERÍSTICAS TÉCNICAS SONIC WALL TZ 180 68
TABLA 2.6.- CARACTERÍSTICAS TÉCNICAS SONIC WALL TZ 190 69
TABLA 2.7.- CARACTERÍSTICAS TÉCNICAS D-LINK DFL-1600 70
TABLA 2.8.- CARACTERÍSTICAS TÉCNICAS FORTIGATE-100A 72
TABLA 2.9.- CARACTERÍSTICAS TÉCNICAS FORTIGATE-200A 73
TABLA 2.10.- CARACTERÍSTICAS TÉCNICAS SONIC WALL PRO 1260 75
TABLA 2.11.- CARACTERÍSTICAS TÉCNICAS SONIC WALL PRO 3060 76
TABLA 2.12.- CARACTERÍSTICAS TÉCNICAS CISCO ASA 5505 FIREWALL EDITION BUNDLE 77
TABLA 2.13.- LICENCIAS MICROSOFT WINDOWS Y FORTICLIENT PC 82
TABLA 2.14.- COMPARATIVA DE SERVIDORES REQUERIMIENTOS MÍNIMOS DE HARDWARE 82
TABLA 2.15.- PRECIOS DE DISPOSITIVOS FIREWALLS 83
TABLA 2.16.- COSTO APROXIMADO DEL PROYECTO DE SEGURIDAD PARA EL LTI 84
TABLA 3.1.- ACCESOS ADMINISTRATIVOS PARA CADA INTERFAZ 100
TABLA 3.2.- ASIGNACIÓN DE DIRECCIONES PARA LAS INTERFACES 100

CAPÍTULO 1: INTRODUCCIÓN

1.1 ASPECTOS GENERALES

1.1.1 ÁMBITO

El Laboratorio de Tecnologías de la Información (LTI) pertenece al Departamento de Informática y Ciencias de la Computación (DICC) de la Escuela Politécnica Nacional (EPN), que funciona como laboratorio académico a las materias de la carrera de Análisis de Sistemas Informáticos (ASI).

1.1.2 PROBLEMA

El LTI y cualquier organización deben proteger la información que considera confidencial dentro de su propia red, al igual que los servicios y recursos internos; de tal forma que si algún usuario malicioso intenta causar algún tipo de daño no sea posible. Actualmente se establecen conexiones a los servicios sin ningún tipo de seguridad, dejando abierta la posibilidad de ataques de agentes externos.

Además considerando que toda organización en la actualidad debe garantizar la transmisión de los datos de manera segura a través de la red Internet, de manera que éstos no sean hurtados y/o manipulados y que lleguen a su destino de forma íntegra.

De tal manera que se plantea separar los servicios privados de los públicos, así como establecer una conexión segura a los servicios, mediante la implantación de un prototipo de DMZ e interconectar con el Laboratorio Marcelo Dávila y, desde cualquier punto distante, mediante VPN usando el Firewall FortiGate 60, aprovechando la infraestructura con la que cuenta el LTI

1.2 ALCANCE

El presente proyecto plantea realizar el análisis, diseño e implementación de un prototipo de una DMZ y la interconexión segura mediante VPN utilizando el firewall FortiGate 60. Esta aplicación permitirá proteger los recursos compartidos de la red interna de cualquier intento de ataque por parte de intrusos maliciosos, y garantizar una conexión segura con otros host a través de Internet.

1.3 OBJETIVOS

1.3.1 GENERAL

Proteger la red interna de una organización, separando los servicios privados de la red pública así como asegurar la transferencia de datos, mediante el diseño e implementación de DMZ y VPN respectivamente.

1.3.2 ESPECÍFICOS

- Investigar los métodos de ataques que usan los intrusos y hackers
- Investigar las distintas herramientas que existen en el mercado para proteger a la red privada y la transmisión segura de datos e información a través de la red pública
- Analizar las alternativas de solución para implementar una red perimetral (DMZ) y VPN.
- Establecer políticas de seguridad.
- Diseñar e implementar un prototipo de red a través de DMZ y VPN.

1.4 JUSTIFICACIÓN

En la actualidad surge la necesidad de estar en constante comunicación, gracias al Internet podemos recibir una respuesta inmediata en cuestión de segundos sin importar que los sujetos de la comunicación se encuentren separados geográficamente.

El prototipo propuesto permitirá mejorar los siguientes aspectos:

- Habilitar el acceso a usuarios remotos; conectarse y acceder a la red.
- Proporcionar conectividad segura entre dos o múltiples redes privadas o LAN.
- Protección durante la transmisión de los datos.

El esquema general de la implementación de DMZ y VPN se detalla en el capítulo tres

CAPÍTULO 2: MARCO TEÓRICO

2.1 REDES DE COMPUTADORAS[1]

2.1.1 RED DE COMPUTADORAS

Es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información, recursos y servicios.

2.1.2 CLASIFICACIÓN DE LAS REDES

2.1.2.1 Por su tecnología de transmisión (difusión)

2.1.2.1.1 Redes de Broadcast

Las redes de Broadcast tienen un solo canal de comunicación, el medio de transmisión es compartido y los paquetes se envían a toda la red aunque vaya dirigido a un solo destinatario, cada máquina ignora el paquete si no está dirigida a ella, caso contrario lo procesa. Si envía a un subconjunto de máquinas (Multicast), a todas las máquinas (Broadcast).

2.1.2.1.2 Redes Punto a Punto

Las redes punto a punto consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete en este tipo de red puede tener que visitar primero una o más máquinas intermedias.
Como regla general, las redes pequeñas geográficamente localizadas tienden a usar la difusión, mientras que las redes más grandes suelen ser punto a punto.

2.1.2.2 Por su tamaño

Las redes de ordenadores se pueden clasificar según la escala o el grado del alcance de la red.

---

1 http://es.wikipedia.org/wiki/Red_de_computadoras

2.1.2.2.1 Red de Área Personal (PAN)

Personal Área Network es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora cerca de una persona. El alcance de una PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación entre los dispositivos personales de ellos mismos (comunicación del intrapersonal), o para conectar con una red de alto nivel y el Internet (un up link).

2.1.2.2.2 Red de Área Local (LAN)

Una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de la localización.

2.1.2.2.3 Red de Área de Campus (CAN)

Se deriva a una red que conecta dos o más LAN's los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.

2.1.2.2.4 Red de Área metropolitana (MAN)

Es una red que conecta las redes de un área dos o más locales juntos pero no extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Las rebajadoras múltiples, los interruptores y los cubos están conectados para crear a una MAN

2.1.2.2.5 Red Metro Ethernet [2]

Es una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN de nivel 2, a través de UNIs Ethernet. Estas redes denominadas "multiservicio", soportan una amplia gama de servicios, aplicaciones, contando con mecanismos donde se incluye soporte a trafico "RTP" (tiempo real), como puede ser Telefonía IP y Video IP, este tipo de trafico resulta especialmente sensible a retardo y al jitter.

---

2 http://es.wikipedia.org/wiki/Metro_Ethernet

2.1.2.2.6 Red Next Generation Networking (NGN)[3]

Red de Siguiente Generación (Next Generation Networking o NGN en inglés) es un amplio término que se refiere a la evolución de la actual infraestructura de redes de telecomunicación y acceso telefónico con el objetivo de lograr la congruencia de los nuevos servicios multimedia (voz, datos, video...) en los próximos años. La idea principal que se esconde debajo de este tipo de redes es el transporte de paquetes encapsulados de información a través de Internet. Estas nuevas redes serán construidas a partir del protocolo Internet Protocol (IP), siendo el término "all-IP" comúnmente utilizado para describir dicha evolución.

2.1.2.2.7 Red de Área amplia (WAN)

Es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías del teléfono. Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de transmisión de datos, y la capa de red.

2.1.2.3 Por método de conexión

Las redes de ordenadores se pueden clasificar según la tecnología que se utiliza para conectar los dispositivos individuales en la red

2.1.2.3.1 Medios guiados [4]

Se conoce como medios guiados a aquellos que utilizan unos componentes físicos y sólidos para la transmisión de datos. También conocidos como medios de transmisión por cable

- Cable coaxial
- Cable par trenzado
- Cable de fibra óptica

---

3 http://es.wikipedia.org/wiki/Red_de_siguiente_generaci%C3%B3n

4 http://www.monografias.com/trabajos17/medios-de-transmision/medios-de-transmision.shtml

2.1.2.3.2 Medios no guiados

Los medios no guiados o sin cable han tenido gran acogida al ser un buen medio de cubrir grandes distancias y hacia cualquier dirección, su mayor logro se dio desde la conquista espacial a través de los satélites y su tecnología no para de cambiar. La transmisión y recepción se realiza por medio de antenas, las cuales deben estar alineadas cuando la transmisión es direccional, o si es omnidireccional la señal se propaga en todas las direcciones. Entre estas tenemos:

- Señales de radio
- Señales de microondas
- Señales de rayo infrarrojo
- Señales de rayo láser

2.1.2.4 Por relación funcional[5]

Las redes de computadoras pueden clasificarse de acuerdo a la relación funcional que existe entre los elementos de una red, Por ejemplo: Redes activas, Cliente/Servidor y Peer to peer

2.1.2.4.1 Redes activas

Este tipo de redes incluyen la transmisión de datos, pero también de programas que pueden ser ejecutados en los diferentes puntos de la red, su propósito es hacer que la red funcione mejor de acuerdo a los requerimientos de la aplicación que la está utilizando.

2.1.2.4.2 Cliente/Servidor

Este es un tipo de arquitectura donde pueden existir uno o más servidores con uno o más clientes conectados a ellos, cada cliente y servidor se le llama nodo. Los nodos pueden enviar solicitudes de datos a uno o más de los servidores.
Esta arquitectura es de las más populares ya que se puede aplicar a diferentes tipos de aplicaciones, manteniendo el mismo concepto. Aplicaciones como la

---

5 http://www.mitecnologico.com/Main/DeAcuerdoASuRelacion

navegación web, consultas a bases de datos, manejo de correos electrónicos e inclusive juegos en línea utilizan esta arquitectura para funcionar.
Esta arquitectura es muy versátil, ya que se basa en el envío de mensajes y en la modularidad, destacándose por su uso, flexibilidad, interoperabilidad y escalabilidad.

2.1.2.4.3 Peer to peer

Ese tipo de redes conecta una gran cantidad de nodos de forma “ad hoc”, no hace distinción de nodos tipo servidor o cliente, cada nodo funciona como cliente servidor. Todos los participantes en la red se suman al ancho de banda acumulativo de la red, en lugar de mantener recursos centralizados.
Su uso principal es compartir archivos que contienen video, audio, datos, todo lo que se necesite transmitir en tiempo real, como el tráfico telefónico, por ejemplo.
Las redes peer to peer son mas confiables y redundantes en el caso de fallas en alguno de los nodos; además de que ayudan a compartir los recursos de manera compensada entre los participantes y realizan una comunicación multi-punto de una forma eficiente sin depender de la infraestructura multicast de IP

2.1.2.5 Por topología de red

Define cómo están conectadas computadoras, impresoras, dispositivos de red y otros dispositivos. Una topología de red describe la disposición de los cables y los dispositivos, así como las rutas utilizadas para las transmisiones de datos. La topología influye enormemente en el funcionamiento de la red.

2.1.2.5.1 Red de bus [6]

En esta topología, los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable; (el bus). Las tramas de información emitidas por un nodo (terminal o servidor) se propagan por todo el bus (en ambas direcciones), alcanzado a todos los demás nodos. Cada nodo de la red se debe encargar de reconocer la información que recorre el bus, para así determinar cuál es la que le corresponde, la destinada a él.

---

6 http://www.geocities.com/timessquare/chasm/7990/topologi.htm

Es el tipo de instalación más sencillo y un fallo en un nodo no provoca la caída del sistema de la red. Por otra parte, una ruptura del bus es difícil de localizar (dependiendo de la longitud del cable y el número de terminales conectados a él) y provoca la inutilidad de todo el sistema.

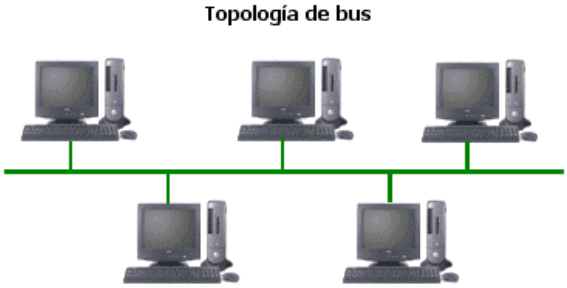


Figura 2.1.- Topología de Bus [7]

2.1.2.5.2 Red de estrella

En la topología en estrella, cada estación tiene una conexión directa a un acoplador (conmutador) central. Una manera de construir esta topología es con conmutadores telefónicos que usan la técnica de conmutación de circuitos.

Otra forma de esta topología es una estación que tiene dos conexiones directas al acoplador de la estrella (nodo central), una de entrada y otra de salida (la cual lógicamente opera como un bus). Cuando una transmisión llega al nodo central, este la retransmite por todas las líneas de salida.

Según su función, los acopladores se catalogan en:

- Acoplador pasivo: cualquier transmisión en una línea de entrada al acoplador es físicamente trasladada a todas las líneas de salida.
- Acoplador activo: existe una lógica digital en el acoplador que lo hace actuar como repetidor. Si llegan bits en cualquier línea de entrada, son automáticamente regenerados y repetidos en todas las líneas de salida. Si llegan simultáneamente varias señales de entrada, una señal de colisión es transmitida en todas las líneas de salida.

---

7 http://members.fortunecity.es/infokmas/index/memorias/memorias_archivos/image004.gif

Figura 2.2.- Topología en estrella 8

2.1.2.5.3 Red de anillo (o doble anillo)

En esta topología la red consiste en un conjunto de repetidores unidos por líneas de comunicación punto a punto, que forman un ciclo cerrado.

Cada repetidor participa en dos enlaces, recibe datos de uno y los transmite al otro; su capacidad de almacenamiento, si tiene, es de sólo unos cuantos bits y la velocidad de recepción y de transmisión es igual en todos los repetidores.

Los enlaces (líneas de comunicación) son simplex, por lo tanto la información fluye en un solo sentido en el anillo. Las estaciones se conectan a la red por medio de los repetidores.

Una red con topología de anillo se organiza conectando nodos de la red en un ciclo cerrado con cada nodo enlazado a los nodos contiguos a la derecha y a la izquierda. La ventaja de esta red es que se puede operar a grandes velocidades, y los mecanismos para evitar colisiones son sencillos.

Algunas veces, estas redes utilizan esquemas de transmisión de señales para determinar qué nodo puede tener acceso al sistema de comunicaciones.

8 http://internett.galeon.com/REDES_archivos/image003.gif

Figura 2.3.- Topología en anillo [9]

2.1.2.5.4 Red en malla (o totalmente conexa)

En una topología en malla, cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta.

Por tanto, una red en malla completamente conectada necesita n(n-1)/2 canales físicos para enlazar n dispositivos. Para acomodar tantos enlaces, cada dispositivo de la red debe tener sus puertos de entrada/salida (E/S).

Figura 2.4.- Topología en malla [10]

2.1.2.5.5 Red en árbol

La topología en árbol es una generalización de la topología en bus. Esta topología comienza en un punto denominado cabezal o raíz (headend). Uno ó más cables

9 http://internett.galeon.com/REDES_archivos/image002.gif

10 http://www.pc-doctor.com.mx/radio%20formula/temas/Redes_archivos/image012.jpg

pueden salir de este punto y cada uno de ellos puede tener ramificaciones en cualquier otro punto. Una ramificación puede volver a ramificarse. En una topología en árbol no se deben formar ciclos.

Una red como ésta representa una red completamente distribuida en la que computadoras alimentan de información a otras computadoras, que a su vez alimentan a otras. Las computadoras que se utilizan como dispositivos remotos pueden tener recursos de procesamientos independientes y recurren a los recursos en niveles superiores o inferiores conforme se requiera.

Figura 2.5.- Topología en árbol [11]

2.1.2.6 Por el tipo de transmisión

Por el tipo de direccionamiento de datos podemos clasificar las redes de la siguiente forma:

2.1.2.6.1 Simplex (unidireccionales)[12]

La transmisión simplex (sx) o unidireccional es aquella que ocurre en una dirección solamente, deshabilitando al receptor de responder al transmisor. Normalmente la transmisión simplex no se utiliza donde se requiere interacción humano-máquina. Ejemplos de transmisión simplex son: La radiodifusión (broadcast) de TV y radio.

---

11 http://internett.galeon.com/REDES_archivos/image004.gif

12 http://www.mitecnologico.com/Main/ModosDeTransmisionSimplexHalfDuplexYFullDuplex

2.1.2.6.2 Half-Duplex (bidireccionales)

La transmisión half-duplex (hdx) permite transmitir en ambas direcciones; sin embargo, la transmisión puede ocurrir solamente en una dirección a la vez. Tanto transmisor y receptor comparten una sola frecuencia. Un ejemplo típico de half-duplex es el radio de banda civil (CB) donde el operador puede transmitir o recibir, pero no puede realizar ambas funciones simultáneamente por el mismo canal. Cuando el operador ha completado la transmisión, la otra parte debe ser avisada que puede empezar a transmitir (diciendo “cambio”).

2.1.2.6.3 Full-Duplex (bidireccionales)

La transmisión full-duplex (fdx) permite transmitir en ambas direcciones, pero simultáneamente por el mismo canal. Existen dos frecuencias una para transmitir y otra para recibir. Ejemplos de este tipo abundan en el terreno de las telecomunicaciones, el caso más típico es la telefonía, donde el transmisor y el receptor se comunican simultáneamente utilizando el mismo canal, pero usando dos frecuencias.

2.2 MODELO OSI

2.2.1 INTRODUCCIÓN [13]

En 1977, la Organización Internacional de Estándares (ISO), integrada por industrias representativas del medio, creó un subcomité para desarrollar estándares de comunicación de datos que promovieran la accesibilidad universal y una interoperabilidad entre productos de diferentes fabricantes.

El resultado de estos esfuerzos es el Modelo de Referencia Interconexión de Sistemas Abiertos (OSI).

OSI nace de la necesidad de uniformizar los elementos que participan en la solución del problema de comunicación entre equipos de cómputo de diferentes fabricantes.

---

13 http://sistemas.itlp.edu.mx/tutoriales/redes/index.htm

2.2.2 CONCEPTO DE MODELO OSI [14]

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI. Así, todo dispositivo de cómputo y telecomunicaciones podrá ser referenciado al modelo y por ende concebido como parte de un sistema interdependiente con características muy precisas en cada nivel.

2.2.3 CAPAS DEL MODELO OSI

Figura 2.6.-. Modelo OSI [15]

2.2.3.1 Capa de Aplicación

Es el nivel más cercano al usuario y a diferencia de los demás niveles, por ser el más alto o el último, no proporciona un servicio a ningún otro nivel.

En OSI el nivel de aplicación se refiere a las aplicaciones de red que vamos a utilizar para transportar las aplicaciones del usuario.

FTP (File Transfer Protocol), Mail, Telnet, son entre otras las aplicaciones incluidas en el nivel 7 del modelo OSI y sólo cobran vida al momento de requerir una comunicación entre dos entidades.

---

14 http://elsitiodetelecomunicaciones.iespana.es/modelo_osi.htm

15http://tbn0.google.com/images?q=tbn:3mTrlL9Q4O5rTM:http://bp0.blogger.com/_GD_DcKMfSls/RdqNw9VVjlI/AAAAAAAAADM/EV5HsVQYyVg/s400/modelo%2Bosi.JPG

2.2.3.2 Capa de Presentación

Se refiere a la forma en que los datos son representados en una computadora. Proporciona conversión de códigos y reformateo de datos de la aplicación del usuario. La información es procesada en forma binaria y en este nivel se llevan a cabo las adaptaciones necesarias para que pueda ser presentada de una manera más accesible. Códigos como ASCII (American Standard Code for Information Interchange) y EBCDIC (Extended Binary Coded Decimal Interchange Code), que permiten interpretar los datos binarios en caracteres que puedan ser fácilmente manejados, tienen su posicionamiento en el nivel de presentación del modelo OSI.

El nivel de Presentación negocia la sintaxis de la transferencia de datos hacia el nivel de aplicación.

2.2.3.3 Capa de Sesión

Este nivel es el encargado de proveer servicios de conexión entre las aplicaciones, tales como iniciar, mantener y finalizar una sesión. Establece, mantiene, sincroniza y administra el diálogo entre aplicaciones remotas.

2.2.3.4 Capa de Transporte

En este nivel se realiza y se garantiza la calidad de la comunicación, ya que asegura la integridad de los datos. Es aquí donde se realizan las retransmisiones cuando la información fue corrompida o porque alguna trama (del nivel 2) detectó errores en el formato y se requiere volver a enviar el paquete o datagrama.

El nivel de transporte notifica a las capas superiores si se está logrando la calidad requerida. Este nivel utiliza reconocimientos, números de secuencia y control de flujo.

Los protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) son característicos del nivel del transporte del modelo OSI, al igual que SPX (Sequenced Packet Exchange) de Novell.

2.2.3.4.1 Orientación de Conexión

Hay dos formas en las que el nivel de red puede funcionar internamente, pero independientemente de que la red funcione internamente con datagramas o con

circuitos virtuales puede dar hacia el nivel de transporte un servicio orientado a conexión:

- Datagramas: Cada paquete se encamina independientemente, sin que el origen y el destino tengan que pasar por un establecimiento de comunicación previo.
- Circuitos virtuales: En una red de circuitos virtuales dos equipos que quieran comunicarse tienen que empezar por establecer una conexión. Durante este establecimiento de conexión, todos los routers que hayan por el camino elegido reservarán recursos para ese circuito virtual específico.

2.2.3.4.2 Tipos de servicio

Hay dos tipos de servicio:

- Servicios Orientados: Sólo el primer paquete de cada mensaje tiene que llevar la dirección destino. Con este paquete se establece la ruta que deberán seguir todos los paquetes pertenecientes a esta conexión. Cuando llega un paquete que no es el primero se identifica a que conexión pertenece y se envía por el enlace de salida adecuado, según la información que se generó con el primer paquete y que permanece almacenada en cada conmutador o nodo.
- Servicios no orientados: Cada paquete debe llevar la dirección destino, y con cada uno, los nodos de la red deciden el camino que se debe seguir. Existen muchas técnicas para realizar esta decisión, como por ejemplo comparar el retardo que sufriría en ese momento el paquete que se pretende transmitir según el enlace que se escoja.

2.2.3.5 Capa de Red [16]

La capa de red, según la normalización OSI, es una capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y

16 http://es.wikipedia.org/wiki/Capa_de_red

se apoya en el nivel de enlace, es decir, utiliza sus funciones.

Para la consecución de su tarea, puede asignar direcciones de red únicas, interconectar subredes distintas, encaminar paquetes y utilizar un control de congestión

2.2.3.6 Capa de Enlace de datos

Conocido también como nivel de Trama (Frame) o Marco, es el encargado de preparar la información codificada en forma binaria en formatos previamente definidos por el protocolo a utilizar.

Tiene su aplicación en el contexto de redes WAN y LAN ya que como se estableció previamente la transmisión de datos no es mas que el envió en forma ordenada de bits de información. Este nivel ensambla los datos en tramas y las transmite a través del medio (LAN o WAN). Es el encargado de ofrecer un control de flujo entre tramas, así como un sencillo mecanismo para detectar errores. Es en este nivel y mediante algoritmos como CRC (Cyclic Redundancy Check), donde se podrá validar la integridad física de la trama; mas no será corregida a este nivel sino que se le notificará al transmisor para su retransmisión.

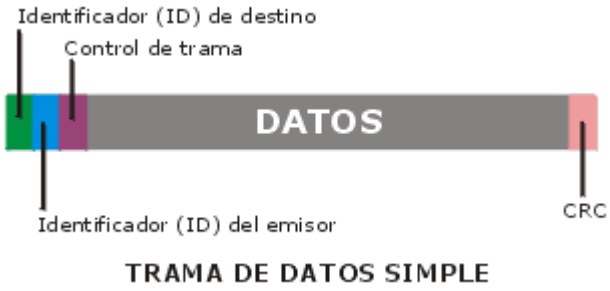


Figura 2.7.- Capa de Enlace de datos [17]

2.2.3.7 Capa Física

Es el primer nivel del modelo OSI y en él se definen y reglamentan todas las características físicas-mecánicas y eléctricas que debe cumplir el sistema para poder operar. Como es el nivel más bajo, es el que se va a encargar de las comunicaciones físicas entre dispositivos y de cuidar su correcta operación. La información computarizada es procesada y transmitida en forma digital siendo

17 http://fmc.axarnet.es/images/redes/paquete_simple.gif

esta de bits: 1 y 0, por lo que, toda aplicación que se desee enviar, será transmitida en forma serial mediante la representación de unos y ceros.

En este nivel se ubican también todos los medios de transmisión como los sistemas de telecomunicaciones para el mundo WAN (Wide Area Network), tales como sistemas satelitales, microondas, radio enlaces, canales digitales y líneas privadas, así como los medios de transmisión para redes de área locales (LAN: Local Area Network), cables de cobre (UTP,STP) y fibra óptica. Además, en este nivel se ubican todos aquellos dispositivos pasivos y activos que permiten la conexión de los medios de comunicación como repetidores de redes LAN, repetidores de microondas y fibra óptica, concentradores de cableado (HUBs), conmutadores de circuitos físicos de telefonía o datos, equipos de modulación y demodulación (módems) y hasta los aparatos receptores telefónicos convencionales o de células que operan a nivel hardware como sistemas terminales.

2.3 MODELO TCP/IP

2.3.1 INTRODUCCIÓN [18]

Internet se desarrolló para brindar una red de comunicación que pudiera continuar funcionando en tiempos de guerra. Aunque la Internet ha evolucionado en formas muy diferentes a las imaginadas por sus arquitectos, todavía se basa en un conjunto de protocolos TCP/IP. El diseño de TCP/IP es ideal para la poderosa y descentralizada red que es Internet.

Todo dispositivo conectado a Internet que desee comunicarse con otros dispositivos en línea debe tener un identificador exclusivo. El identificador se denomina dirección IP. Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI.

---

18 http://www.alfinal.com/Temas/tcpip.shtml

El TCP/IP es la base de Internet, y sirve para comunicar todo tipo de dispositivos, computadoras que utilizan diferentes sistemas operativos, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN). TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa del departamento de defensa.

2.3.2 CONCEPTO MODELO TCP /IP [19]

TCP/IP es junto con OSI una arquitectura de protocolos que ha sido determinante y básica en el desarrollo de los estándares de comunicación. Es la arquitectura más adoptada para la interconexión de sistemas. Al contrario de lo que ocurre con OSI, el modelo TCP/IP es software, es decir, es un modelo para ser implementado en cualquier tipo de red. Facilita el intercambio de información independientemente de la tecnología y el tipo de subredes a atravesar, proporcionando una comunicación transparente a través de sistemas heterogéneos.

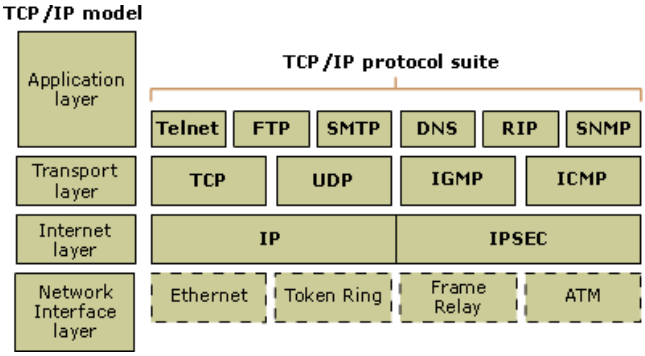


Figura 2.8.- Modelo TCP/IP [20]

Este modelo está compuesto por cuatro capas o niveles que a continuación se indican:

2.3.2.1 Capa de Aplicación [21]

La capa de aplicación del modelo TCP/IP maneja protocolos de alto nivel,

---

19 http://ceres.ugr.es/~alumnos/redrs232/tcpip.htm

20http://technet2.microsoft.com/QueryWS/GetOpenContent.aspx?assetID=4aade787-d5e9-45b4-b779-7475d9b77d98&DocumentSet=es-ES&RenderKey=XML

21 http://www.alfinal.com/Temas/tcpip.shtml

aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y asegura que estos datos estén correctamente empaquetados antes de que pasen a la capa siguiente. TCP/IP incluye no sólo las especificaciones de Internet y de la capa de transporte, tales como IP y TCP, sino también las especificaciones para aplicaciones comunes. TCP/IP tiene protocolos que soportan la transferencia de archivos, e-mail, y conexión remota.

2.3.2.2 Capa de Transporte

La capa de transporte proporciona servicios de transporte desde el host origen hacia el host destino. En esta capa se forma una conexión lógica entre los puntos finales de la red, el host transmisor y el host receptor. Los protocolos de transporte segmentan y reensamblan los datos mandados por las capas superiores en el mismo flujo de datos, o conexión lógica entre los extremos. La corriente de datos de la capa de transporte brinda transporte de extremo a extremo.

La capa de transporte envía los paquetes de datos desde la fuente transmisora hacia el destino receptor a través de la nube (Internet). El control de punta a punta, que se proporciona con las ventanas deslizantes y la confiabilidad de los números de secuencia y acuses de recibo, es el deber básico de la capa de transporte cuando utiliza TCP. La capa de transporte también define la conectividad de extremo a extremo entre las aplicaciones de los hosts.

2.3.2.3 Capa de Internet

Esta capa tiene como propósito seleccionar la mejor ruta para enviar paquetes por la red. El protocolo principal que funciona en esta capa es el Protocolo de Internet (IP). La determinación de la mejor ruta y la conmutación de los paquetes ocurren en esta capa.

2.3.2.4 Capa de Acceso de Red

También denominada capa de host de red. Esta es la capa que maneja todos los aspectos que un paquete IP requiere para efectuar un enlace físico real con los medios de la red. Esta capa incluye los detalles de la tecnología LAN y WAN y

todos los detalles de las capas; física y de enlace de datos del modelo OSI.
Los controladores para las aplicaciones de software, las tarjetas de módem y otros dispositivos operan en la capa de acceso de red. La capa de acceso de red define los procedimientos para realizar la interfaz con el hardware de la red y para tener acceso al medio de transmisión.
Son funciones de esta capa: la asignación de direcciones IP a las direcciones físicas, el encapsulamiento de los paquetes IP en tramas. Basándose en el tipo de hardware y la interfaz de la red, la capa de acceso de red definirá la conexión con los medios físicos de la misma.

2.4 DIRECCIONAMIENTO IP [22]

Para poder comunicarse en una red, cada equipo debe tener una dirección IP exclusiva. En el direccionamiento IP en clases, existen tres clases de dirección que se utilizan para asignar direcciones IP a los equipos. El tamaño y tipo de la red determinará la clase de dirección IP que aplicaremos cuando proporcionemos direcciones IP a los equipos y otros hosts de nuestra red.
La dirección IP es el único identificador que diferencia un equipo de otro en una red y ayuda a localizar dónde reside ese equipo. Se necesita una dirección IP para cada equipo y componente de red, como un router, que se comunique mediante TCP/IP.

2.4.1 DIRECCIONAMIENTO IPV4

Un Router envía los paquetes desde la red origen a la red destino utilizando el protocolo IP. Los paquetes deben incluir un identificador tanto para la red origen como para la red destino.
Utilizando la dirección IP de una red destino, un Router puede enviar un paquete a la red correcta. Cuando un paquete llega a un Router conectado a la red destino, este utiliza la dirección IP para localizar el computador en particular conectado a la red.
Cada dirección IP consta de dos partes. Una parte identifica la red donde se

22 http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

conecta el sistema y la segunda identifica el sistema en particular de esa red.

2.4.1.1 Componentes de una dirección IP

Una dirección IP está formada por dos partes:
ID de host y el ID de red.

- ID de red: La primera parte de una dirección IP es el ID de red, que identifica el segmento de red en el que está ubicado el equipo. Todos los equipos del mismo segmento deben tener el mismo ID de red.
- ID de host: La segunda parte de una dirección IP es el ID de host, que identifica un equipo, un router u otro dispositivo de un segmento.

El ID de cada host debe ser exclusivo en el ID de red. La combinación del ID de red y el ID de host debe ser exclusivo para todos los equipos que se comuniquen entre sí.

2.4.1.2 Clases de direcciones de Internet IPV4

Las direcciones IP se dividen en clases para definir las redes de tamaño pequeño, mediano y grande.

2.4.1.2.1 Clase A

Las direcciones de clase A se asignan a redes con un número muy grande de hosts. Esta clase permite 126 redes, utilizando el primer número para el ID de red. Los tres números restantes se utilizan para el ID de host, permitiendo 16.777.214 hosts por red.
La red 127.0.0.0 se reserva para las pruebas de loopback. Los Routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes nuevamente hacia ellos mismos. Por lo tanto, no se puede asignar este número a una red.

2.4.1.2.2 Clase B

Las direcciones de clase B se asignan a redes de tamaño mediano a grande. Esta clase permite 16.384 redes, utilizando los dos primeros números para el ID de red. Los dos números restantes se utilizan para el ID de host, permitiendo 65.534 hosts por red.

2.4.1.2.3 Clase C

Las direcciones de clase C se utilizan para redes de área local (LANs) pequeñas. Esta clase permite aproximadamente 2.097.152 redes utilizando los tres primeros números para el ID de red. El número restante se utiliza para el ID de host, permitiendo 254 hosts por red.

2.4.1.2.4 Clase D Y E

Las clases D y E no se asignan a hosts. Las direcciones de clase D se utilizan para la multidifusión, y las direcciones de clase E se reservan para uso futuro.
Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.

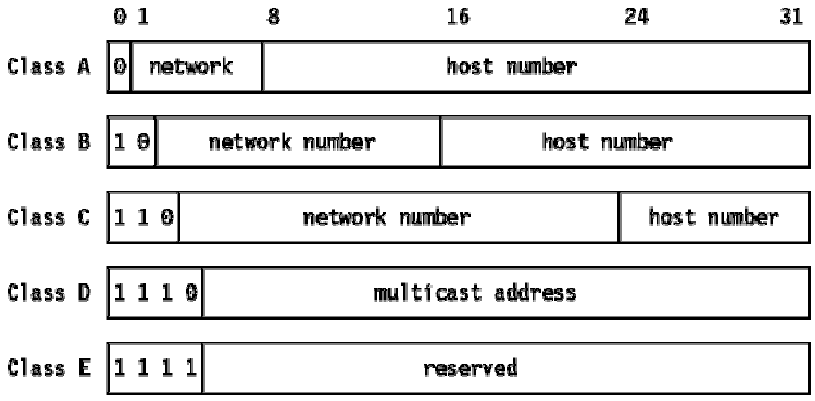


Figura 2.9.- Clases asignadas de direcciones de Internet [23]

2.4.1.3 Cabecera IPV4 [24]

La cabecera IP tiene un tamaño de 160 bits (20 bytes) y está formada por varios campos de distinto significado. Estos campos son:

23 http://ditec.um.es/laso/docs/tut-tcpip/3376f2.gif

24 http://www.gratisweb.com/gulle79/netw ork/ip/ipv4.htm

Figura 2.10.- Cabecera IPV4

Donde:

- Versión: Número de versión del protocolo IP utilizado. Tendrá que tener el valor 4. Tamaño: 4 bit..
- Longitud de la cabecera: (Internet Header Length, IHL) Especifica la longitud de la cabecera expresada en el número de grupos de 32 bit que contiene. Tamaño: 4 bit.
- Tipo de servicio: o calidad de servicio se utiliza para indicar la prioridad o importancia de los datos que se envían, lo que condicionará la forma en que éstos serán tratados durante la transmisión. Tamaño: 8 bit.
- Longitud total: Es la longitud en bytes del datagrama completo, incluyendo la cabecera y los datos. Como este campo utiliza 16 bit, el tamaño máximo del datagrama no podrá superar los 65.535 bytes, aunque en la práctica este valor será mucho más pequeño. Tamaño: 16 bit.
- Identificación: Valor de identificación que se utiliza para facilitar el ensamblaje de los fragmentos del datagrama. Tamaño: 16 bit.
- Flags: Indicadores utilizados en la fragmentación. Tamaño: 3 bit.
- Fragmentación: Contiene un valor (offset) para poder ensamblar los datagramas que se hayan fragmentado. Está expresado en número de grupos de 8 bytes (64 bit), comenzando con el valor cero para el primer fragmento. Tamaño: 16 bit.
- Tiempo de existencia: Contiene un número que disminuye cada vez que el paquete pasa por un sistema. Si este número llega a cero, el paquete será descartado. Esto es necesario por razones de seguridad para evitar un bucle infinito, ya que aunque es bastante improbable que esto suceda en

una red correctamente diseñada, no debe descuidarse esta posibilidad. Tamaño: 8 bit.

- Protocolo: El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. Tamaño: 8 bit.
- Suma Comprobación: El campo de comprobación (checksum) es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del campo de comprobación de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el límite de existencia. Tamaño: 16 bit.
- Dirección de origen: Contiene la dirección del host que envía el paquete. Tamaño: 32 bit.
- Dirección de destino: Esta dirección es la del host que recibirá la información. Los routers o gateways intermedios deben conocerla para dirigir correctamente el paquete. Tamaño: 32 bit.
- Opciones IP: Permite que IP soporte varias opciones, como la seguridad (longitud variable)
- Relleno: se agregan ceros adicionales a este campo para garantizar que el encabezado IP siempre sea un múltiplo de 32 bits

2.4.2 DIRECCIONAMIENTO IPV6 [25]

El cambio más grande de IPv4 a IPv6 es la longitud de las direcciones de red. Las direcciones IPv6, definidas en el RFC 2373 y RFC 2374, son de 128 bits; esto corresponde a 32 dígitos hexadecimales, que se utilizan normalmente para escribir las direcciones IPv6, como se describe en la siguiente sección.

El número de direcciones IPv6 posibles es de $2^{128} \approx 3.4 \times 10^{38}$. Este número

25 http://es.wikipedia.org/wiki/IPv6

puede también representarse como 16^{32}, con 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores.

En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

2.4.2.1 Tipos de direcciones en IPV6

2.4.2.1.1 Unicast [26]

Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPV4 actuales.

2.4.2.1.2 Anycast

Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos.) Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de encaminado). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el routing).

2.4.2.1.3 Multicast

Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (broadcast).

2.4.2.2 Representación de las direcciones

La representación de las direcciones tiene la siguiente representación:

---

26 http://bjcu.uca.edu.ni/LibrosIsti/Tutorial_de_IPV6.pdf

- x:x:x:x:x:x:x:x, donde “x” es un valor hexadecimal de 16 bits de la porción correspondiente a la dirección IPV6. No es preciso escribir los ceros a la izquierda de cada campo
- Dado que por el direccionamiento que se ha definido, podrán existir largas cadenas de bits “cero”, se permite la escritura de su abreviación, mediante el uso de “::”, que representa múltiples grupos consecutivos de 16 bits “cero”. Este símbolo sólo puede aparecer una vez en la dirección IPV6.
- Una forma alternativa y muy conveniente, cuando se encuentra en un entorno mixto IPV4 e IPV6, es x:x:x:x:x:x:d:d:d:d, donde “x” representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y “d” representa valores decimales de las 4 porciones de 8 bits de menor peso (representación estándar IPV4).

2.4.2.3 Cabecera IPv6

La cabecera principal de IPv6 tiene, al contrario que la cabecera de IPv4, un tamaño fijo de 40 octetos. Y esta es su estructura:

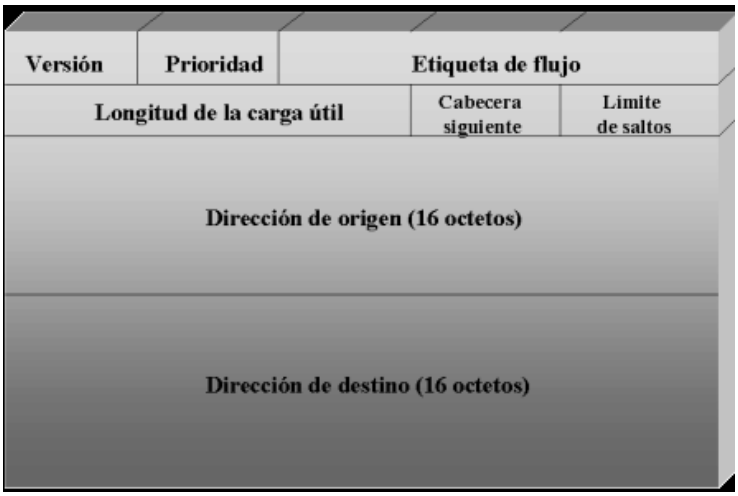


Figura 2.11.- Cabecera Fija IPV6 [27]

Donde:

- Versión deberá valer 6, en formato de 4 bits.
- Prioridad indicará el tipo de tráfico (se pretende asignar prioridades al trafico según sus necesidades).

27 http://www.dei.uc.edu.py/tai2003/ipv6/imagenes/cabeipv4.gif

- Etiqueta de flujo permitirá tratar de manera más eficiente lso flujos de información como los que se generan en aplicaciones multimedia.
- Longitud de la carga útil indica el tamaño de los datos enviados en la trama.
- Cabecera siguiente avisa de la existencia de cabeceras adicionales (o de extensión).
- Limite de saltos viene a sustituir al antiguo TTL, dándole un nombre adecuado al uso que de ese campo se hacía.
- Dirección de origen y dirección de destino Los dos campos de dirección son de 16 bytes.

2.5 COMPARACIÓN ENTRE MODELOS OSI Y TCP/IP

2.5.1 SIMILITUD ENTRE EL MODELO OSI Y EL MODELO TCPIP

Ambos se dividen en capas o niveles.

Se supone que la tecnología es de conmutación de paquetes (no de conmutación de circuitos).

Los profesionales de networking deben conocer ambos: OSI como modelo; TCP/IP como arquitectura real.

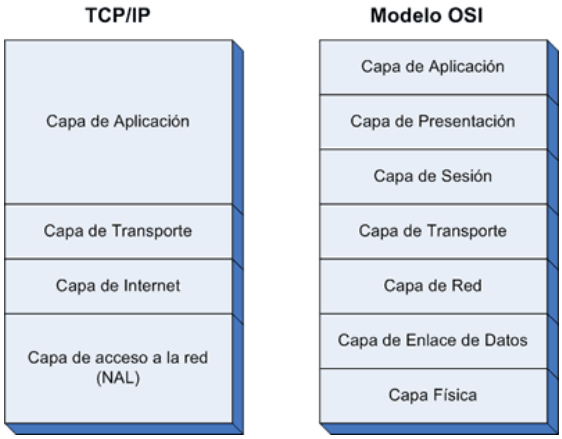


Figura 2.12.- Comparación modelos TCP/IP OSI [28]

28 http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

2.5.2 DIFERENCIA ENTRE EL MODELO OSI Y EL MODELO TCPI

- OSI distingue de forma clara los servicios, las interfaces y los protocolos. TCP/IP no lo hace así, no dejando de forma clara esta separación.
- OSI fue definido antes de implementar los protocolos, por lo que algunas funcionalidades necesarias fallan o no existen. En cambio, TCP/IP se creó después que los protocolos, por lo que se amolda a ellos perfectamente.
- TCP/IP parece ser más simple porque tiene menos capas.

2.6 PROTOCOLOS DE TCP /IP [29]

TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. En Internet se diferencian cuatro niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- Aplicación: Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).
- Transporte: Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar

29 http://elsitiodetelecomunicaciones.iespana.es/protocolo_tcp_ip.htm

los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

- Internet: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.
- Enlace: Los niveles OSI correspondientes son el de enlace y el nivel físico. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada host, como puede ser una línea punto a punto o una red Ethernet.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

2.7 SEGURIDAD INFORMÁTICA

2.7.1 INTRODUCCIÓN [30]

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

---

30 http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. “hackers”, “crakers”, entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes

Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red.

2.7.2 CONCEPTO DE SEGURIDAD INFORMÁTICA [31]

La seguridad informática consiste en asegurar que los recursos de los sistemas de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

2.7.3 GENERALIDADES

2.7.3.1 Alias

Nombre diferente por el cual se conoce un virus.

2.7.3.2 Cracker

Persona que elimina las protecciones lógicas y físicas de los sistemas para acceder a los mismos sin autorización y generalmente con malas intenciones.

2.7.3.3 Hacker [32]

Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos con el fin de obtener información secreta. Además, este término incluye a los cibernautas que realizan operaciones delictivas a través de

31 http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

32 http://www.mastermagazine.info/termino/5204.php

las redes de ordenadores existentes

2.7.3.4 Pirata Informático

Persona que accede a un sistema informático sin autorización para observar su funcionamiento interno y explotar vulnerabilidades. Este término se suele utilizar indistintamente con el término cracker (intruso), pero supuestamente hacker no implica necesariamente malas intenciones, mientras que cracker sí.

2.7.4 VIRUS INFORMÁTICOS[33]

Los virus informáticos son programas diseñados expresamente para interferir en el funcionamiento de una computadora, registrar, dañar o eliminar datos, o bien para propagarse a otras computadoras y por Internet, a menudo con el propósito de hacer más lentas las operaciones y provocar otros problemas en los procesos.

2.7.4.1 Tipos de Virus de Informáticos [34]

Todos los virus tienen en común una característica, y es que crean efectos perniciosos. A continuación tipos de virus informáticos, basada en el daño que causan y efectos que provocan.

2.7.4.1.1 Gusano o Worm

Es un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, se copia así mismo sucesivamente, hasta que desborda la RAM, siendo ésta su única acción maligna.

2.7.4.1.2 Virus de sobreescritura

Sobrescriben en el interior de los archivos atacados, haciendo que se pierda el contenido de los mismos.

2.7.4.1.3 Virus de Programa

Comúnmente infectan archivos con extensiones .EXE, .COM, .OVL, .DRV, .BIN,

---

33 http://www.microsoft.com/latam/athome/security/viruses/intro_viruses_what.mspx

34 http://www.cafeonline.com.mx/virus/tipos-virus.html

.DLL, y .SYS., los dos primeros son atacados más frecuentemente por que se utilizan mas.

2.7.4.1.4 Virus falso o Hoax

Los denominados virus falsos en realidad no son virus, sino cadenas de mensajes distribuidas a través del correo electrónico y las redes. Estos mensajes normalmente informan acerca de peligros de infección de virus, los cuales mayormente son falsos y cuyo único objetivo es sobrecargar el flujo de información a través de las redes y el correo electrónico de todo el mundo

2.7.4.1.5 Virus Múltiples

Son virus que infectan archivos ejecutables y sectores de booteo simultáneamente, combinando en ellos la acción de los virus de programa y de los virus de sector de arranque.

2.7.5 TIPOS DE ATAQUES [35]

2.7.5.1 Shoulder Surfing

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El Surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora (generalmente en post–it adheridos al monitor o teclado). Cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior uso. Otra técnica relacionada al surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y password.

2.7.5.2 Eavesdropping–Packet Sniffing

Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red.
Esto se realiza con Packet Sniffers, los cuales son programas que monitorean los paquetes que circulan por la red. Los Sniffers pueden ser colocados tanto en una

35 http://www.segu-info.com.ar/ataques/ataques_monitorizacion.htm

estación de trabajo conectada a la red, como a un equipo Router o a un Gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

2.7.5.3 Snooping–Downloading

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla.
Sin embargo los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

2.7.5.4 Spoofing

Es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

2.7.5.5 Barrido de puertos [36]

Un barrido de puertos trata de identificar qué puertos TCP y UDP están abiertos en el computador para aprovechar ciertos servicios que dependen de ellos para entrar en el sistema. Existen infinidad de herramientas de barrido de puertos accesibles en la red a cualquiera y ésta será una de las cosas que primero compruebe un atacante.

2.7.5.6 Detección de Proxies

La finalidad de este tipo de ataque es buscar proxies que puedan estar instalados mal configurados o de mala calidad, pero no para comprometer la seguridad de los equipos a los que éste apantalla, sino para convertir sus ataques en anónimos. Dado que casi todos los servidores llevan un registro de las direcciones IP desde las que se accede a ellos, si un individuo malintencionado

---

36 http://www.zonagratuita.com/a-cursos/hacking/UtilizacionFirewalls.htm

quisiera atacarlos sería fácil seguirle la pista a través de su IP. Sin embargo, utilizando un proxie ajeno que enmascararía su verdadera IP, el ataque parecería que proviene de dicho proxie, ocultando las huellas del verdadero agresor y cargando las culpas a quien no las tiene.

2.7.5.7 Ataques Smurf/Fraggle

Este ataque se basa en el envío de paquetes de difusión a los ordenadores de una subred (que llegan a todos los ordenadores). Estos paquetes llevan falseada la dirección de origen, apuntando en realidad a un servidor que se desea atacar (técnica conocida como spoofing). Todos los ordenadores de la subred responden a los paquetes falsos dirigiéndolos a la víctima, la cual se ve sobrecargada instantáneamente por el enorme efecto multiplicador debido a la difusión.

2.7.6 MÉTODOS DE HACKING [37]

2.7.6.1 Caballo de Troya

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente (Formatear el disco duro, modificar un fichero, sacar un mensaje, etc.)
Suele ser utilizado para cambiar la pantalla de login (imitandola), descubriendo de esta manera la password del usuario

2.7.6.2 Superzapping

Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador. El nombre proviene de una utilidad llamada SUPERZAP diseñada para Mainframes y que permite acceder a cualquier parte del ordenador y modificarlo.

---

37 http://hezek-x.galeon.com/aficiones159608.html

2.7.6.3 Puertas Falsas

Es una práctica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, con objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario éstas rutinas no se eliminan del programa y proveen al hacker accesos o facilidades en su labor si sabe descubrirlas.

2.7.6.4 Bombas lógicas

Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá o modificará la información, o provocará el cuelgue del sistema.

2.7.7 VULNERABILIDADES

2.7.7.1 Negación de servicio (denial of service)

Es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos.

2.7.7.2 Cracking de password

Una vez encriptada una clave, no se puede desencriptar. Sin embargo, esto no garantiza la seguridad de la clave, puesto que no significa que la clave no se pueda averiguar.

El mecanismo que se utiliza para descubrir (no desencriptar) las claves consiste en efectuar encriptaciones de palabras (posibles claves) y comparar estas encriptaciones con el original.

2.7.7.3 E-mail bombing y spamming

E-mail bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando el mailbox del destinatario.

El spamming que es una variante del e-mail bombing, se refiere a enviar el email a centenares o millares de usuarios e, inclusive, a listas de interés. El Spamming

puede resultar aún más perjudicial si los destinatarios contestan el mail, haciendo que todos reciban la respuesta.

2.7.7.4 Consideraciones de software [38]

Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el software pirata o sin garantías aumenta los riesgos).

2.7.7.5 Consideraciones de una red

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles. Mantener al máximo el número de recursos de red sólo en modo lectura, impide que ordenadores infectados propaguen virus.

2.7.8 SISTEMAS OPERATIVOS [39]

2.7.8.1 Software Libre (Open Source)

2.7.8.1.1 GNU/Linux

El proyecto GNU se inició en 1984 con el objetivo de crear un sistema operativo completo tipo Unix de software libre.
GNU es el término empleado para referirse al sistema operativo similar a Unix que utiliza como base las herramientas de sistema de GNU y el núcleo Linux. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo el código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL de GNU (Licencia Pública General de GNU)

2.7.8.1.1.1 Características

- **Multiplataforma.-** Dispone de varios tipos de sistema de archivos para poder acceder a archivos en otras plataformas.

---

38 http://www.jbex.net/seguridad-informatica

39 http://es.wikipedia.org/wiki/

- **Multiusuario.-** Es un sistema operativo capaz de responder, simultáneamente, a las solicitudes de varios usuarios que empleen el mismo ordenador, incluso con necesidades distintas. Además proporciona los elementos necesarios para garantizar la seguridad y privacidad de los datos entre los diferentes usuarios.
- **Multitarea.-** Permite ejecutar varios programas a la vez, de forma que no tiene que esperar a que termine uno para empezar otro. La multitarea está controlada por el Sistema Operativo y no por las aplicaciones, por lo que es muy difícil que el fallo de un programa colapse el sistema por una mala utilización de los recursos del equipo.
- **Estabilidad.-** Es robusto, por lo que si un programa falla no interrumpirá el trabajo de los demás. Esta característica permite que el sistema funcione durante períodos muy largos de tiempo sin necesidad de parar y volver a arrancar.
- **Es libre.-** Al disponer del código fuente, se puede hacer cualquier modificación sin tener que esperar que alguien envíe un parche para solucionarlo.

2.7.8.2 Software bajo licenciamiento

2.7.8.2.1 Windows Server 2003 (Servidor)

Es un sistema operativo de la familia Windows de la marca Microsoft para servidores que salió al mercado en el año 2003

Windows Server 2003 se podría considerar como un Windows XP modificado, no con menos funciones, sino que se encuentran deshabilitadas por defecto para obtener un mejor rendimiento y para centrar el uso de procesador en las características de servidor

2.7.8.2.1.1 Características

- Sistema de archivos NTFS:
- Gestión de almacenamiento, backups; incluye gestión jerárquica del almacenamiento, consiste en utilizar un algoritmo de caché para pasar los datos menos usados de discos duros a medios ópticos o similares más lentos, y volverlos a leer a disco duro cuando se necesitan.

- Windows Driver Model: Implementación básica de los dispositivos más utilizados, de esa manera los fabricantes de dispositivos sólo han de programar ciertas especificaciones de su hardware.
- ActiveDirectory Directorio de organización basado en LDAP, permite gestionar de forma centralizada la seguridad de una red corporativa a nivel local.
- Autentificación Kerberos5
- DNS con registro de IP's dinámicamente
- Políticas de seguridad

2.7.8.2.2 Windows XP (Cliente)

Windows XP es una línea de sistemas operativos desarrollado por Microsoft que fueron hechos públicos el 25 de octubre de 2001

XP provienen de la palabra 'e**XP**erience' en inglés. Tiene una interfaz gráfica de usuario (GUI) perceptiblemente reajustada, un cambio de Microsoft promovido para un uso más fácil que en las versiones anteriores. Es también la primera versión de Windows que utiliza la activación del producto para reducir la piratería del software,

2.7.8.2.2.1 Características

- Ambiente totalmente gráfico
- Secuencias más rápidas de inicio y de hibernación.
- Capacidad del sistema operativo de desconectar un dispositivo externo, de instalar nuevas aplicaciones y controladores sin necesidad de reiniciar.
- Una nueva interfaz de uso más fácil, incluyendo herramientas para el desarrollo de temas de escritorio.
- Uso de varias cuentas, que permite un usuario guarde el estado actual y aplicaciones abiertos en su escritorio y permita que otro usuario abra una sesión sin perder esa información.
- ClearType, diseñado para mejorar legibilidad del texto encendido en pantallas de cristal líquido (LCD) y monitores similares.
- Escritorio Remoto, que permite a los usuarios abrir una sesión con una computadora que funciona con Windows XP a través de una red o Internet,

teniendo acceso a sus usos, archivos, impresoras, y dispositivos;

2.8 SERVIDORES

2.8.1 SERVIDOR DE CORREO [40]

El correo electrónico clasifica como el servicio más utilizado de todos los que existen actualmente de arquitectura cliente-servidor, teniendo la posibilidad de comunicarse rápidamente con todo el mundo desde una estación de trabajo de forma muy simple y barata. Basta con tener un buzón en un servidor de correo correctamente configurado y una aplicación cliente para operar con dicho buzón. Un buzón de correo electrónico no es más que un fichero o un conjunto de ellos agrupados en un directorio donde se almacenan en cierto formato los mensajes que llegan

2.8.1.1 Protocolo de transporte de correo

2.8.1.1.1 SMTP (Protocolo Simple de Transferencia)

Se encarga de transmitir correo entre servidores de correo. Sin embargo, es crítico para los clientes de correo también. Para poder enviar correo, el cliente envía el mensaje a un servidor de correo saliente, el cual luego contacta al servidor de correo de destino para la entrega. Por esta razón, es necesario especificar un servidor SMTP cuando se esté configurando un cliente de correo.
No requiere autenticación; esto permite que cualquiera en el Internet pueda enviar correo a cualquier otra persona o a grandes grupos de personas.

2.8.1.2 Protocolos de acceso a correo

Hay dos protocolos principales usados por las aplicaciones de correo cliente para recuperar correo desde los servidores de correo: el Post Office Protocol (POP) y el Internet Message Access Protocol (IMAP).
A diferencia de SMTP, estos protocolos requieren autenticación de los clientes usando un nombre de usuario y una contraseña. Por defecto, las contraseñas

40 http://www.ispcmw.rimed.cu/sitios/digbiblio/cont/EI/SO_Linux/Avanzado-html/node96.html

para ambos protocolos son pasadas a través de la red sin encriptar.

2.8.1.2.1 POP

Cuando se utiliza POP, los mensajes de correo son descargados a través de las aplicaciones de correo cliente. Por defecto, la mayoría de los clientes de correo POP son configurados para borrar automáticamente el mensaje en el servidor de correo después que éste ha sido transferido exitosamente, sin embargo esta configuración se puede cambiar.
La versión más reciente del protocolo estándar POP es POP3.

2.8.1.2.2 Imap

Al utilizar un servidor de correo IMAP, los mensajes de correo se mantienen en el servidor donde los usuarios pueden leerlos o borrarlos. IMAP también permite a las aplicaciones cliente crear, renombrar o borrar directorios en el servidor para organizar y almacenar correo.
Lo utilizan principalmente los usuarios que acceden a su correo desde varias máquinas.
El protocolo es conveniente también para usuarios que se estén conectando al servidor de correo a través de una conexión lenta, porque sólo la información de la cabecera del correo es descargada para los mensajes, hasta que son abiertos, ahorrando de esta forma ancho de banda. El usuario también tiene la habilidad de eliminar mensajes sin verlos o descargarlos.
IMAP, como POP, es completamente compatible con estándares de mensajería de Internet, tales como MIME, que permite los anexos de correo.

2.8.1.3 Clasificación de los programas de correo

2.8.1.3.1 MTAs (Mail Transport Agent)

Agentes para la transmisión de correo son aquellos programas servidores que permiten transportar el correo electrónico de una máquina a otra a través de la red. Como ejemplos de MTAs se pueden citar a Sendmail, Postfix y otros. Todos hablan el mismo idioma, o sea utilizan un protocolo común para la comunicación: el SMTP (Simple Mail Transfer Protocol). El SMTP como su nombre lo indica es un protocolo muy simple orientado a caracteres y que permite el traslado de los

correos tanto desde el cliente al servidor como entre servidores. Normalmente los servidores de correo utilizan el puerto 25 para comunicarse mediante el SMTP.

2.8.1.3.1.1 Sendmail

Es el agente de transporte de correo (MTA) por defecto de FreeBSD. La responsabilidad de sendmail consiste en aceptar correo de agentes de correo de usuario (MUA) y en entregar dichos correos al agente de transporte de correo apropiado, según se especifique en su archivo de configuración. Sendmail también acepta conexiones de red provenientes de otros agentes de transporte y puede depositar el correo recibido en carpetas locales o entregarlo a otros programas.

2.8.1.3.1.2 Postfix [41]

Es un agente de transporte de correo electrónico (MTA) bastante reciente que se suma a la lista de alternativas al legendario Sendmail. En su diseño han primado factores como la seguridad, la eficiencia y la facilidad de configuración y administración, junto con la compatibilidad con Sendmail y con otros sistemas de correo. .

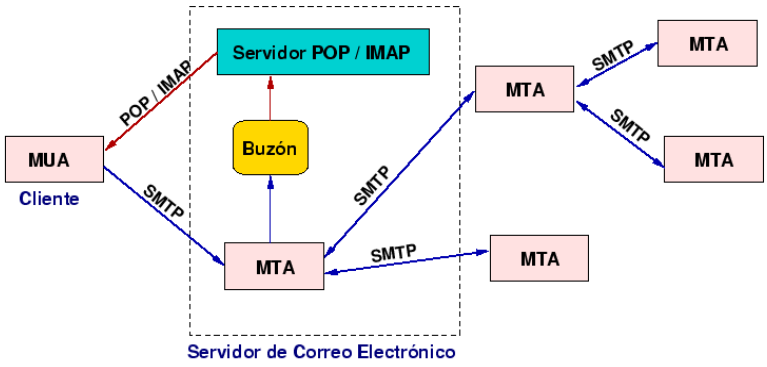


Figura 2.13.- Representación esquemática del servicio de correo electrónico

2.8.1.3.2 MDA (Mail Delevery Agents) [42]

Los Agentes de entrega de correo forman el núcleo del sistema de correo electrónico. Estos programas, que por regla general se ejecutan en segundo

41 http://www.uco.es/ccc/sistemas/postfix/intro.html

42 http://docs.hp.com/es/5992-4614/ch07s01.html

plano, son responsables de enrutar y entregar el correo electrónico.
Un MTA invoca a un Agente de entrega de correos (MDA) para archivar el correo entrante en el buzón de correo del usuario. En muchos casos, el MDA es en realidad un Agente de entregas local (LDA), tal como mail o Procmail.
Cualquier programa que maneje la entrega de mensajes hasta el punto en que puede ser leído por una aplicación cliente de correos se puede considerar un MDA.
Por esta razón, algunos MTAs (tales como Sendmail y Postfix) pueden tener el papel de un MDA cuando ellos anexan nuevos mensajes de correo al archivo spool de correo del usuario.

2.8.1.3.3 MUAs (Mail User Agents)

Son los programas clientes que posibilitan a los usuarios manipular su mensajería. Estos programas son ejecutados directamente por los usuarios. Proveen facilidades para escribir los mensajes, enviarlos, descargar y leer los que llegan, organizarlos en directorios, hacer búsquedas, imprimirlos, mantener un libro de direcciones electrónicas, etc.
Muchos MUAs son capaces de recuperar mensajes a través de los protocolos POP o IMAP, configurando los buzones de correo para almacenar mensajes y enviando los mensajes salientes a un MTA. Los MUAs pueden ser de interfaz gráfica, tal como Thunderbird, o tener una interfaz basada en texto muy sencilla, tal como mutt.
Aunque parezca que los Agentes de usuario de correo realizan todo el trabajo de transmisión y recepción de correo electrónico, dichos agentes sólo constituyen la parte visible de todo el sistema de correo electrónico. En realidad, no entregan el correo electrónico; son los Agentes de entrega de correo los que entregan el correo electrónico

2.8.2 SERVIDOR WEB [43]

Es un programa que implementa el protocolo HTTP (HyperText Transfer

43 http://es.wikipedia.org/wiki/IIS

Protocol). Este protocolo pertenece a la capa de aplicación del modelo OSI y está diseñado para transferir lo que llamamos hipertextos, páginas web o páginas HTML (HyperText Markup Language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música.

2.8.2.1 Apache

El Servidor Apache HTTP es un servidor Web de tecnología Open Source sólido y para uso comercial desarrollado por la Apache Software Foundation (www.apache.org). Red Hat Enterprise Linux incluye el Servidor Apache HTTP versión 2.0 así como también una serie de módulos de servidor diseñados para mejorar su funcionalidad.

Apache ocupa un enorme porcentaje del mercado, superando de esta forma a cualquier otro servidor Web de cualquier otro sistema operativo por la cantidad de sitios Web que maneja.

2.8.2.1.1 Características

- Portabilidad: Puede ser instalado en casi cualquier sistema operativo
- Modularidad: Acepta la instalación de módulos realizados por terceras personas para agregarle funcionalidad
- Independencia de los lenguajes de generación de páginas: cualquier lenguaje que su autor decida, puede ser modularizado y usado para generar páginas web.
- Puede manejar varios sitios web, tantos como el sistema operativo pueda aguantar

2.8.2.2 Internet Information Servers (IIS)

Es una serie de servicios para los ordenadores que funcionan con Windows. Originalmente era parte del Option Pack para Windows NT. Luego fue integrado en otros sistemas operativos de Microsoft (Windows 2000 o Windows Server 2003. Windows XP Profesional incluye una versión limitada de IIS) destinados a ofrecer servicios como son: FTP, SMTP, NNTP y HTTP/HTTPS.

2.8.2.2.1 Características

- Cifrado y métodos de autenticación mediante certificados de cliente y servidor, mediante SSL (Secure Sockets Layer). Esto proporciona un método para transferir datos entre el cliente y el servidor de forma segura, permitiendo también que el servidor pueda comprobar al cliente antes de que inicie una sesión de usuario.
- Otra característica nueva es la autenticación implícita que permite a los administradores autenticar a los usuarios de forma segura a través de servidores de seguridad y proxy.
- También es capaz de impedir que aquellos usuarios con direcciones IP conocidas obtengan acceso no autorizado al servidor, permitiendo especificar la información apropiada en una lista de restricciones

2.8.3 SERVIDOR BASE DE DATOS

Un servidor de base de datos es un programa que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio. Los sistemas de administración de base de datos (SGBD) generalmente proveen funcionalidades para servidores de base de datos, en cambio otros (como por ejemplo, MySQL) solamente proveen construcción y acceso a la base de datos.
Dentro de los servidores de datos más conocidos tenemos; Oracle, Informix, MySQL, PostgreSQL, DB2, SAP pero el que se va a implementar es MySQL.

2.8.3.1 MySQL

Es un sistema de administración de bases de datos (Database Management System, DBMS) para bases de datos relacionales. Como base de datos relacional, utiliza múltiples tablas para almacenar y organizar la información.
MySQL fue escrito en C y C++ y destaca por su gran adaptación a diferentes entornos de desarrollo, permitiendo su interacción con los lenguajes de programación más utilizados como PHP, Perl y Java y su integración en distintos sistemas operativos.

2.8.3.1.1 PhpMyAdmin

Es una herramienta escrita en PHP con la intención de manejar la administración de MySQL a través de páginas Web, utilizando Internet. Actualmente puede crear y eliminar Bases de Datos, crear, eliminar y alterar tablas, borrar, editar y añadir campos, ejecutar cualquier sentencia SQL, administrar claves en campos, administrar privilegios, exportar datos en varios formatos y está disponible en 50 idiomas. Se encuentra disponible bajo la licencia GPL

2.8.3.1.2 MySQL Administrator [44]

MySQL Administrador es el nuevo software de administración de servidores de Bases de Datos de MySQL que ha creado MySQL AB. Se trata de un software multiplataforma, que por el momento se encuentra disponible para Linux y Microsoft Windows y que cuenta con un entorno gráfico de usuario muy intuitivo. MySQL Administrador es una herramienta que permite realizar tareas administrativas sobre servidores de MySQL incluyendo:

- Configuración de las opciones de inicio de los servidores
- Inicio y detención de servidores
- Monitoreo de conexiones al servidor
- Administración de usuarios
- Monitoreo del estado del servidor, incluyendo estadísticas de uso
- Visualización de los logs de servidor
- Gestión de copias de seguridad y recuperaciones
- Visualización de catálogos de datos.

2.9 MECANISMOS DE SEGURIDAD EN REDES

2.9.1 RED PRIVADA VIRTUAL (VPN) [45]

Las redes de área local (LAN) son las redes internas de las organizaciones, es

---

44 http://www.desarrolloweb.com/articulos/1798.php

45 http://es.kioskea.net/initiation/vpn.php3

decir las conexiones entre los equipos de una organización particular. Estas redes se conectan cada vez con más frecuencia a Internet mediante un equipo de interconexión. Muchas veces, las empresas necesitan comunicarse por Internet con filiales, clientes o incluso con el personal que puede estar alejado geográficamente.

2.9.1.1 Características

- Seguridad.- verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados.
- Confiabilidad.- en vista que los datos viajan a través de Internet, es necesario protegerlos para que no puedan ser comprendidos por personas no autorizadas.
- Escalabilidad.- se debe asegurar que pueda crecer la red para múltiples conexiones VPN cliente.
- Administración.- debe ser fácil de administrar
- Desempeño.- la VPN debe dar el rendimiento que requiere cada aplicación y tipo de servicio.

2.9.1.2 Elementos de una VPN

- Servidor VPN.- ordenador que acepta conexiones VPN de clientes VPN.
- Cliente VPN.- ordenador que inicia conexiones VPN a un servidor VPN. Puede ser enrutador o un ordenador individual.
- Túnel.- aquella porción de la conexión en que los datos están encapsulados.
- Protocolos de entubación (tunneling protocols) estándares de comunicación utilizados para gestionar el túnel y encapsular los datos privados.
- Red de tránsito.- es la red pública o compartida a través de la que circulan los datos.

Figura 2.14.- Elementos de una VPN [46]

2.9.1.3 Requerimientos Básicos [47]

- **Identificación de usuario:** Las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.
- **Codificación de datos:** Los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos. Esta tarea se realiza con algoritmos de cifrado como DES o 3DES que sólo pueden ser leídos por el emisor y receptor.
- **Administración de claves:** Las VPN deben actualizar las claves de cifrado para los usuarios.

2.9.1.4 Funcionamiento de una VPN [48]

Una red privada virtual se basa en un protocolo denominado protocolo de túnel, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro.

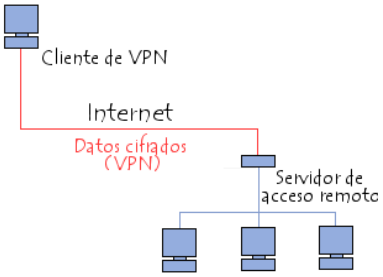


Figura 2.15.- Funcionamiento de una VPN [49]

---

46 http://www.novadevices.com/images1/vpn.pdf

47 http://es.wikipedia.org/wiki/Red_privada_virtual

48 http://es.kioskea.net/initiation/vpn.php3

49 http://es.kioskea.net/initiation/vpn.php3

La palabra "túnel" se usa para simbolizar el hecho que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella y, por lo tanto, son incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN, como si los datos viajaran a través de un túnel. En una VPN de dos equipos, el cliente de VPN es la parte que cifra y descifra los datos del lado del usuario y el servidor VPN (comúnmente llamado servidor de acceso remoto) es el elemento que descifra los datos del lado de la organización.

De esta manera, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite sin cifrar al sistema de pasarela, que se conecta con la red remota mediante la infraestructura de red pública como intermediaria; luego transmite la solicitud de manera cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y éste envía la respuesta cifrada. Cuando el cliente de VPN del usuario recibe los datos, los descifra y finalmente los envía al usuario.

2.9.1.5 Tipos de VPN

Existen tres arquitecturas de conexión VPN:

2.9.1.5.1 VPN de acceso remoto

Es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hotel, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura «dial-up» (módems y líneas telefónicas).

2.9.1.5.2 VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar el costoso vínculo punto a punto tradicional,

sobre todo en las comunicaciones internacionales. Es más común el punto anterior, también llamada tecnología de túnel o tunneling.

2.9.1.5.3 Tunneling

Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (Secure SHell), a través de las cuales se realizan las transferencias inseguras, que pasarán de este modo a ser seguras. De esta analogía viene el nombre de la técnica, siendo la conexión segura (en este caso de ssh) el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar.

2.9.1.6 Protocolos de túnel

2.9.1.6.1 Protocolo PPTP (Protocolo de túnel punto a punto)

El principio del PPTP consiste en crear tramas con el protocolo PPP y encapsularlas mediante un datagrama de IP.
Por lo tanto, con este tipo de conexión, los equipos remotos en dos redes de área local se conectan con una conexión de igual a igual (con un sistema de autenticación/cifrado) y el paquete se envía dentro de un datagrama de IP.

Figura 2.16.- Datagrama IP [50]

De esta manera, los datos de la red de área local (así como las direcciones de los equipos que se encuentran en el encabezado del mensaje) se encapsulan dentro de un mensaje PPP, que a su vez está encapsulado dentro de un mensaje IP.

---

50 http://es.kioskea.net/initiation/vpn.php3

2.9.1.6.2 Protocolo L2F (Reenvío de capa dos) [51]

Protocolo desarrollado por Cisco, a diferencia del PPTP el protocolo L2F no depende de IP con lo cual es capaz de trabajar directamente bajo otros protocolos.

Utiliza PPP para la autenticación de usuarios remotos. Los túneles que crea pueden soportar más de una conexión.

Trabaja con un servicio de enlace llamado Virtual Dial-Up (VDU), que nos permite acceder a la utilización de toda la infraestructura de Internet, no solo para conectar a través de diferentes protocolos al IP sino también cuando las direcciones IP no son reconocidas.

El protocolo L2F es capaz de encapsular payloads PPP o payloads SLIP que serán enviados a sus destinos.

2.9.1.6.3 Protocolo L2TP (Protocolo de túnel de capa dos)

L2TP es un protocolo de túnel estándar (estandarizado en una RFC, solicitud de comentarios) muy similar al PPTP. L2TP encapsula tramas PPP, que a su vez encapsulan otros protocolos (como IP, IPX o NetBIOS).

2.9.1.6.4 Protocolo IPSec

IPSec es un protocolo definido por el IETF que se usa para transferir datos de manera segura en la capa de red. En realidad es un protocolo que mejora la seguridad del protocolo IP para garantizar la privacidad, integridad y autenticación de los datos enviados.

IPSec se basa en tres módulos:

- Encabezado de autenticación IP (AH), que incluye integridad, autenticación y protección contra ataques de REPLAY a los paquetes.
- Carga útil de seguridad encapsulada (ESP), que define el cifrado del paquete. ESP brinda privacidad, integridad, autenticación y protección contra ataques de REPLAY.

---

51 http://www.textoscientificos.com/redes/redes-virtuales/tuneles/l2f

- Asociación de seguridad (SA) que define configuraciones de seguridad e intercambio clave. Las SA incluyen toda la información acerca de cómo procesar paquetes IP (los protocolos AH y/o ESP, el modo de transporte o túnel, los algoritmos de seguridad utilizados por los protocolos, las claves utilizadas, etc.). El intercambio clave se realiza manualmente o con el protocolo de intercambio IKE (en la mayoría de los casos), lo que permite que ambas partes se escuchen entre sí.

2.9.1.6.4.1 Protocolo de intercambio de claves de Internet (IKE) [52]

Después de cada negociación satisfactoria, los servidores VPN regeneran las claves que protegen la conexión, de forma que resulte más difícil para un agresor capturar información de la conexión. Adicionalmente, si utiliza el secreto progresivo perfecto, los agresores no podrán deducir las futuras claves en base a información de claves anterior.

2.9.2 ZONA DESMILITARIZADA (DMZ) [53]

Una zona desmilitarizada (DMZ, demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

---

52 http://as400bks.rochester.ibm.com/html/as400/v5r1/ic2931/index.htm?info/rzaja/rzajasecassociations.htm

53 http://es.wikipedia.org/wiki/DMZ

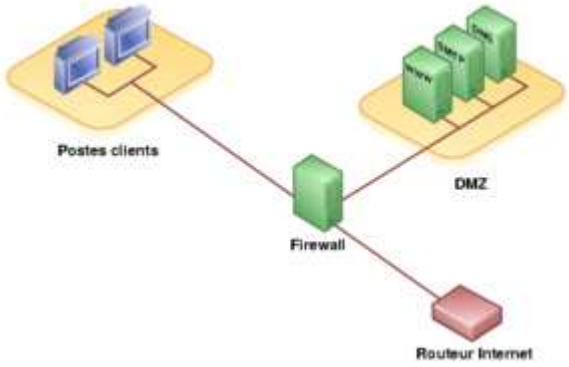


Figura 2.17.- Zona Desmilitarizada 54

2.9.2.1 Arquitectura para una DMZ [55]

Cuando algunas máquinas de la red interna deben ser accesibles desde una red externa (servidores web, servidores de correo electrónico, servidores FTP), a veces es necesario crear una nueva interfaz hacia una red separada a la que se pueda acceder tanto desde la red interna como por vía externa sin correr el riesgo de comprometer la seguridad de la compañía. El término "zona desmilitarizada" o DMZ hace referencia a esta zona aislada que posee aplicaciones disponibles para el público. La DMZ actúa como una "zona de búfer" entre la red que necesita protección y la red hostil.

Los servidores en la DMZ se denominan **"anfitriones bastión"** ya que actúan como un puesto de avanzada en la red de la compañía.

Por lo general, la política de seguridad para la DMZ es la siguiente:

- El tráfico de la red externa a la DMZ está **autorizado**
- El tráfico de la red externa a la red interna está **prohibido**
- El tráfico de la red interna a la DMZ está **autorizado**
- El tráfico de la red interna a la red externa está **autorizado**
- El tráfico de la DMZ a la red interna está **prohibido**
- El tráfico de la DMZ a la red externa está **denegado**

De esta manera, la DMZ posee un nivel de seguridad intermedio, el cual no es lo suficientemente alto para almacenar datos imprescindibles de la compañía.

---

54 http://es.wikipedia.org/wiki/DMZ

55 http://es.kioskea.net/contents/protect/dmz-cloisonnement.php3

2.9.2.1.1 Screened Subset [56]

La arquitectura Screened Subnet, también conocida como red perimétrica o De-Militarized Zone (DMZ) es con diferencia la más utilizada e implantada hoy en día, ya que añade un nivel de seguridad en las arquitecturas de cortafuegos situando una subred (DMZ) entre las redes externa e interna, de forma que se consiguen reducir los efectos de un ataque exitoso al host bastión,

En este esquema se utilizan dos Routers: uno exterior y otro interior. El Router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno).

Es posible definir varios niveles de DMZ agregando más Routers, pero destacando que las reglas aplicadas a cada uno deben ser distintas ya que en caso contrario los niveles se simplificarían a uno solo.

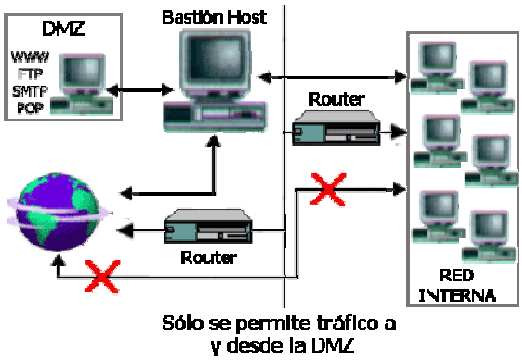


Figura 2.18.- Arquitectura Screened Subset [57]

Como puede apreciarse la Zona Desmilitarizada aísla físicamente los servicios internos, separándolos de los servicios públicos. Además, no existe una conexión directa entre la red interna y la externa.

Los sistemas Dual-Homed Host y Screnned pueden ser complicados de configurar y comprobar, lo que puede dar lugar, paradójicamente, a importantes agujeros de seguridad en toda la red. En cambio, si se encuentran bien

56http://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node239.html

57 http://www.segu-info.com.ar/firewall/screenedsubnet.htm

configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas:

Ocultamiento de la información: los sistemas externos no deben conocer el nombre de los sistemas internos. El Gateway de aplicaciones es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitada o sospechosa.

Registro de actividades y autenticación robusta: El Gateway requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.

Reglas de filtrado menos complejas: Las reglas del filtrado de los paquetes por parte del Router serán menos compleja dado a que él sólo debe atender las solicitudes del Gateway.

Así mismo tiene la desventaja de ser intrusos y no transparentes para el usuario ya que generalmente este debe instalar algún tipo de aplicación especializada para lograr la comunicación.

2.9.3 FIREWALL [58]

Un cortafuegos (o firewall en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

58 http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica

2.9.3.1 Tipos de cortafuegos

2.9.3.1.1 Cortafuegos de capa de red o de filtrado de paquetes [59]

Se utilizan Routers con filtros y reglas basadas en políticas de control de acceso. El Router es el encargado de filtrar los paquetes (un Choke) basados en cualquiera de los siguientes criterios:

Protocolos utilizados.

- Dirección IP de origen y de destino.
- Puerto TCP-UDP de origen y de destino.

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico. Restringiendo las comunicaciones entre dos computadoras (mediante las direcciones IP) se permite determinar entre cuales máquinas la comunicación está permitida.

El filtrado de paquetes mediante puertos y protocolos permite establecer qué servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la WWW (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).

Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de Firewalls trabajan en los niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red.

Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo presenta debilidades como:

- No protege las capas superiores a nivel OSI.
- Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
- No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.
- Sus capacidades de auditoria suelen ser limitadas, al igual que su capacidad de registro de actividades.

---

59 http://www.segu-info.com.ar/firewall/filtradopaquetes.htm

- No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

2.9.3.1.2 Proxy Gateways de Aplicaciones [60]

Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host.

El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real y devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma.

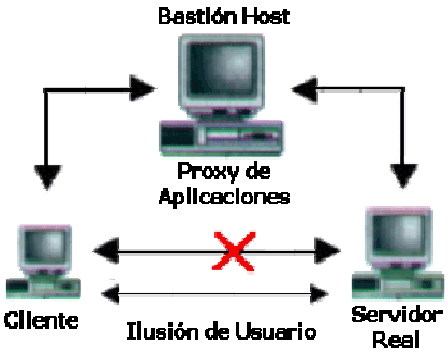


Figura 2.19.- Proxy de aplicaciones [61]

2.9.3.1.3 Dual Comed Host

Son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del Filtrado de Paquetes), por lo que se dice que actúan con el "IP-Forwarding desactivado".

Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectará al servicio exterior

60 http://www.segu-info.com.ar/firewall/proxygateways.htm

61 http://www.segu-info.com.ar/firewall/proxygateways.htm

solicitado y hará de puente entre este y el usuario interior.

Es decir que se utilizan dos conexiones. Uno desde la máquina interior hasta el Firewall y el otro desde este hasta la máquina que albergue el servicio exterior

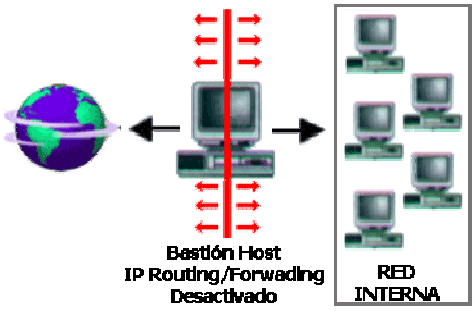


Figura 2.20.- Dual Comed Host [62]

2.9.3.1.4 Screened Subset

En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida. Como se manifestó en la arquitectura de una zona desmilitarizada.

2.9.3.1.5 Inspección de Paquetes [63]

Este tipo de Firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas

2.9.3.1.6 Firewalls personales

Estos Firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada

62 http://www.segu-info.com.ar/firewall/dualhomed.htm

63 http://www.segu-info.com.ar/firewall/firewall.htm

2.9.3.2 Tipos de Cortafuegos según su implementación

Según la implementación los firewall se pueden clasificar en:

- Por hardware
- Por software

2.9.3.2.1 Firewall por hardware [64]

Como hardware, el firewall es un dispositivo externo que se ubica entre la computadora o la red y el Internet. Algunos dispositivos son llamados "routers" o ruteadores que tienen características de firewall. El firewall basado en hardware es particularmente útil para proteger una red de computadoras, aunque esto no quiere decir que para una sola computadora no sea útil, ya que por el contrario le proporciona un alto nivel de protección aunque puede ser muy costoso.

2.9.3.2.1.1 Principales fabricantes de Firewalls

Fortinet.- [65] Es una empresa privada estadounidense, que se dedica especialmente al diseño y fabricación de componentes y dispositivos de seguridad de redes (firewalls, UTM.)

Actualmente es la marca de referencia en sistemas de seguridad UTM, habiendo superado a Cisco y Checkpoint en su lucha por este mercado.

Las aplicaciones de FortiGate proporcionan protección rentable, comprensiva contra amenazas de red - incluyendo los ataques complejos sin degradar el rendimiento de la red.

Las plataformas de FortiGate incorporan características sofisticadas de red, tales como alta disponibilidad (activa/activa, activa/voz pasiva) para la máxima disponibilidad, capacidades virtuales de dominio para separar las varias redes que requieren diversas políticas de la seguridad.

Cisco.- [66] Cisco Systems es el líder mundial en redes para Internet. Las soluciones de conectividad de Cisco basadas en el protocolo de Internet (IP), son

---

64 http://www.auditoria.com.mx/noticias/boletin/2004/0402_p.htm

65 http://www.conectapymes.com/ficha.aspx?Id=40&mn=smenu5

66 http://www.elyteonline.com/Marcas_y_Fabricantes/index.html

la base de Internet y de las redes corporativas, educativas y de gobierno en todo el mundo. Cisco entrega la línea más amplia de soluciones para el transporte de datos, voz y video. Aquí encontrará toda la información técnica y de negocios sobre redes e Internet.

3Com.- Desde la fundación de 3Com en 1979 y la creación del estándar Ethernet, el mundo ha adoptado su visión de un networking dominante.3Com está focalizada en ofrecer productos y soluciones innovadoras con amplias funcionalidades que destaquen junto a un bajo coste de adquisición y propiedad.

D-Link.- Es uno de los líderes mundiales en proveer equipamiento de networking, conectividad y de comunicaciones de datos. La compañía diseña, fabrica y comercializa hardware necesario para permitir a los usuarios compartir recursos y comunicarse sobre una red de área local, y equipos que permiten a los individuos y oficinas conectarse a WANs y a Internet fáciles, rápidos y con una buena relación calidad-precio.

Proporciona equipos de seguridad tales como router y firewall de fácil instalación y más efectivos que aquellos basados en software, dada su conexión Plug-and-Play, seguridad completa para dejar fuera de la red a los intrusos, soporte de VPN con encriptación de datos y autentificación.

A través de su línea de Firewalls NetDefend la mejor plataforma de seguridad proactiva, en conjunto con su familia de switches X-Stack.

Sonicwall.- (Fundada en 1991), es uno de los mas prestigiosos fabricantes de sistemas de seguridad (Firewall, VPN, Aceleradores SSL, etc) ofrece una calidad excepcional a unos precios ventajosos, con una gama de productos que cubren desde las Pymes a grandes empresas y proveedores de servicios, sus soluciones son utilizadas por una gran variedad de compañías, a nivel mundial.

Checkpoint.- Checkpoint Software Technologies LTD, creada en el año 1993, está especializada única y exclusivamente en soluciones de seguridad lógica, cubriendo desde usuarios finales hasta proveedores de servicios de Internet (ISP/ASP).

Las soluciones de seguridad de Checkpoint destacan por su arquitectura

unificada, lo que, por ejemplo, permite gestionar multitud de sus productos de seguridad perimetral o seguridad interna, desde un único punto de forma centralizada.

2.9.3.2.1.2 Alternativas de solución de firewalls en el mercado

2.9.3.2.1.2.1 D-Link DFL-800

El firewall VPN DFL-800 ofrece una protección de red completa así como servicios de red privada virtual, a las pequeñas empresas de hasta 150 usuarios, mediante robustas funciones de seguridad, una configuración flexible y la máxima protección de red.

Alojado en un chasis normalizado, el firewall VPN DFL-800 ofrece un impresionante conjunto de funciones de hardware que incluyen un procesador de alta velocidad, una base de datos de gran capacidad y un potente firewall que puede gestionar hasta 25.000 sesiones simultáneas.

Interfaces:

- 2 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (WAN)
- 7 x red - Ethernet 10Base-T/100Base-TX - RJ-45
- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (DMZ)
- 1 x gestión - RS-232

CARACTERISTICAS		DESCRIPCIÓN
CONEXIÓN DE REDES	*Factor de forma:* *Tecnología de conectividad:* *Protocolo de interconexión de datos:* *Características de protección* *Protección firewall,* *Encaminamiento,* *Asistencia técnica VPN,* *Limitación de tráfico*	***Externo*** ***Cableado*** ***Ethernet, Fast Ethernet***

Tabla 2.1.- Características técnicas D-Link DFL-800 [67]

67 http://www.acuista.com/x/15134-d_link_dfl_800/#ficha_tecnica

2.9.3.2.1.2.2 D-Link NetDefend DFL-860

El DFL-860 usa un acelerador por hardware para llevar a cabo las funciones de escaneado antivirus e IPS simultáneamente, sin que se degrade el rendimiento del firewall ni de la red privada virtual. Este potente acelerador le permite al firewall trabajar con un rendimiento muy superior al de los firewall UTM con función antivirus del mercado. Potente rendimiento de la red privada virtual El DFL-860 dispone de un motor de red privada virtual basado en hardware para soportar y gestionar hasta 300 túneles VPN. Admite los protocolos IPSec, PPTP y L2TP en modo cliente/servidor y también puede manejar el tráfico que pasa a través de él. La autentificación de usuario puede llevarse a cabo por medio de un servidor RADIUS externo o a través de la base de datos interna del firewall, que admite hasta 500 cuentas.

El firewall UTM DFL-860 ofrece una potente solución de seguridad para las oficinas de pequeño o medio tamaño, con hasta 150 usuarios, contra una amplia variedad de amenazas para la red en tiempo real.

Interfaces:

- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (DMZ)
- 2 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (WAN)
- 7 x red - Ethernet 10Base-T/100Base-TX - RJ-45

CARACTERÍSTICAS		DESCRIPCIÓN
CONEXIÓN DE REDES	*Factor de forma:*	***Externo***
	Tecnología de conectividad:	***Cableado***
	Protocolo de interconexión de datos:	***Ethernet, Fast Ethernet***
	Red / Protocolo de transporte:	***PPTP, L2TP, IPSec***
	Protocolo de direccionamiento	***OSPF***
	Rendimiento	
	Capacidad de cortafuegos	***150 Mbps***
	Capacidad de VPN (3DES,AES)	***60 Mbps***
	Capacidad:	
	Sesiones concurrentes:	***25000***
	Políticas de seguridad:	***1000***
	Túneles VPN (de sitio a sitio) :	***300***

	Características de protección *Protección firewall, Puerto DMZ* *Soporte de DHCP, Soporte de NAT* *Asistencia técnica VPN, Soporte para PAT* *Equilibrio de carga* *Soporte VLAN, Limitación de tráfico,* *Stateful Packet Inspection (SPI),* *Prevención contra ataque de DoS (denegación de servicio)* *Filtrado de contenido, Soporte ALG,* *Intrusion Detection System (IDS),* *Alerta de correo electrónico,* *Análisis de antivirus* *Alta disponibilidad,* *Sistema de prevención de intrusiones (IPS), filtrado de URL,* *IPSec NAT-Traversal (NAT-T)* *Algoritmo de cifrado:* *DES, Triple DES, Blowfish, Twofish, CAST, AES, IKE* *Método de autentificación:* *RADIUS*	

Tabla 2.2.- Características técnicas D-Link DFL-860 [68]

2.9.3.2.1.2.3 FortiGate-60 [69]

Proporciona todas las mismas funcionalidades que otros dispositivos FortiGate y está diseñado para trabajadores de casa y pequeñas oficinas remotas.

Conector dual WAN para una conexión de Internet redundante, 4 puertos switch elimina la necesidad de un switch o hub externo, dando a los dispositivos de red una conexión directa al FortiGate-60.

Entrega rendimiento superior y fiabilidad del hardware acelerado, arquitectura basada en ASIC.

68 http://www.acuista.com/x/74575-d_link_netdefend_dfl_860/

69 http://www.sc-telecom.com/productos2.asp?id=44

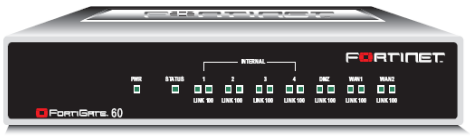


Figura 2.21.- FortiGate 60 [70]

Interfaces:

- 2 Conexiones WAN
- 4 Puertos Switch
- 1 Puerto DMZ

CARACTERÍSTICA	DESCRIPCIÓN	BENEFICIOS
ANTIVIRUS (CERTIFICADO ICSA)	*Detecta y elimina virus, gusanos en tiempo real. Escanea datos adjuntos de correos electrónicos de entrada y salida (SMTP, POP3, IMAP), también todo el tráfico FTP y HTTP*	*Cerrando estas vulnerabilidades no entran virus ni gusanos a la red local*
PREVENCIÓN Y DETECCIÓN DE INTRUSIÓN DINÁMICAS (CERTIFICADO ICSA)	*Detección y prevención de más de 1300 intrusiones y ataques basada en configuraciones de usuarios. Actualizaciones automáticas de IPS desde el FortiProyect Network*	*Detecta ataques que evaden los antivirus convencionales, en tiempo real*
FIREWALL (CERTIFICADO ICSA)	*Controla todas las comunicaciones que pasa de una red a la otra y en función de lo que se permite o se deniegue en la política*	*Protección certificada, máximo funcionamiento y escalabilidad*
FILTRADO DE CONTENIDO WEB	*Bloquea todo contenido Web inapropiado y scripts maliciosos provenientes de la Web*	*Bloqueo de sitios web que no son permitidos por las políticas de la empresa, aumentando la productividad del personal y reduciendo la posibilidad de infección*

70 http://service.pcconnection.com/images/inhouse/bf5fe86c-44c8-43d5-b252-9a7b502a31e7.jpg

		de virus.
VPN (CERTIFICADO ICSA)	*Soporta túneles IPSec,PPTP y L2TP*	*Provee comunicación segura en el túnel entre redes y clientes*
ACCESOS REMOTOS	*Soporta accesos remotos desde cualquier PC equipadas con el software* ***FORTICLIENT HOST SECURITY***	*Bajo costo, en cualquier momento y todas partes tendrán acceso sus trabajadores móviles y remotos*
INTERFACES WAN	*Proporcionan conexiones a Internet*	*Con dos interfaces WAN proporcionan redundancia a Internet si una interface falla, la otra Automáticamente toma todas las sesiones*

Tabla 2.3.- Características técnicas FortiGate 60 [71]

2.9.3.2.1.2.3.1 FortiClient PC [72]

Entrega característica de agente de seguridad para computadores personales (PC), incluyendo Firewall Personal, VPN IPSec, antivirus, antispyware, antispam y filtro de contenido Web. El agente de protección FortiClient es entregado por los servicios de suscripción de FortiGuard para asegurar dispositivos y proteger contra las amenazas de hoy en día Los agentes livianos de software unificado FortiClient está disponible para sistemas operativos Microsoft Windows

Características Clave:

- VPN IPsec segura.- Entrega el poder a los equipos de escritorio, y cualquier dispositivo basado en Windows, con la capacidad de acceder de manera segura a las aplicaciones empresariales con encriptación DES / 3DES.
- Antivirus y Antispyware.- Entrega una protección completa en contra de virus, spyware, keyloggers, troyanos, adware y greyware para sistemas

71 http://www.sc-telecom.com/productos2.asp?id=44

72 http://www.solint.cl/forticlient_fortinet.html

Windows.

- Poderoso Firewall Personal.- Monitorea tráfico de red y aplica un apropiado control de acceso a las aplicaciones basados en Windows.
- Antispam Avanzado.- Antispam Incorporado que se integra con MS Outlook.
- Filtro de Contenido Web.- Entrega protección contra acceso a contenidos en tiempo real para asegurar cumplimiento de políticas corporativas.

2.9.3.2.1.2.4 FortiGate-60B

Es una solución ideal para oficinas pequeñas (10 a 25 usuarios). El FortiGate-60 tiene 2 puertos WAN para conexiones redundantes a internet, y un switch 10/100 integrado de 4 puertos que eliminan la necesidad de un switch externo, dando conexión directa a dispositivos de red. Además cuenta con un puerto DMZ.

Interfaces:

- 2 Conexiones WAN
- 4 Puertos Switch
- 1 Puerto DMZ

CARACTERÍSTICA	DESCRIPCIÓN	BENEFICIOS
ANTIVIRUS (CERTIFICADO ICSA)	*Detecta y elimina virus, gusanos en tiempo real.* *Escanea datos adjuntos de correos electrónicos de entrada y salida (SMTP, POP3, IMAP), también todo el tráfico FTP y HTTP*	*Cerrando estas vulnerabilidades no entran virus ni gusanos a la red local*
PREVENCIÓN Y DETECCIÓN DE INTRUSIÓN DINÁMICAS (CERTIFICADO ICSA)	*Detección y prevención de más de 1300 intrusiones y ataques basada en configuraciones de usuarios.* *Actualizaciones automáticas de IPS desde el FortiProyect Network*	*Detecta ataques que evaden los antivirus convencionales, en tiempo real*
FIREWALL (CERTIFICADO ICSA)	*Controla todas las comunicaciones que pasa de una red a la otra y en función de lo que se permite o se deniegue en la política*	*Protección certificada, máximo funcionamiento y escalabilidad*

FILTRADO DE CONTENIDO WEB	*Bloquea todo contenido Web inapropiado y scripts maliciosos provenientes de la Web*	*Bloqueo de sitios Web que no son permitidos por las políticas de la empresa, aumentando la productividad del personal y reduciendo la posibilidad de infección, de virus que dañan los equipos de computo*
VPN (CERTIFICADO ICSA)	*Soporta túneles IPSec,PPTP y L2TP*	*Provee comunicación segura en el túnel entre redes y clientes*
ACCESOS REMOTOS	*Soporta accesos remotos desde cualquier PC equipadas con el software FortiClient Host Security*	*Bajo costo, en cualquier momento y todas partes tendrán acceso sus trabajadores móviles y remotos*
INTERFACES DUALES WAN	*Las Interfaces duales WAN proporcionan la ayuda para dos conexiones separadas al Internet*	*Con dos interfaces WAN proporcionan redundancia a Internet si una interface falla, la otra Automáticamente toma todas las sesiones*
PUERTOS DE EXPANSIÓN USB	*Los puertos del USB pueden apoyar los realces futuros incluyendo los módems de marcado manual o de banda ancha*	*Expansibilidad, protección de inversión*
INTERRUPTOR INCORPORADO 4 PUERTOS	*Interruptor integrado con cuatro puertos de 10/100 Ethernet para los dispositivos directamente de conexión de la red*	*Elimina la necesidad de un interruptor externo o de un eje*

Tabla 2.4.- Características técnicas FortiGate 60B [73]

2.9.3.2.1.2.5 SonicWALL TZ 180

SonicWALL TZ 180 es ideal para empresas pequeñas, oficinas remotas, sucursales y para el comercio minorista.

73 http://www.net.com.mx/PDF/Fortinet/FGT60DS2.pdf

Interfaces:

- 5 x red - Ethernet 10Base-T/100Base-TX - RJ-45
- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (WAN)
- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (LAN / DMZ WAN)
- 1 x gestión - consola

CARACTERÍSTICAS		DESCRIPCIÓN
CONEXIÓN DE REDES	*Factor de forma:* *Tecnología de conectividad:* *Protocolo de interconexión de datos:* *Protocolo de conmutación:* *Red / Protocolo de transporte:* *Protocolo de gestión remota* *<u>Rendimiento:</u>* *Capacidad de pleno estado* *Rendimiento 3DES y AES :* *<u>Capacidad:</u>* *Conexiones concurrentes:* *Indicadores de estado:* *<u>Características de protección:</u>* *Señal ascendente automática (MDI/MDI-X automático)* *Soporte de DHCP, Soporte de NAT,* *Prevención contra ataque de DoS (denegación de servicio),* *Servidor DNS dinámico* *Prevención de ataque DDos* *<u>Algoritmo de cifrado:</u>* *DES, Triple DES, MD5, IKE, SHA-1, AES de 128 bits, AES de 192 bits, AES de 256 bits* *<u>Método de autentificación:</u>*	***Externo*** ***Cableado*** ***Ethernet, Fast Ethernet*** ***Ethernet*** ***L2TP, IPSec*** ***SNMP 2, HTTP, HTTPS*** ***90 Mbps*** ***30+ Mbps*** ***6000*** ***Actividad de enlace, alimentación, modo de prueba, dispositivo conectado a 100M***

	RADIUS, certificados X.509, LDAP, Active Directory	

Tabla 2.5.- Características técnicas Sonic WALL TZ 180 [74]

2.9.3.2.1.2.6 SonicWALL TZ 190

Es un dispositivo de seguridad de red multicapa que puede utilizarse como acceso principal a Internet o como sistema de reserva cuando la conexión DSL (u otra conexión por cable) no funciona

Interfaces:

- 8 x red - Ethernet 10Base-T/100Base-TX - RJ-45
- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (WAN)
- 1 x gestión - consola
- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (LAN / DMZ WAN)

CARACTERÍSTICAS		**DESCRIPCIÓN**
PROCESADOR / MEMORIA / ALMACENAMIENTO	*RAM instalada (máx.)* *Memoria flash instalado (máx.):*	***128 MB*** ***16 MB Flash***
	Factor de forma: *Tecnología de conectividad:* *Protocolo de interconexión de datos:* *Protocolo de conmutación:* *Red / Protocolo de transporte:* *Modo comunicación:* *<u>Rendimiento:</u>* *Capacidad de pleno estado :* *Capacidad de antivirus de pasarela:*	***Externo*** ***Cableado*** ***Ethernet, Fast Ethernet*** ***Ethernet*** ***L2TP, IPSec*** ***Semidúplex, dúplex pleno*** ***90+ Mbps*** ***10 Mbps***

74 http://www.acuista.com/x/176558-sonicwall_tz_180_01_ssc_6557/

CONEXIÓN DE REDES	*Rendimiento 3DES y AES :*	***30+ Mbps***
	Capacidad de prevención (intrusiones)	***8 Mbps***
	Capacidad:	
	Conexiones concurrentes:	***6000***
	Políticas de seguridad:	***250***
	VPN tunnels (remote access) :	***2***
	Nodos:	***Ilimitado***
	Zonas de seguridad:	***8***
	Túneles VPN (de sitio a sitio) :	***15***
	Características de protección:	
	Protección firewall, Conmutación	
	Criptografía 128 bits	
	Soporte de DHCP, Soporte de NAT	
	Asistencia técnica VPN	
	Prevención contra ataque de DoS (denegación de servicio)	
	Filtrado de contenido, Filtrado de URL	
	Inspección profunda, Cifrado de 256 bits	
	Algoritmo de cifrado:	
	DES, Triple DES, MD5, AES, IKE, SHA-1	
	Método de autentificación:	
	RADIUS, certificados X.509	

Tabla 2.6.- Características técnicas Sonic WALL TZ 190 [75]

2.9.3.2.1.2.7 D-Link DFL-1600

El firewall VPN DFL-1600 ofrece una protección de red completa así como servicios de red privada virtual, o VPN (Virtual Private Network), a las grandes empresas. Mediante robustas funciones de seguridad, una configuración flexible y la máxima protección de red, ofrece un considerable retorno de la inversión para las empresas que exigen un alto rendimiento a precios competitivos.

Interfaces:

- 6 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45
- 1 x gestión - RS-232 - D-Sub de 9 espigas (DB-9)

75 http://www.acuista.com/x/83681-sonicwall_tz_190_with_3g_wirel_01_ssc_6850/#ficha_tecnica

CARACTERÍSTICAS		DESCRIPCIÓN
CONEXIÓN DE REDES	*Factor de forma:* *Tecnología de conectividad:* *Protocolo de interconexión de datos:* *Indicadores de estado:* *Características de protección:* *Protección firewall,* *Encaminamiento, Soporte de NAT* *Asistencia técnica VPN, Limitación de tráfico*	***Externo*** ***Cableado*** ***Ethernet, Fast Ethernet, Gigabit Ethernet*** ***Pantalla de cristal líquido***

Tabla 2.7.- Características técnicas D-Link DFL-1600 [76]

2.9.3.2.1.2.8 FortiGate-100A

El sistema FortiGate-100A es una solución ideal para oficinas pequeñas, medianas. FortiGate-100A tiene dos puertos WAN que soportan conexiones de Internet redundantes y cuenta con 4 puertos switch que elimina la necesidad de un switch o hub externo, dando a los dispositivos de red una conexión directa al FortiGate-100A

- Los puertos dual DMZ proporcionan una segmentación de red adicional para servidores Web de correo.
- Los puertos dual WAN soportan conectores redundantes, balanceados para ISPs múltiples.

Interfaces:

- 2 Conexiones WAN
- 4 Puertos Switch
- 2 Puerto DMZ

76 http://www.acuista.com/x/15130-d_link_dfl_1600/#ficha_tecnica

CARACTERÍSTICA	DESCRIPCIÓN	BENEFICIOS
ANTIVIRUS (CERTIFICADO ICSA)	*Detecta y elimina virus, gusanos en tiempo real. Escanea datos adjuntos de correos electrónicos de entrada y salida (SMTP, POP3, IMAP), también todo el tráfico FTP y HTTP*	*Cerrando estas vulnerabilidades no entran virus ni gusanos a la red local*
PREVENCIÓN Y DETECCIÓN DE INTRUSIÓN DINÁMICAS (CERTIFICADO ICSA)	*Detección y prevención de más de 1300 intrusiones y ataques basada en configuraciones de usuarios. Actualizaciones automáticas de IPS desde el FortiProyect Network*	*Detecta ataques que evaden los antivirus convencionales, en tiempo real*
FIREWALL (CERTIFICADO ICSA)	*Controla todas las comunicaciones que pasa de una red a la otra y en función de lo que se permite o se deniegue en la política*	*Protección certificada, máximo funcionamiento y escalabilidad*
FILTRADO DE CONTENIDO WEB	*Bloquea todo contenido Web inapropiado y scrips maliciosos provenientes de la Web*	*Bloqueo de sitios Web que no son permitidos por las políticas de la empresa, aumentando la productividad del personal y reduciendo la posibilidad de infección, de virus que dañan los equipos de computo*
VPN (CERTIFICADO ICSA)	*Soporta túneles IPSec, PPTP y L2TP*	*Provee comunicación segura en el túnel entre redes y clientes*
ACCESOS REMOTOS	*Soporta accesos remotos desde cualquier PC equipadas con el software FortiClient Host Security*	*Bajo costo, en cualquier momento y todas partes tendrán acceso sus trabajadores móviles y remotos*
INTERFACES WAN	*Proporcionan conexiones a Internet*	*Con dos interfaces WAN proporcionan redundancia a Internet si una interface falla, la otra Automáticamente*

		toma todas las sesiones
PUERTOS DE EXPANSIÓN USB	*Los puertos del USB pueden apoyar los realces futuros incluyendo los módems de marcado manual o de banda ancha*	*Expansibilidad, protección de inversión*
INTERRUPTOR INCORPORADO 4-PUERTOS	*Interruptor integrado con cuatro puertos de 10/100 Ethernet para los dispositivos directamente de conexión de la red*	*Elimina la necesidad de un interruptor externo o de un eje*

Tabla 2.8.- Características técnicas FortiGate-100A [77]

2.9.3.2.1.2.9 FortiGate-200A

El Firewall Antivirus FortiGate-200A es una solución ideal para organizaciones pequeñas y de tamaño medio que requieran servicios de seguridad de la red en tiempo real. La plataforma FortiGate-200A destaca el soporte de conexiones dual WAN para conexiones de Internet redundantes y 4 puertos switch integrados que elimina la necesidad de un hub y switch externo, proporcionando a los dispositivos de red una conexión directa a la unidad del FortiGate-200A.

CARACTERÍSTICA	DESCRIPCIÓN	BENEFICIOS
ANTIVIRUS (CERTIFICADO ICSA)	*Detecta y elimina virus, gusanos en tiempo real.* *Escanea datos adjuntos de correos electrónicos de entrada y salida (SMTP, POP3, IMAP), también todo el tráfico FTP y HTTP*	*Cerrando estas vulnerabilidades no entran virus ni gusanos a la red local*
PREVENCIÓN Y DETECCIÓN DE INTRUSIÓN DINÁMICAS (CERTIFICADO ICSA)	*Detección y prevención de más de 1300 intrusiones y ataques basada en configuraciones de usuarios. Actualizaciones automáticas de IPS desde el FortiProyect Network*	*Detecta ataques que evaden los antivirus convencionales, en tiempo real*
FIREWALL (CERTIFICADO ICSA)	*Controla todas las comunicaciones que pasa de una red a la otra y en función de lo que se permite*	*Protección certificada, máximo funcionamiento y escalabilidad*

77 http://www.sc-telecom.com/productos2.asp?id=47

	o se deniegue en la política	
FILTRADO DE CONTENIDO WEB	*Bloquea todo contenido Web inapropiado y scrips maliciosos provenientes de la Web*	*Bloqueo de sitios Web que no son permitidos por las políticas de la empresa, aumentando la productividad del personal y reduciendo la posibilidad de infección, de virus que dañan los equipos de computo*
VPN (CERTIFICADO ICSA)	*Soporta túneles IPSec,PPTP y L2TP*	*Provee comunicación segura en el túnel entre redes y clientes*
ACCESOS REMOTOS	*Soporta accesos remotos desde cualquier PC equipadas con el software FortiClient Host Security*	*Bajo costo, en cualquier momento y todas partes tendrán acceso sus trabajadores móviles y remotos*
INTERFACES WAN	*Proporcionan conexiones a Internet*	*Con dos interfaces WAN proporcionan redundancia a Internet si una interface falla, la otra Automáticamente toma todas las sesiones*

Tabla 2.9.- Características técnicas FortiGate-200A [78]

2.9.3.2.1.2.10 SonicWALL PRO 1260

Interfaces:

- 24 x red - Ethernet 10Base-T/100Base-TX - RJ-45
- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (WAN)
- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (DMZ)
- 1 x gestión - consola
- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45

78 http://www.sc-telecom.com/productos2.asp?id=49

CARACTERÍSTICAS		DESCRIPCIÓN
PROCESADOR / MEMORIA / ALMACENAMIENTO	*RAM instalada (máx.)* *Memoria flash instalado (máx.):*	***64MB*** ***8 MB Flash***
CONEXIÓN DE REDES	*Factor de forma:* *Cantidad de puertos* *Tecnología de conectividad:* *Protocolo de interconexión de datos:* *Protocolo de conmutación:* *Red / Protocolo de transporte:* *Protocolo de gestión remota* *Rendimiento:* *Capacidad de pleno estado :* *Capacidad de antivirus de pasarela:* *Rendimiento 3DES y AES :* *Capacidad de prevención (intrusiones)* *Capacidad:* *Conexiones concurrentes:* *Políticas de seguridad:* *VPN tunnels (remote access) :* *Nodos:* *Túneles VPN (de sitio a sitio) :* *Características de protección:* *Enlace ascendente,* *Protección firewall,* *Conmutación Layer 2,* *Soporte de DHCP, Soporte de NAT,* *Asistencia técnica VPN,* *Señal ascendente automática (MDI/MDI-X automático),* *Soporte para Syslog,* *Prevención contra ataque de DoS (denegación de servicio),* *Servidor DNS dinámico, inspección profunda,* *Algoritmo de cifrado:*	***Externo*** ***24*** ***Cableado*** ***Ethernet, Fast Ethernet*** ***Ethernet*** ***TCP/IP, PPTP, UDP/IP, L2TP, ICMP/IP, IPSec, PPPoE*** ***SNMP 2, HTTP, HTTPS*** ***90+ Mbps*** ***8 Mbps*** ***30+ Mbps*** ***8 Mbps*** ***6000*** ***100*** ***5*** ***Ilimitado*** ***25***

	DES, Triple DES, MD5, AES, IKE, SHA-1,FIPS 140-2 *Método de autentificación:* *RADIUS, certificados X.509 base de datos de usuarios internos*	

Tabla 2.10.- Características técnicas Sonic WALL PRO 1260 [79]

2.9.3.2.1.2.11 SonicWALL PRO 3060

Interfaces:

- 1 x gestión - consola - D-Sub de 9 espigas (DB-9)
- 5 x red - Ethernet 10Base-T/100Base-TX - RJ-45
- 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (WAN)

CARACTERÍSTICAS		DESCRIPCIÓN
PROCESADOR / MEMORIA / ALMACENAMIENTO	*RAM instalada (máx.)* *Memoria flash instalado (máx.):*	***256 MB*** ***64 MB Flash***
CONEXIÓN DE	*Factor de forma:* *Tecnología de conectividad:* *Protocolo de interconexión de datos:* *Protocolo de conmutación:* *Red / Protocolo de transporte:* *Protocolo de gestión remota* *Rendimiento:* *Capacidad de pleno estado :* *Capacidad de antivirus de pasarela:* *Rendimiento 3DES y AES :* *Capacidad de prevención (intrusiones)* *Capacidad:* *Conexiones concurrentes:*	***Externo*** ***Cableado*** ***Ethernet, Fast Ethernet*** ***Ethernet*** ***TCP/IP, PPTP, UDP/IP, L2TP, ICMP/IP, IPSec, PPPoE*** ***SNMP 2, HTTP, HTTPS*** ***300 Mbps*** ***99 Mbps*** ***75 Mbps*** ***98 Mbps*** ***128000*** ***300***

79 http://www.acuista.com/x/930-sonicwall_pro_1260_01_ssc_5861/

REDES	*Políticas de seguridad:* *VPN tunnels (remote access) :* *Nodos:* *Túneles VPN (de sitio a sitio) :* *Indicadores de estado:* *Actividad de enlace,* *Alimentación,* *Modo de prueba,* *Despertador* *Características de protección:* *Protección firewall,* *Puerto DMZ,* *Auto-sensor por dispositivo,* *Soporte de DHCP, Soporte de NAT* *Cifrado del hardware* *Asistencia técnica VPN* *Señal ascendente automática (MDI/MDI-X automático),* *Prevención contra ataque de DoS (denegación de servicio)* *Activable, Inspección profunda* *Algoritmo de cifrado:* *DES, Triple DES, AES, IKE,* *Método de autentificación:* *RADIUS, certificados X.509 base de datos de usuarios internos*	***25*** ***Ilimitado*** ***500***

Tabla 2.11.- Características técnicas Sonic WALL PRO 3060 [80]

2.9.3.2.1.2.12 Cisco ASA 5505 Firewall Edition Bundle

El dispositivo de seguridad adaptable de la serie Cisco ASA 5500 es una plataforma que proporciona servicios de seguridad y VPN de próxima generación para entornos que van desde oficinas pequeñas/hogareñas y empresas medianas hasta grandes empresas. Número ilimitado de usuarios. La serie Cisco ASA 5500 permite la estandarización en una sola plataforma para reducir el costo operativo general de la seguridad.

80 http://www.acuista.com/x/851-sonicwall_pro_3060_01_ssc_5366/

Interfaces:

- 6 x red - Ethernet 10Base-T/100Base-TX - RJ-45
- 2 x red / energía - Ethernet 10Base-T/100Base-TX - RJ-45
- 3 x Hi-Speed USB - 4 PIN USB tipo A
- 1 x gestión - consola - RJ-45

CARACTERÍSTICAS		DESCRIPCIÓN
PROCESADOR / MEMORIA / ALMACENAMIENTO	*RAM instalada (máx.)* *Memoria flash instalado (máx.):*	***256 MB*** ***64 MB Flash***
CONEXIÓN DE REDES	*Factor de forma:* *Tecnología de conectividad:* *Protocolo de interconexión de datos:* *Red / Protocolo de transporte:* *Rendimiento:* *Capacidad del cortafuegos :* *Capacidad de la VPN:* *Capacidad:* *Peers VPN IPSec :* *Peers VPN SSL :* *Sesiones concurrentes :* *Características de protección:* *Protección firewall, Puerto DMZ,* *Asistencia técnica VPN, Soporte VLAN,* *Algoritmo de cifrado:* *Triple DES, AES , SSL*	***Externo*** ***Cableado*** ***Ethernet, Fast Ethernet*** ***IPSec*** ***150 Mbps*** ***100 Mbps*** ***10*** ***2*** ***10000***

Tabla 2.12.- Características técnicas Cisco ASA 5505 Firewall Edition Bundle [81]

2.9.3.2.2 Firewall por software

El firewall basado en software es un programa que una vez instalado en la computadora, analiza las peticiones de entrada y/o salida para bloquearlas si el usuario Administrador está de acuerdo con las políticas que se definan, si así lo

81 http://www.acuista.com/x/118470-cisco_asa_5505_firewall_editio_asa5505_50_bun_k9/

decide.

Existe actualmente software firewall personal que, considerando lo que se quiere proteger, es útil en las computadoras de escritorio y portátiles que tienen necesidad de conectarse a Internet o a la red corporativa.

El firewall basado en software ayuda para poner barreras al intruso en la computadora antes de que entre al sistema. Algunos firewalls personales soportan la característica de autenticación de aplicaciones, que sirve para legitimar a la aplicación que pretende salir a Internet.

2.9.3.2.2.1 Alternativas de solución de firewalls en el mercado

2.9.3.2.2.1.1 Symantec Sygate Enterprise Protection [82]

Symantec™ Sygate™ Enterprise Protection ofrece protección avanzada de puntos finales e integración perfecta con el control de acceso a la red en una sola arquitectura de administración. Protección de estaciones de trabajo administradas contra ataques conocidos y desconocidos con firewall de escritorio, prevención de intrusiones basadas en host y tecnologías de protección de gran adaptación.

Protege las redes contra las estaciones de trabajo que no cumplen con las políticas mediante la integración con Symantec™ Network Access Control (control de acceso a la red), que ofrece un amplio soporte para la integración de infraestructuras de la red. Elimina los hallazgos de auditoría no deseados al aplicar Compliance on Contact™ con la red de la empresa, mediante el uso de la opción de Control de acceso a redes para las estaciones de trabajo, Symantec Network Access Control y Endpoint Discovery. Administra una solución integrada con la administración de políticas de Symantec, que ofrece distribución de políticas en tiempo real, facilidad de uso y escalabilidad comprobada.

Características y especificaciones técnicas

Funciones

- Creación e implementación de políticas administradas en forma centralizada mediante Symantec™ Policy Manager

82 http://eval.symantec.com/mktginfo/enterprise/fact_sheets/DS-00309_SL_SMS_SMTP.pdf

- Los controles de la integridad del host incluyen estado del cumplimiento mediante Symantec™ Protection Agent
- El sistema de prevención de intrusiones en la red bloquea los ataques basados en la red y permite el tráfico autorizado en la red
- El control del dispositivo bloquea la transferencia de datos a dispositivos no autorizados de almacenaje portátil y permite la transferencia de datos a dispositivos autorizados
- Control de acceso a redes para las estaciones de trabajo por medio de Symantec Network Access Control Enforcers
- Estandarización automática que proporciona a las estaciones de trabajo cumplir con las políticas sin necesidad de intervención del usuario
- Las políticas de adaptación aplican regulaciones adecuadas en base al tipo de conexión a la red y/o ubicación en la red

2.9.3.2.2.1.2 eConceal Firewall [83]

eConceal Firewall para Servidores es un poderoso y avanzado firewall a nivel de Gateway, diseñado para proteger las redes privadas contra ataques que provienen desde Internet. Ofreciendo una seguridad totalmente personalizada, con reglas predefinidas por usuario tanto para el filtrado de paquetes como para los controles de acceso, cuenta con la funcionalidad de crear reglas basadas en protocolos no IP tales como ARP y es posible configurarlo con múltiples zonas.

Características:

- Filtrar los datos de la red y un seguimiento continuo de los filtros de red IP y del tráfico no IP.
- Reglas definidas por el usuario - Proporciona un potente sistema de filtrado de tráfico definidas por el usuario, con reglas de procesamiento. Los usuarios pueden definir reglas de acuerdo a sus necesidades y aplicar

83 http://translate.google.com.ec/translate?hl=es&sl=en&u=http://www.mwti.net/products/firewall/econceal_server/econceal_firewall_server.asp&ei=XfZgSuO-Ac2LtgfPvbjWDA&sa=X&oi=translate&resnum=1&ct=result&prev=/search%3Fq%3DeCONSEAL%2BFIREWALL%26hl%3Des%26sa%3DG

filtrado de tráfico.

- Reglas predefinidas- Ofrece un conjunto de reglas predefinidas los usuarios pueden elegir, con el fin de hacer cumplir el control de acceso. Los diferentes tipos de normas son ARP, DHCP y BOOTP, DNS, E-mail, Web, Noticias, Red Bios, FTP, ICMP, ICQ, Telnet y SSH, IRC, MSN, y VPN.
- Supervisor de tráfico de red - Muestra los datos actuales del tráfico en el sistema, incluida la información relativa a los programas abiertos y los puertos utilizados en la comunicación.
- Puerto de Vigilancia - Toda la comunicación entre su sistema y el mundo exterior se realizan a través de los puertos. eConceal impide la exploración de estos puertos y le avisa de cualquier intento no autorizado de los usuarios y los atacantes.
- Escaneo de páginas Web de - Proporciona control mediante el bloqueo de sitios Web pornográficos y ofensivos; para evitar el desperdicio de ancho de banda y acelerar la productividad.
- Informes de seguimiento del tráfico en tiempo real - Proporciona claro, conciso informes no gráficos sobre el tráfico interno y externo.
- Contraseña de protección - Garantiza la seguridad mediante la aplicación de contraseña para el firewall con el fin de evitar el acceso no autorizado a sus configuración.
- Fácil instalación y configuración

2.9.3.2.2.1.3 Shorewall

Es un lenguaje de alto nivel de propósito específico para manipular la infraestructura de control de paquetes del núcleo Linux, Netfilter. Shorewall es un script en lenguaje BASH (o en Perl en caso de utilizar shorewall-perl) que interpreta una serie de archivos de configuración a partir de los cuales hace sucesivas llamadas a iptables para definir el conjunto de reglas necesarias representadas por la configuración.

Además de iptables, Shorewall también utiliza otras herramientas para controlar otros módulos de red núcleo Linux como modprobe (para cargar los módulos de Netfilter), iproute (para la definición de reglas de ruteo) y tc (para el control de

tráfico de paquetes).

Características y funcionalidades de Shorewall

- Permite el filtrado de paquetes stateful gracias a las capacidades de monitoreo de conexiones de Netfilter.
- Puede utilizarse en múltiples aplicaciones de router (enrutador), firewall (corta-fuegos) o gateway (pasarela).
- Completamente configurable mediante el uso de archivos de configuración.
- Número de interfaces de red ilimitadas.
- Permite dividir las redes en zonas, permitiendo extenso control sobre las conexiones establecidas entre ellas.
- Múltiples interfaces por zona y múltiples zonas por interfaz.
- Soporta zonas anidadas y solapadas.

2.9.3.2.2.1.4 Iptables

Red Hat Enterprise Linux contiene herramientas avanzadas para el filtrado de paquetes de red, el proceso dentro del kernel de controlar los paquetes de red al entrar, mientras se mueven y cuando salen de la red. Los kernels anteriores al 2.4 confiaban en ipchains para el filtrado de paquetes y usaban listas de reglas aplicadas a los paquetes en cada paso del proceso de filtrado. La introducción de kernel 2.4 trajo consigo iptables (también llamado netfilter), lo cual es similar a ipchains pero expande enormemente el ámbito y el control disponible para el filtrado de paquetes de red.

2.9.4 ANÁLISIS COMPARATIVO

2.9.4.1 Costos de Software

Las licencias de Microsoft Windows y FortiClient Pc se detallan a continuación:

NOMBRE	VALOR
Windows Server 2003 Estándar (5 clt)	848.2 USD
Windows XP Pro Sp2 (1 clt)	244,3 USD
FortiClient Pc Host Security (1 usuario)	69 USD

Tabla 2.13.- Licencias Microsoft Windows y FortiClient PC [84]

2.9.4.2 Comparativa con Servidores

Requerimientos mínimos del Hardware de los sistemas Operativos Windows y Linux para su funcionamiento.

WINDOWS	LINUX
➢ Procesador 550 MHZ ➢ RAM 256 MB ➢ Disco duro 20 GB ➢ Un dispositivo desde donde instalar: CD –ROM o DVD-ROM ➢ Monitor VGA que admita la redirección de consola con resolución 800x600	➢ Procesador 550MHz (o mejor) ➢ RAM 512 MB ➢ Disco duro 10 GB ➢ Un dispositivo desde donde instalar, unidad de CD, tarjeta de red

Tabla 2.14.- Comparativa de servidores requerimientos mínimos de hardware [85]

2.9.4.3 Costos de los Dispositivos (Firewall)

A continuación los costos de los dispositivos de firewall que se mencionaron en el acápite **2.9.3.2.12** considerando el tamaño de la organización.

---

84 http://www.preciomania.com/search_getprod.php/masterid=701201/
http://www.injoule.com/microsoft-get-genuine-kit-for-windows-xp-professional-sp2-9PF-00088_7576_d.htm
http://www.navtek.com.mx/FortiGate60.htm

85 http://technet.microsoft.com/es-co/library/cc739866(WS.10).aspx
http://www.linuxparatodos.net/portal/staticpages/index.php?page=instalacion-texto-centos5

DISPOSITIVO	TAMAÑO EMPRESA	PRECIO
D-LINK DFL-800	Pequeña empresa	834,86 USD
D-LINK NetDefend DFL-860	Pequeña y mediana empresa	1261,76 USD
FortiGate-60	Pequeña empresa	799 USD
FortiGate-60B	Pequeña empresa	695. USD
SonicWALL TZ 180	Pequeña empresa	846,87 USD
SonicWALL TZ 190	Pequeña empresa	833.89 USD
D-Link DFL-1600	Grandes empresas	3178.82 USD
FortiGate 100A	Pequeña y mediana empresa	1.899 USD
FortiGate 200A	Pequeña y mediana empresa	2,995.00 USD
SonicWALL PRO 1260	Pequeña y mediana empresa	1671.32 USD
SonicWALL PRO 3060	Pequeña y mediana empresa	4659.53 USD
Cisco ASA 5505 Firewall Edition Bundle	Pequeña y mediana empresa	611,239 USD

Tabla 2.15.- Precios de dispositivos firewalls [86]

2.9.5 SELECCIÓN Y DETERMINACIÓN DE LA ALTERNATIVA DE SOLUCIÓN

Considerando que el Laboratorio LTI es una pequeña empresa que se desarrolla como un centro de apoyo académico para los estudiantes de la carrera; y el equipo FortiGate 60 se encuentra en el laboratorio; se concluye que es necesario aprovechar todas las características que ofrece este dispositivo en cuanto a protección de red se refiere.

2.9.6 PRESUPUESTO

El costo aproximado del proyecto de seguridad para el Laboratorio de

86 http://www.acuista.com/
http://www.navtek.com.
http://www.avfirewalls.com
http://www.avfirewalls.com/FortiGate-60B.asp

Tecnologías de la Información se muestra a continuación en la siguiente tabla;

DESCRIPCIÓN			VALOR	
		HORAS	**VALOR /HORA**	**COSTO TOTAL $**
RECURSO HUMANO	Administrador	96	40	3840
SOFTWARE	Windows XP Profesional Sp2			244,3
	FortiClient PC Host Security			69
HARDWARE	Firewall FortiGate 60			799
	Servidores			1226,4
GASTOS VARIOS	Internet			20
COSTO APROXIMADO $				6198,7

Tabla 2.16.- Costo aproximado del proyecto de seguridad para el LTI

Fuente Tecnicorp (Servidores)

CAPÍTULO 3: DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PARA EL LTI

En este capítulo se realiza el diseño y la implementación de un prototipo con el cual se separa los servicios públicos (correo, web) de la red interna, utilizando una Zona Perimetral (DMZ). Por otra parte garantizar una conexión segura al realizar una administración remota para esto se utiliza una red remota privada (VPN), todo esto con la finalidad de permitir que los usuarios de la intranet sean los únicos que puedan acceder a los recursos, servicios del laboratorio y la seguridad en la conectividad.

Para el desarrollo de este sistema de seguridad se utilizará el firewall FortiGate 60 que es un firewall a nivel de hardware, después de haber realizado el análisis de costo, el tamaño de empresa en el que se ubica el laboratorio y sobretodo porque el equipo se encuentra en el laboratorio LTI; disponible para hacer uso del potencial con el que fue adquirido

3.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

El LTI en la actualidad no cuenta con un ningún tipo de seguridad.

A continuación los inconvenientes que presenta el laboratorio:

- Tráfico en la red (no deseado).
- Falta de protección en la información.
- Unificación de servidores y estaciones de trabajo.
- Con la finalidad de solucionar estos inconvenientes se propone emplear el firewall FortiGate 60, a través de la configuración de este dispositivo que permita proteger los recursos y brindar una conexión segura desde otros hosts

3.2 ESTRUCTURA FÍSICA DE RED DEL LABORATORIO LTI ANTES DE LA IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD

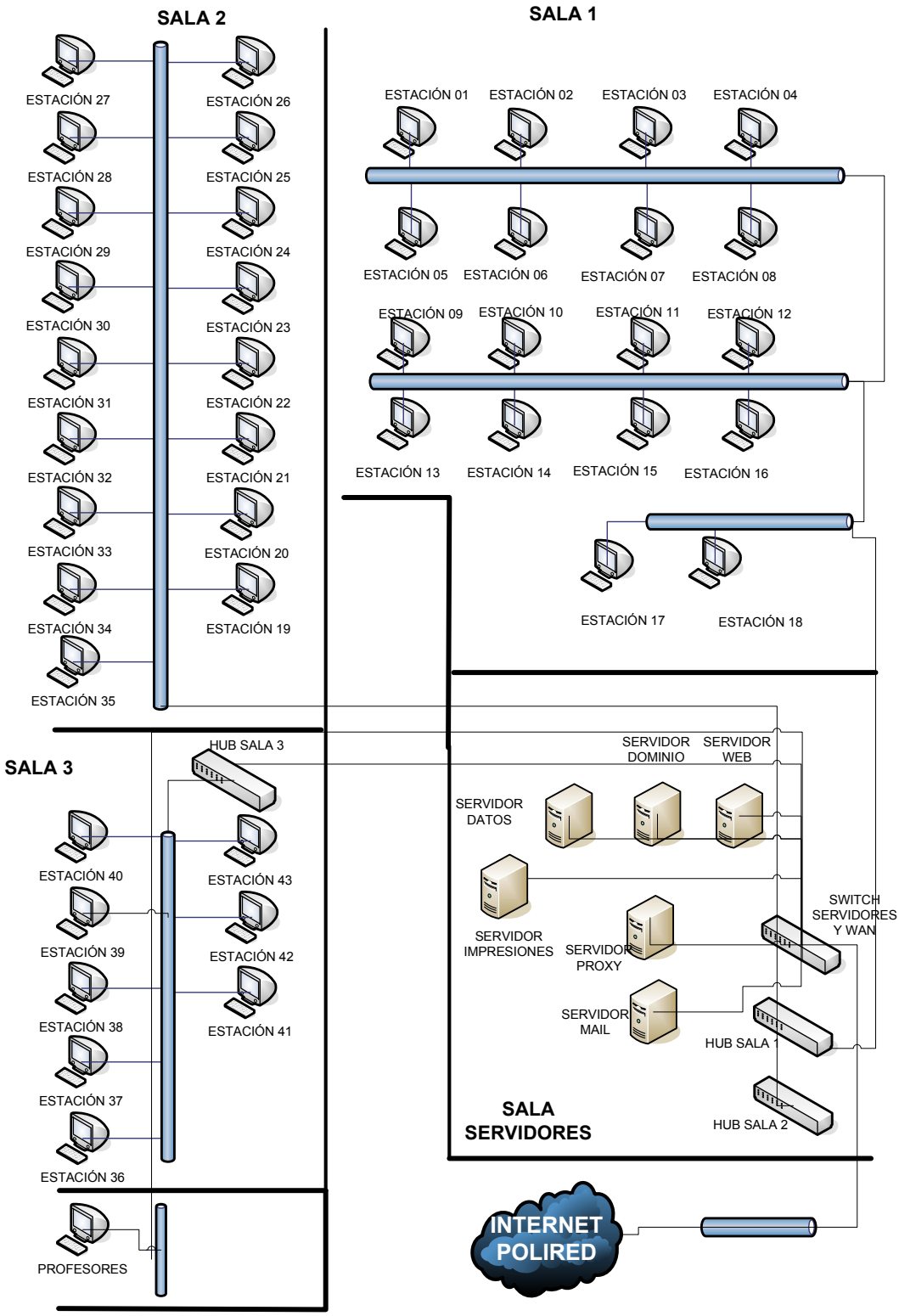


Figura 3.1.- Estructura de Red del LTI antes de la implementación de DMZ y VPN

Fuente Laboratorio LTI

3.3 ESTRUCTURA FÍSICA DE LOS SERVIDORES DEL LABORATORIO LTI ANTES DE LA IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD

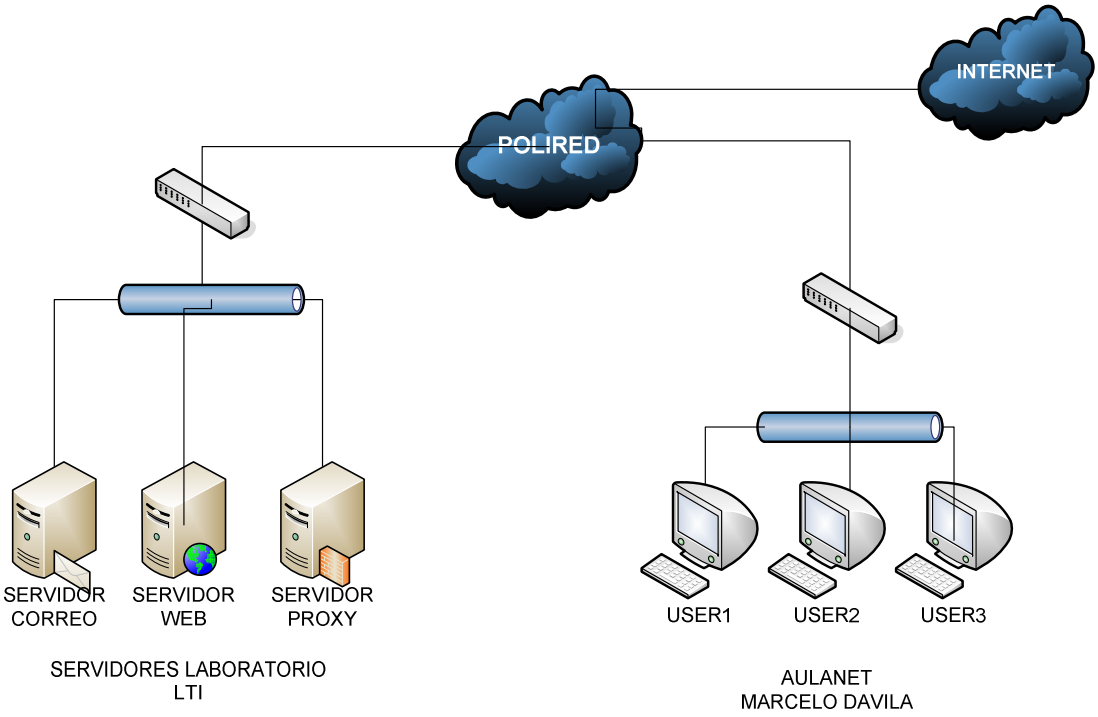


Figura 3.2.- Estructura de servidores del laboratorio LTI en la Polired antes de la implementación de DMZ y VPN

Fuente Laboratorio LTI

3.4 DISEÑO DE SOLUCIÓN DEL SISTEMA DE SEGURIDAD CON EL FIREWALL FORTIGATE 60

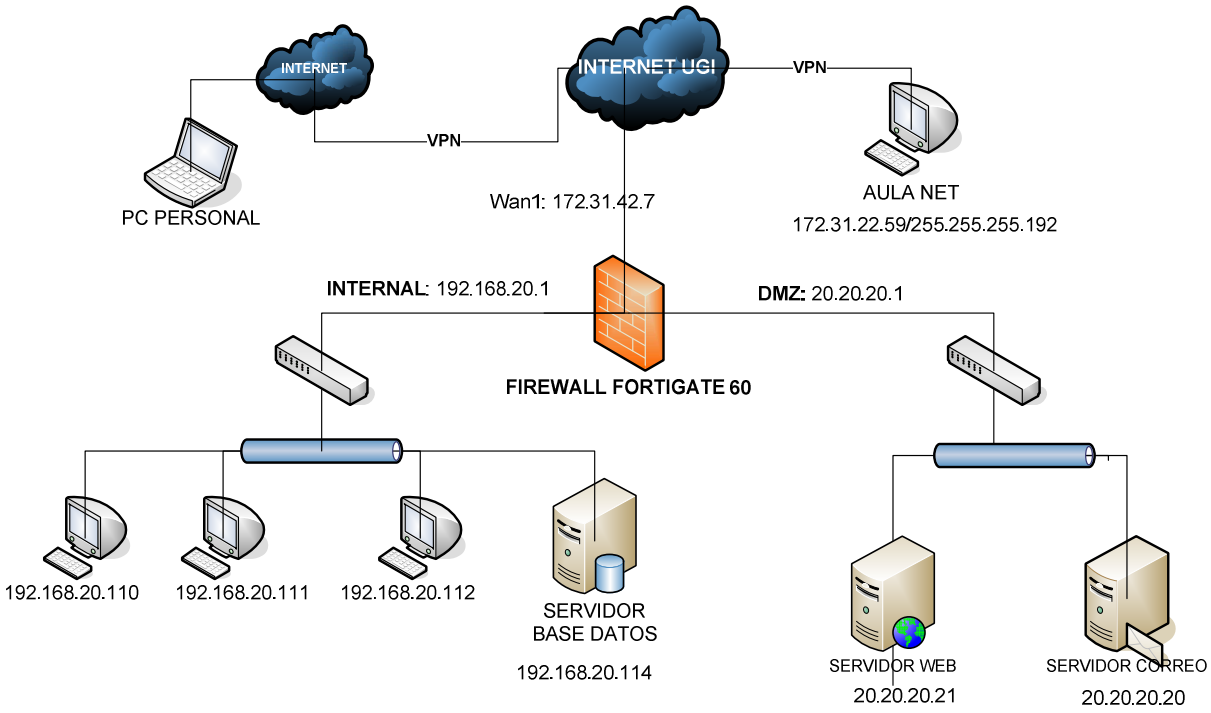


Figura 3.3.- Topología de Red del LTI con la implementación de Firewall

Elaborado por Andrea Elizabeth Conza Gonsález

3.5 CONFIGURACIÓN DE LOS SERVICIOS

Los servicios que se ubicarán en la DMZ son:

- Servicio Correo
- Servicio Web

El servicio que estará en la red interna es:

- Servicio Base de Datos

3.5.1 SERVIDOR CORREO

Para la instalación de este servicio se lo realiza en Centos 5, empleando **SquirrelMail.**

Configuración de las tarjetas de red

1. Ingresar la dirección IP estática en la tarjeta de red

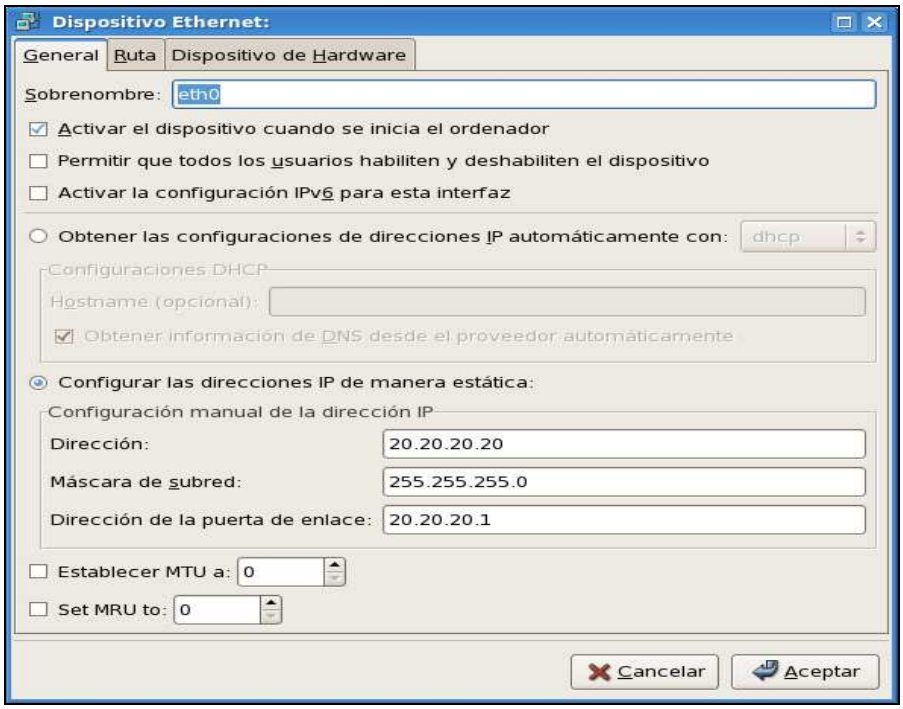


Figura 3.4.- Configuración de la tarjeta de red servidor de correo

2. Guardar la configuración de la tarjeta y activar la interfaz de red eth0.

Instalación y configuración del servicio

1. Abrir una Terminal y digitar:

   yum – y install httpd dovecot squirrelmail

   El servidor POP bajo CentOS es DOVECOT y es proporcionado por el paquete dovecot.
2. Reiniciar el servicio

   service httpd restart.
3. Editar el fichero de configuración de dovecot con cualquier editor en este caso se utiliza el vim <*vim /etc/dovecot.conf* >. Luego descometar la siguiente línea

   protocols= imap pop3

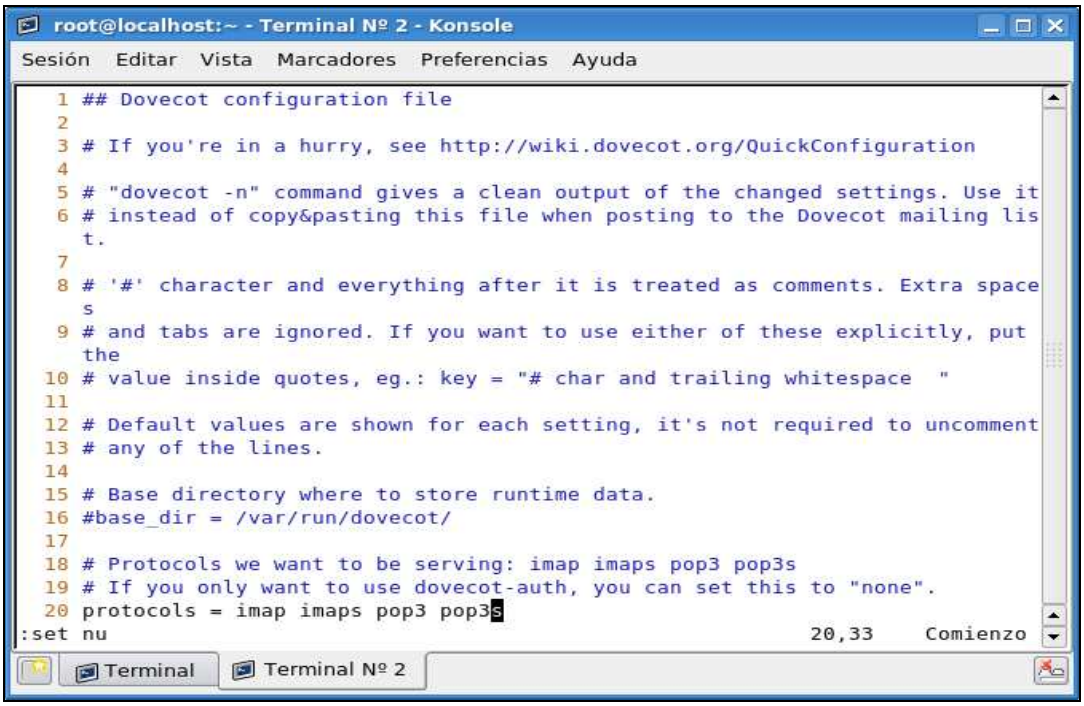


Figura 3.5.- Archivo de configuración de dovecot

4. Añadir este servicio al arranque del sistema

   chkconfig dovecot on.

5. Reiniciar el servicio dovecot y sendmail

   service dovecot restart.

   service sendmail restart

6. Ingresar a un navegador y digitar 20.20.20.20/webmail para ingresar a la página de inicio del correo.

Figura 3.6.- Ingreso al navegador de correo

7. Crear cuentas de usuario, y especificar la contraseña para el usuario

useradd <nombre_usuario>

passwd <nombre_usuario>

<contraseña>

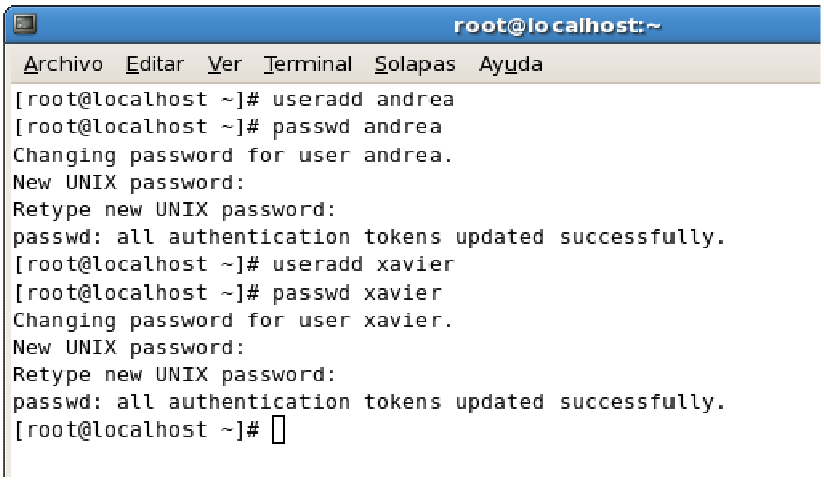


Figura 3.7.- Creación de cuenta de usuario

3.5.2 SERVIDOR WEB

Este servidor está instalado en Centos 5, a través del servidor Web **Apache**

Configuración de las tarjetas de red

1. Ingresar la dirección IP estática en la tarjeta de red

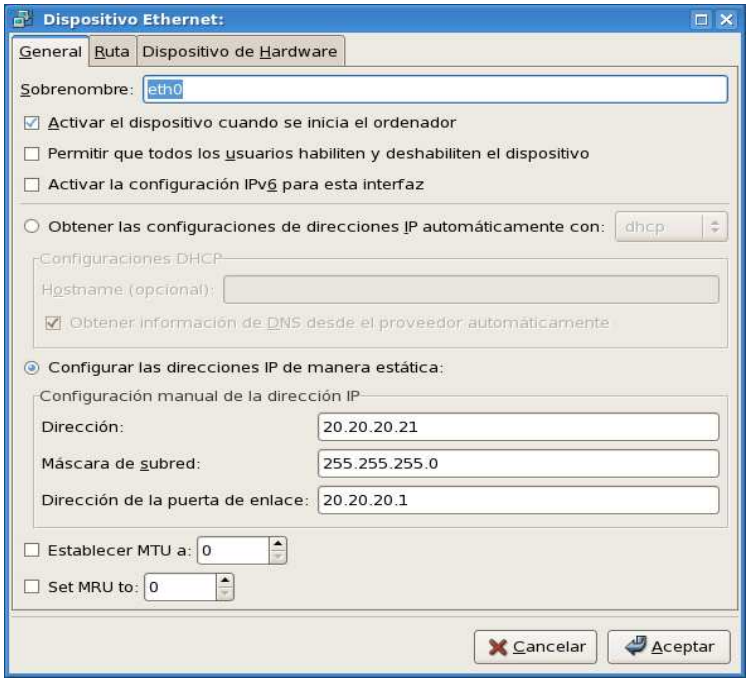


Figura 3.8.- Configuración de la tarjeta de red servidor web.

2. Guardar la configuración de la tarjeta y activar la interfaz de red eth0.

Instalación y configuración del servicio

1. Abrir una Terminal y digitar:

   yum – y install httpd.

2. Reiniciar el servicio

   service httpd restart.

3. Añadir este servicio al arranque del sistema

   chkconfig httpd on.

4. Ubicar el index del sitio web en:

   /var/www/html/index.hml

Figura 3.9.- Ubicación del directorio index.html

5. Ingresar a un navegador y digitar 20.20.20.21 para ingresar al index del sitio web.

Figura 3.10.- Página de inicio sitio web

3.5.3 SERVIDOR BASE DE DATOS

Un servidor de base de datos es un programa que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. En este caso el servidor de base de datos elegido es **MySQL** Este servidor prestará el servicio en la red interna, a través de la VPN se demostrará el acceso a este servidor

Para la instalación de este servicio se lo realiza en Centos 5, y para la administración visual de este servidor se utiliza **PhpMyAdmin.**

Configuración de las tarjetas de red

1. Ingresar la dirección IP estática en la tarjeta de red

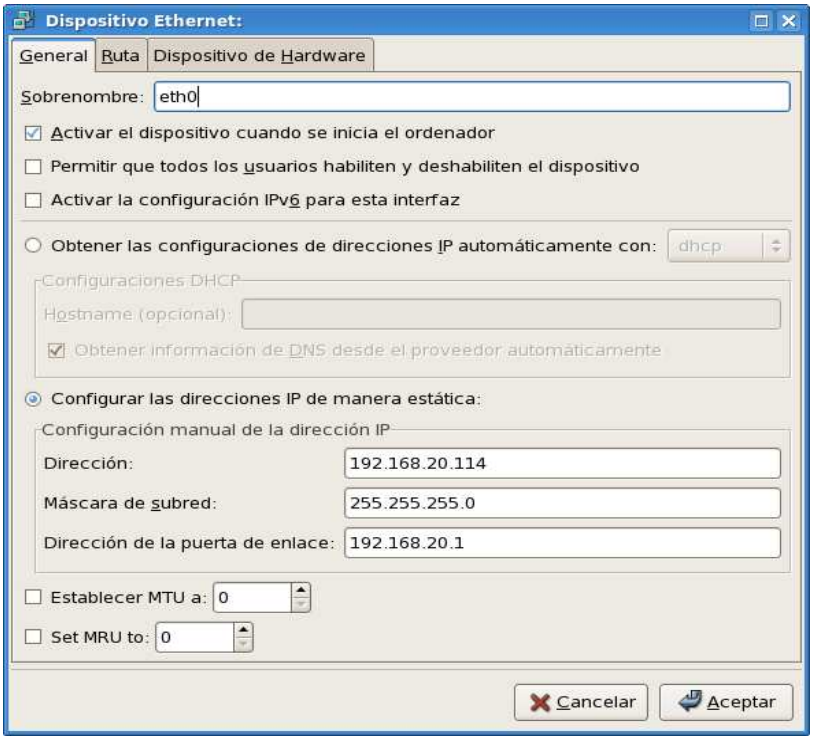


Figura 3.11.- Configuración de la tarjeta de red servidor de base de datos

2. Guardar la configuración de la tarjeta y activar la interfaz de red eth0

Instalación y configuración del servicio

1. Abrir una Terminal y digitar

   yum – y install httpd

   yum – y install php

yum – y install mysql mysql-server

2. Reiniciar los servicios.

   service httpd restart.

   service mysqld restart

3. Añadir este servicio al arranque del sistema

   chkconfig httpd on.

   chkconfig mysqld on.

4. Asignar una clave para ingresar al servidor de Mysql por defecto root no tiene contraseña

   mysqladmin –u root password <clave_acceso>

5. Probar la conexión con el servidor ingresando la contraseña

   mysql –u root –p

   mysql-> <clave_acceso>

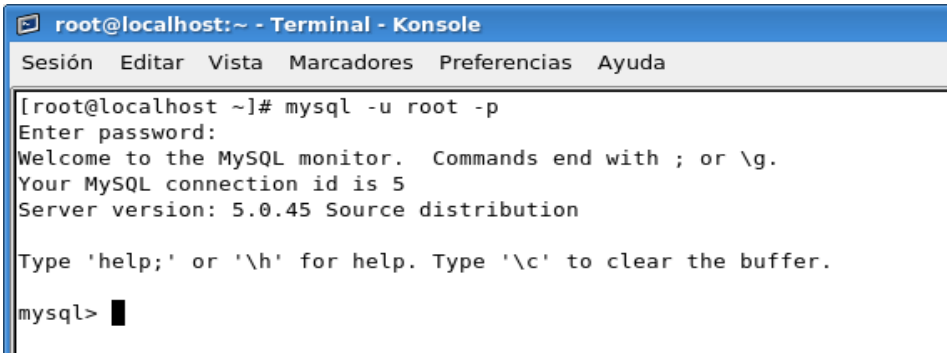


Figura 3.12.- Ingresar la clave de mysql

Instalación y configuración de phpmyadmin

1. Instalar phpmyadmin para obtener una interfaz más interactiva y amigable del servidor

   yum –y install phpmyadmin

2. Revisar los ficheros config.inc.php y config.sample.inc.php dentro del directorio */usr/share/phpmyadmin* si no existe alguno de ellos copiar y renombrar por el que falte especialmente < config.inc.php> ya que este será el index de phpmyadmin

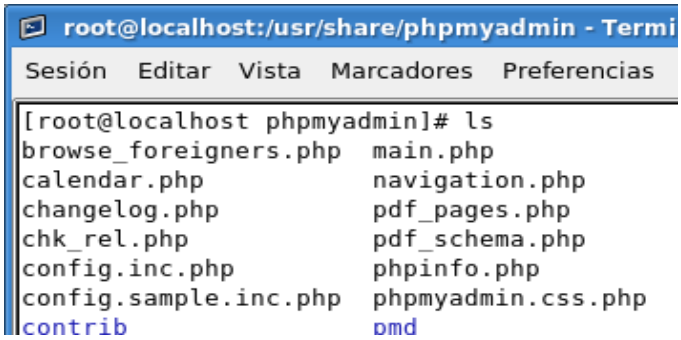


Figura 3.13.- Verificar la existencia de los archivos

3. Editar el fichero */usr/share/phpmyadmin/config.inc.php* y agregar una palabra secreta en la línea:

   cfg ['blowfish_secret'] ='<palabra_secreta';

```
13 /*
14  * This is needed for cookie based authentication to encrypt password in
15  * cookie
16  */
17 $cfg['blowfish_secret'] = 'mysql'; /* YOU MUST FILL IN THIS FOR COOKIE AUTH!
    */
18
```

Figura 3.14.- Edición de la palabra secreta

4. Reiniciar los servicios http y mysql

   service httpd restart.

   service mysqld restart

5. Ingresar a un navegador y digitar:

   192.168.20.114 /phpmyadmin/index.php

Figura 3.15.- Ingresar a la página de inicio de phpmyadmin

6. Crear una cuenta de usuario, y especificar el tipo de permisos para ese usuario; en este caso que tenga todos los privilegios porque se empleará para la implementación de la VPN
7. Ingresar a phpmyadmin Figura 3.16 y en la Figura 3.17 seleccionar Privilegios.

Figura 3.16.- Seleccionar privilegios en la página principal de phpMyAdmin

8. Seleccionar Agregar un nuevo usuario

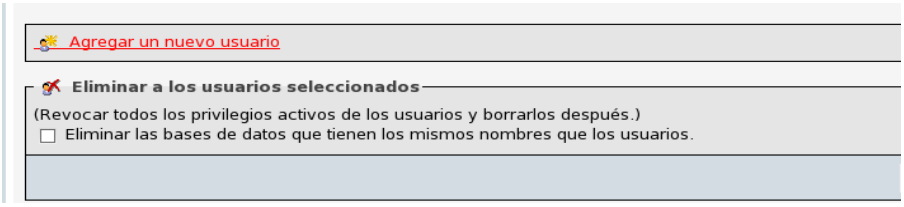


Figura 3.17.- Agregar un usuario nuevo

9. Asignar todos los permisos porque necesita acceder completamente a la base de datos sin ningún tipo de restricción

   Nombre de usuario: Xavier

   Servidor: Cualquiera

   Contraseña: *******

   Otorgar todos los privilegios

   Marcar todos los privilegios (privilegios globales)

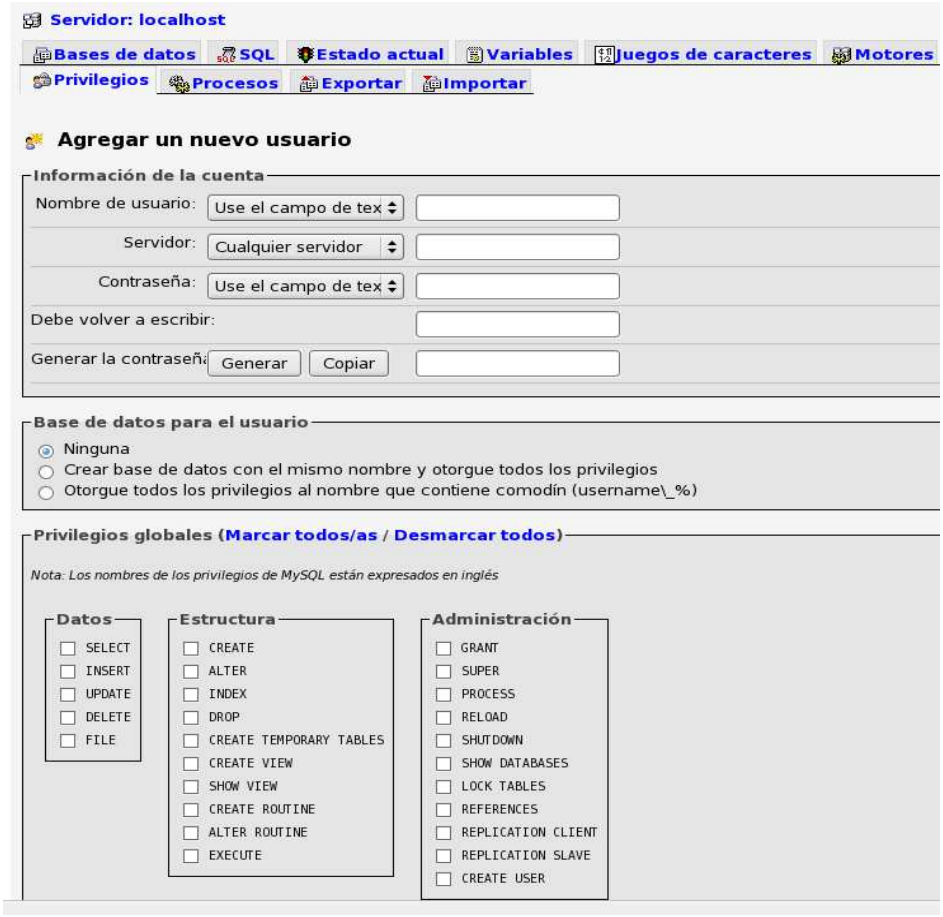


Figura 3.18.- Configuración de privilegios para el nuevo usuario

3.6 CONFIGURACIÓN DEL FIREWALL FORTIGATE 60

3.6.1 CONFIGURACIÓN INICIAL

Para la conexión del equipo se necesita lo siguiente:

Internet Explorer 6, Firefox 1.0 o Mozilla 1.6 o (nuevas versiones) con soporte Java para acceder a la consola de administración basada en web.

La conexión física del Firewall FortiGate con una PC se puede realizar de dos maneras:

Para la configuración basada en Web

Hub o switch

- Conectar un cable ethernet (directo) desde la tarjeta de red de la computadora hacia el hub o switch y otro cable al equipo FortiGate 60 en la interfaz internal.

Directamente Firewall FortiGate a la computadora

- Conectar un cable cruzado a la tarjeta de red de la computadora y el otro extremo hacia el firewall en la interfaz internal.

Interfaz Línea de Comandos

- Un conector DB9F-null para cable modem y un programa de emulación Terminal, (HyperTerminal para Windows, Minicom en Linux).

3.6.1.1 Configuración mediante CLI (interfaz de Línea de Comandos)

Al configurar a través de este modo los cambios que se realizan son inmediatos sin necesidad de resetear el equipo o interrumpir algún servicio.

Conexión de firewall FortiGate mediante interfaz CLI

1. Conectar el cable modem al puerto de comunicaciones del computador y el otro extremo al puerto de consola de firewall.
2. Encender el firewall FortiGate 60.
3. Iniciar la conexión con el programa Hyperterminal.
4. Registrar los siguientes parámetros:
   Bits por Segundo: 9600
   Bits de Datos: 8
   Paridad: No
   Bits de paridad: 1
   Control de Flujo: Ninguno
5. Para ingresar al equipo modo comando ingresar un nombre de usuario administrador en este caso admin. Si se necesita restablecer la configuración de fábrica se debe ejecutar el comando: *execute factoryreset*.

3.6.1.2 Configuración mediante la Interfaz de Administración basada en Web

La administración basada en web, es mucho más amigable puesto que es gráfica y permite tener una visión clara de los cambios que se realizan.

Conexión de firewall FortiGate mediante interfaz de Administración Basada en Web.

Previamente es necesario conocer cómo esta la anterior configuración para ingresar al equipo sin inconveniente. Se procede a realizar lo siguiente:

1. Configurar las direcciones IP del computador de manera estática: 192.168.1.20 con máscara de subred: 255.255.255.0 También se puede trabajar con DHCP del FortiGate.
2. Iniciar el navegador de Internet preferido y digitar: https://192.168.1.99.
3. Ingresar nombre de usuario: admin y clic en login.

Figura 3.19.- Interfaz inicial de administrador basada en web

Figura 3.20.- Menú principal

3.6.2 CONFIGURACIÓN DE INTERFACES

Estos son los tipos de acceso administrativo que se van a permitir en cada interfaz.

INTERFAZ	ACCESO ADMINISTRATIVO
INTERNAL	*HTTPS* para administración del firewall basada en web desde la red interna *PING* para conectividad troubleshooting *SSH* para obtener acceso a interfaz (CLI) desde la red interna.
WAN1	*HTTP* para acceso remoto a una administración basada en web desde el internet
DMZ	*PING* acceso por troubleshooting

Tabla 3.1.- Accesos administrativos para cada interfaz

INTERFAZ	DIRECCIONES
INTERNAL	*192.168.20.0/255.255.255.0*
WAN1	*172.31.42.7/255.255.255.0*
DMZ	*20.20.20.0/255.255.255.0*

Tabla 3.2.- Asignación de direcciones para las interfaces

3.6.2.1 Configuración de DHCP

Para realizar la nueva configuración en el firewall FortiGate es necesario activar el servicio de DHCP con la finalidad de iniciar la conexión con el firewall a través del nuevo Gateway. Como referencia del proyecto de titulación **"DISEÑO E IMPLEMENTACIÓN DE UNA RED SEGURA PARA EL LABORATORIO DE TECNOLOGÍAS DE LA INFORMACIÓN"**

Configuración DHCP

1. En el menú *System,* (Figura 3.20), seleccionar *DHCP*
2. Clic en *Service.*

3. Desplegar la interfaz *internal*,
4. Seleccionar *Servers*
5. Editar *internal_dhcp_server,*

   Enable, marcar esta opción para habilitar el servicio.

   Type, seleccionar Regular

   IP Range, 192.168.20.110 – 192.168.20.210 rango de direcciones IP dinámicas.

   Network Mask, máscara de red correspondiente al IP Range

   Default Gateway, dirección IP asignada para la interfaz Internal en este caso 192.168.20.1

   Lease, Time habilitar *Unlimited*
6. Clic en *OK*.

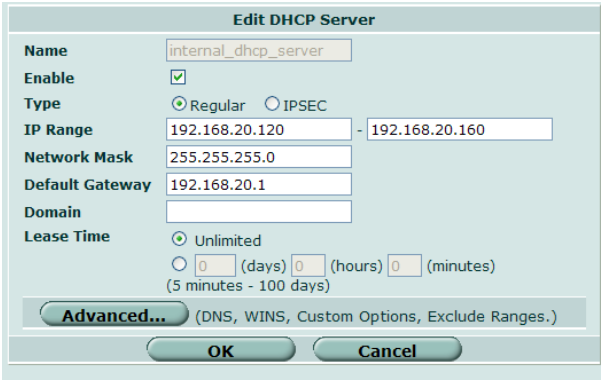


Figura 3.21.- Configuración DHCP

Después de realizar esta configuración es necesario modificar la interfaz Internal del firewall para ingresar con la nueva dirección sin problema.

3.6.2.2 Configuración de interfaz Internal

Configuración internal

1. En el menú *System,* (Figura 3.20), seleccionar *Network*
2. Clic en *Interface.*
3. Editar la interfaz *internal,*

   Addressing mode, marcar la opción *manual*.

   IP/Netmask, es la asignada como <Default Gateway> (Figura 3.21) y su respectiva máscara.

   Administrative Access, son los tipos de acceso administrativos en para

está interfaz: *HTTPS, PING, SSH*, ver (tabla 3.1)

4. Clic en *OK*.

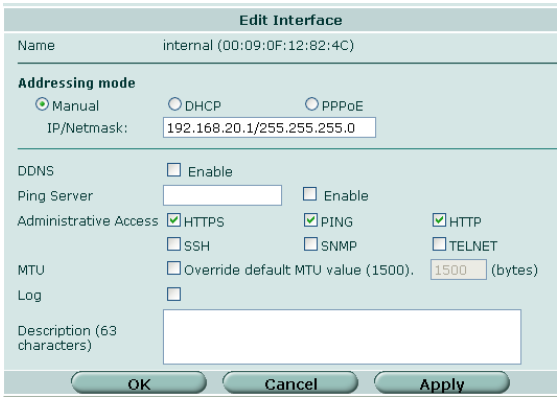


Figura 3.22.- Configuración interfaz Internal

3.6.2.3 Configuración de interfaz WAN1

Configuración Wan1

1. En el menú *System,* seleccionar *Network*
2. Clic en *Interface.*
3. Editar la interfaz *wan1*

   Addressing mode, marcar la opción *manual*.

   IP/Netmask, escribir la dirección IP pública de salida y su respectiva máscara de subred 172.31.42.7/255.255.255.0

   Administrative Access, marcar la opción *HTTPS* para tener conexiones seguras https para la administración del firewall a través de la administración basada en web desde la red wan.

4. Clic en *OK*.

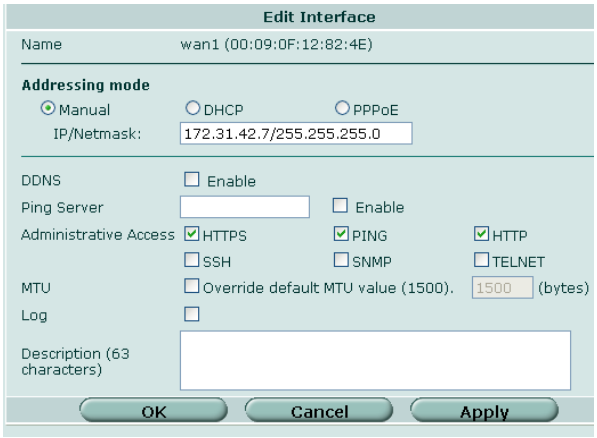


Figura 3.23.- Configuración interfaz wan1

3.6.2.4 Configuración de interfaz DMZ

Configuración DMZ

1. En el menú *System,* seleccionar *Network*
2. Clic en *Interface.*
3. Editar la interfaz *dmz,*

   Addressing mode, marcar la opción *manual*.

   IP/Netmask, escribir 20.20.20.1/255.255.255.0

   Administrative Access, marcar la opción *PING* para realizar pruebas de funcionamiento.
4. Clic en *OK*.

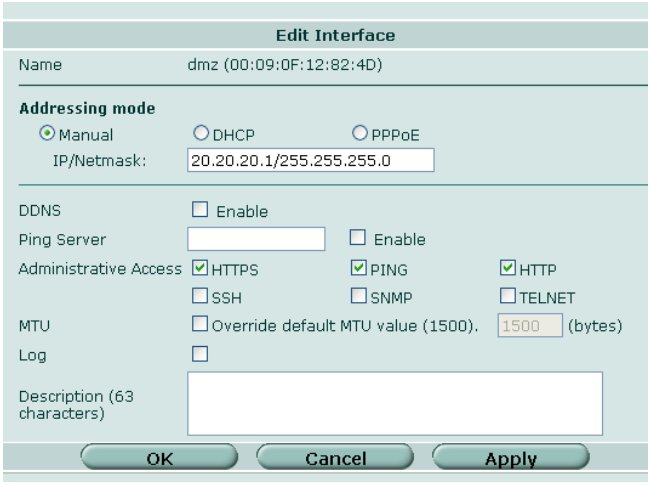


Figura 3.24.- Configuración interfaz dmz

3.6.2.5 Configuración Static Route [87]

Las rutas estáticas controlan el destino del tráfico saliente de la unidad FortiGate. Se configura rutas añadiendo direcciones IP de destino y máscara de red. Entonces se añade el gateway al cual el tráfico de estas direcciones es enrutado.

La unidad FortiGate asigna rutas utilizando el mejor algoritmo de coincidencia.

87 Tesis Carina Fiallos y Susana Toro, Diseño e implementación de una red segura para el laboratorio de tecnologías de la información, Abril 2007, Pág. 67

Para seleccionar una ruta para un paquete, la unidad FortiGate busca de una tabla, la ruta que mejor coincida con la dirección destino del paquete. Si no se encuentra coincidencia, la unidad FortiGate enruta el paquete utilizando la ruta por defecto.

Configuración Static Route

1. En el menú *Router,* (Figura 3.20), seleccionar *Static.*
2. Editar *Static Route* (Figura 3.25).

   Destination IP/Mask, 0.0.0.0/0.0.0.0 ruta de destino y su máscara representa hacia cualquier dirección IP.

   Device, dispositivo de salida por el cual se enrutará el tráfico.

   Gateway, escribir la puerta de enlace 172.31.42.1 asignada por la UGI

   Distance, ingresar una nueva distancia.
3. Clic en *OK*

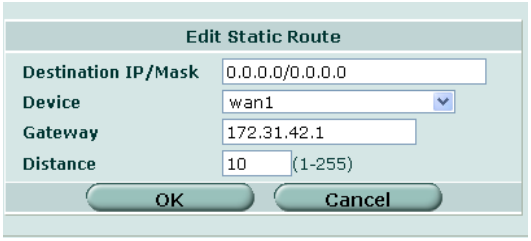


Figura 3.25.- Configuración Static Route

3.6.2.6 Configuración de DNS

Configuración DNS

1. En el menú *System,* seleccionar *Network.*
2. Clic en *Options*.
3. Seleccionar *Use the following DNS Server* addresses
4. Registrar *Primary DNS Server* 192.188.57.242
5. Registrar *Secondary DNS Server* 172.31.4.2
6. Habilitar el DNS para la interfaz Internal.
7. Seleccionar *Apply*.

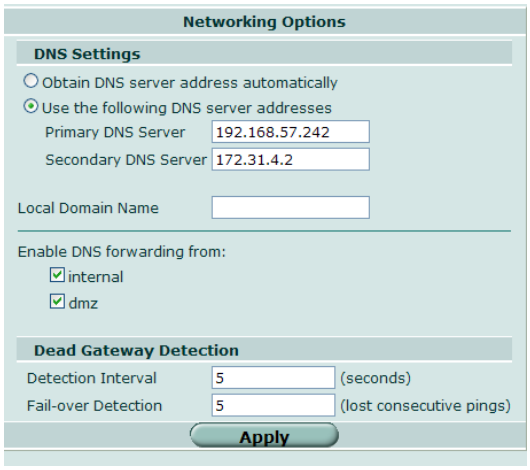


Figura 3.26.- Configuración DNS

3.6.3 MODO DE OPERACIÓN

3.6.3.1 Modo NAT (Network Address Translation) [88]

En modo NAT,/Route la unidad FortiGate es visible a la red. Todas las interfaces son de subredes diferentes. Las interfaces disponibles en este modo de operación son las siguientes:

Internal: es la interfaz de la red interna, en la cual se pueden conectar todas las subredes LAN.

- WAN 1: es la interfaz por default de la red externa, (usualmente Internet).
- WAN2: es la interfaz redundante de la red externa
- DMZ: es la interfaz de la red de-militarizada (DMZ).

Las políticas de Firewall controlan el flujo de tráfico basándose en las direcciones de origen, las direcciones de destino y el servicio de cada paquete. En el modo NAT, el firewall realiza la traducción de las direcciones de red antes de enviar el paquete a la red de destino.

88 Tesis Carina Fiallos y Susana Toro, Diseño e implementación de una red segura para el laboratorio de tecnologías de la información, Abril 2007, Pág. 61

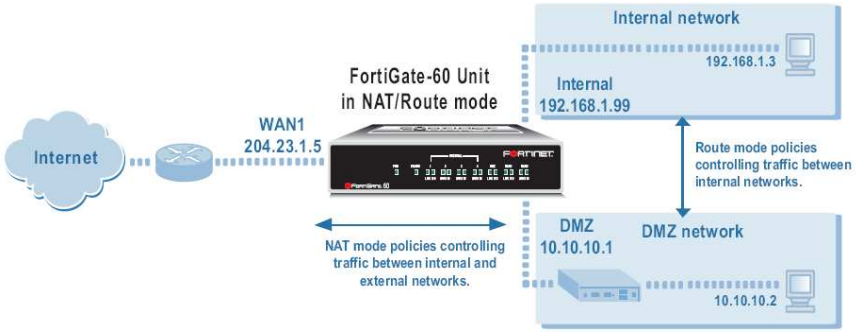


Figura 3.27.- Ejemplo de configuración de red con Modo NAT/Route

3.6.4 FIREWALL

3.6.4.1 Políticas de firewall

Una política de Firewall es un conjunto de instrucciones usadas por la unidad FortiGate para decidir qué hacer con las conexiones requeridas. Cuando el Firewall recibe una petición de conexión en forma de paquete, éste analiza el paquete para extraer la dirección de origen, la dirección de destino y el servicio por su número de puerto.

Para el paquete que debe ser conectado a través de la unidad FortiGate, una política de firewall debe estar en el sitio que coincida la dirección origen, la dirección destino y el servicio de dicho paquete. La política direcciona la acción del firewall sobre el paquete. Esta acción puede ser la de permitir la conexión, denegar la conexión, requerir autenticación previa a la conexión que es permitida, o también procesar el paquete como un IPSec VPN. También se pueden añadir horarios a las políticas así el firewall puede procesar conexiones diferentemente dependiendo de la hora del día, o del día de la semana, mes o año.

3.6.4.2 Registro de Direcciones

Ingreso de Direcciones

1. En el menú *Firewall*, (Figura 3.20), seleccionar *Address*.
2. Clic sobre *Create New*
3. Ingresar la siguiente información:

   Address Name, <usuario1>

Type, Subnet/IP Range

Subnet/IP Range, 192.168.20.110

4. Clic en *OK.*

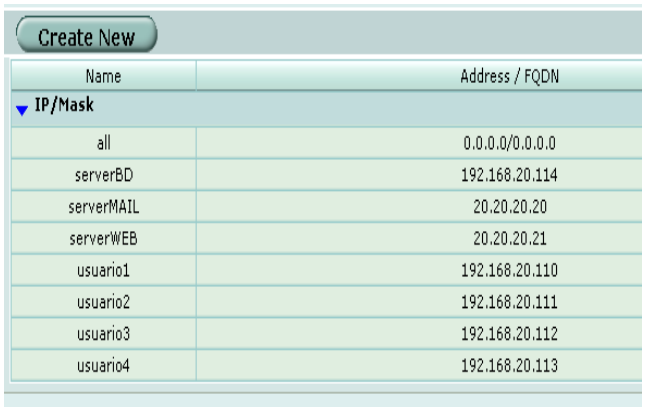


Figura 3.28.- Registro de direcciones usuarios

3.6.4.3 Grupo de Direcciones

Para obtener un fácil manejo de direcciones al momento de configurar las políticas es recomendable organizar por grupos

Creación de Grupos de direcciones

1. En el menú *Firewall,* seleccionar *Address*.
2. Seleccionar la pestaña *Group*.
3. Clic en *Create New* (Figura 3.26).
4. Ingresar la siguienteinformación:

   Group Name, intranet nombre del grupo.

   Available Address, seleccionar los usuarios que van a pertenecer a la lista de *Members* del grupo con la flecha↓.
5. Clic en *OK*.

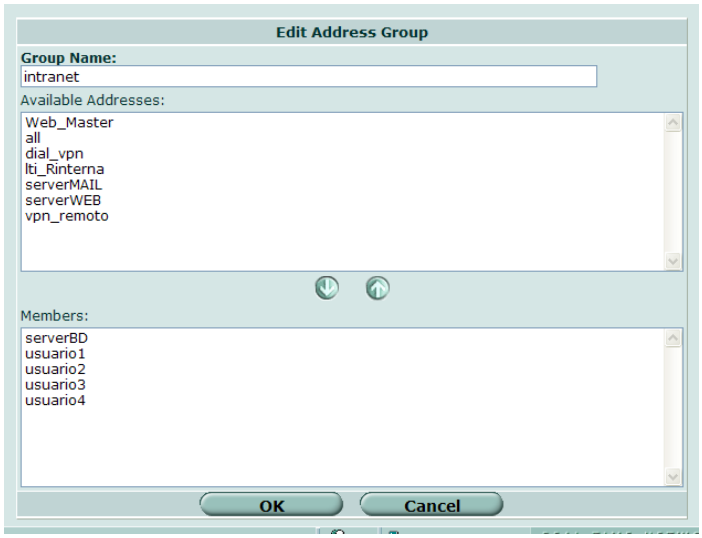


Figura 3.29.- Registro grupo de usuarios

3.6.5 SCHEDULES (INTERVALOS DE TIEMPO)

3.6.5.1 Recurring Schedules

Creación de Recurring Schedules

1. En el menú *Firewall,* seleccionar *Schedule*.
2. Seleccionar la pestaña *Recurring*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   Name, almuerzo, nombre de Schedule

   Seleccionar los días de la semana sobre los que Schedule estaría activo. Mon - Fri

   Registrar la hora y minuto de inicio

   Registrar la hora y minuto de finalización.
5. Clic en *OK*.

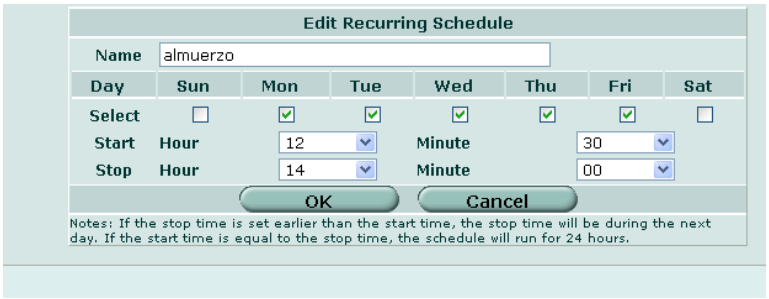


Figura 3.30- Creación recurring schedules

3.6.6 SERVICIOS

3.6.6.1 Grupos de Servicios

Creación de Grupos de Servicios

1. En el menú *Firewall,* seleccionar *Services*.
2. Seleccionar la pestaña *Group*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   Group Name, Chat como nombre de grupo.

   Available Services, seleccionar los servicio que van a pertenecer a la lista *Members* del grupo de servicios con la flecha →.
5. Clic en *OK.*

Figura 3.31- Creación de un servicio

3.6.7 WEB URL FILTERING Y CATEGORY BLOCK

A través de firewall se puede bloquear la visita de ciertas páginas, sea por su contenido, por sus URLs y aplicando las excepciones en cuanto a visitas

3.6.7.1 Content Blocking

Configuración Content Block

1. En el menú *Web Filter,* (Figura 3.20).
2. Seleccionar *Content Block*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

Pattern, palabra o frases, para aplicar el bloqueo sobre todas las páginas web que contengan esa palabra o frase.

Pattern Type, seleccionar el tipo de patrón;

Wildcard

Regular Expression

Language,.seleccionar un lenguaje.

Enable, habilitar.

5. Clic en *OK.*

Figura 3.32.- Contenido bloqueado

3.6.7.2 URL Blocking

Bloque accesos a páginas web con sólo agregar a una lista de URL's bloqueados. La unidad FortiGate bloque cualquier página web que coincida con los URL's o patrones especificados, enviando un mensaje al usuario.

Configuración URL Block

1. En el menú *Web Filter,*
2. Seleccionar *URL Filter*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   URL, ingresar una URL completa o parcial, dirección IP o un sufijo de dominio para bloquear.

   Type, Simple.

   Action, Block.

   Seleccionar Enable
5. Clic en *OK.*

Figura 3.33.- Lista de URL's bloqueadas

3.6.8 PROTECTION PROFILES (PERFILES DE PROTECCIÓN)

Los Perfiles de Protección permiten tener control sobre los usuarios aplicando la configuración realizada anteriormente, (Recurring Schedule)

Para los usuarios que se crearon se trabajará en dos aspectos; horario de trabajo en cuanto a páginas bloqueadas y su contenido.

Creación de Protection Profiles (horario de trabajo)

1. En el menú *Firewall,* seleccionar *Protection Profile*.
2. Seleccionar la pestaña *Group*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   Profile Name, <usuarios_trabajo> nombre del perfil.

   Web Filtering, habilitar las opciones que se configuraron para contenido web, (Web URL block y Web URL exempt list).
5. Clic en *OK.*

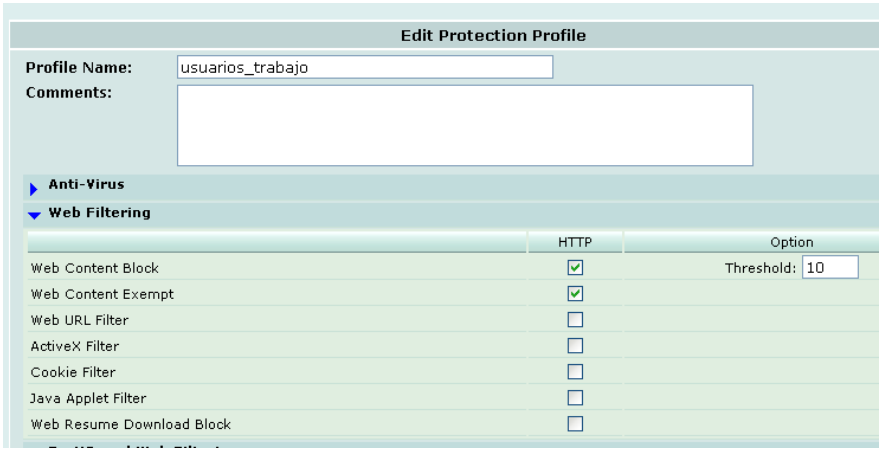


Figura 3.34 Creación de un Perfil nuevo

3.6.9 POLÍTICAS DE FIREWALL

Las políticas se establecen para cada grupo de usuarios implementando configuración Web block, uso de Schedule y bloqueo a Chat y cualquier tipo de mensajería. Las políticas pueden ser de acuerdo origen y destino.

3.6.9.1 Configuración de Políticas usuarios

Las políticas siempre deben ir de lo específico a lo general.

Configuración de Políticas

1. En el menú *Firewall,* seleccionar *Policy*.
2. Clic en *Create New*
3. Ingresar la siguiente información:

   Source *Interface/Zone,* desde la internal

   Address Name, nombre del recurso intranet

   Destination *Interface/Zone,* hacia la wan1

   Address Name, all.

   Schedule, always.

   Service, ANY

   Action, ACCEPT

   Habilitar *NAT*

   Habilitar *Protection Profile*, <usuarios_trabajo > (Figura 3.34).
4. Clic en *OK.*
5. Clic en *Create New*
6. Ingresar la siguiente información:

   Source *Interface/Zone,* internal

   Address Name, nombre del recurso intranet

   Destination *Interface/Zone,* wan1

   Address Name, all.

   Schedule, always.

   Service, chat.

   Action, DENY

   Habilitar *NAT*.
7. Clic en *OK.*

NOTA: Ubicar esta nueva política en primer lugar

3.6.10 SERVICIOS PROTEGIDOS DMZ

3.6.10.1 Servidor Web

Un servidor Web es un ordenador que usa el protocolo http para enviar páginas web al ordenador de un usuario cuando el usuario las solicita.

3.6.10.1.1 Virtual IP

Configuración unidad FortiGate con una Virtual IP

Con el servidor web localizado en la interfaz DMZ, se necesita configurar una dirección virtual IP (VIP), para que los requerimientos al sitio web sean enrutados correctamente. La virtual IP puede ser incluida después en las políticas internal → wan1.

1. En el menú *Firewall,* seleccionar *Virtual IP*.
2. Clic en *Create New*
3. Ingresar la siguiente información:

   Name serverWEB_VIP
   External Interface, wan1
   Type, *Static* NAT.
   External IP Address/Range, 172.31.42.65
   Map to IP Address/Range, 20.20.20.21.
4. Clic en *OK.*

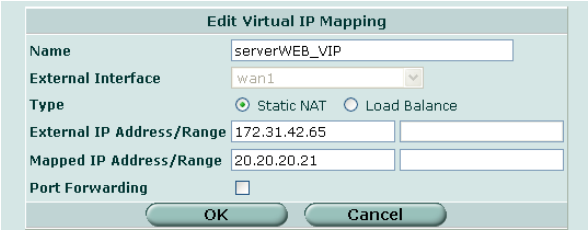


Figura 3.35.- Configuración VIP servidor web

3.6.10.1.2 Agregar al Registro de Direcciones servidor web

Agregar el servidor web al registro de Direcciones

1. En el menú *Firewall,* seleccionar *Address*.

2. Seleccionar la pestaña *Address*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   Address Name, serverWEB.

   Type, Subnet/IP Range

   Subnet / IP Range 20.20.20.21
5. Clic en *OK*.

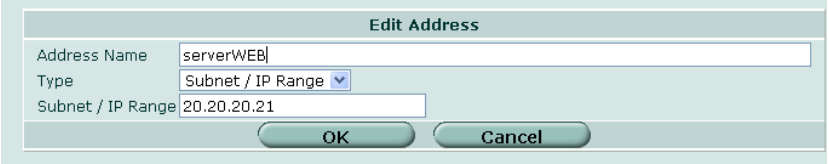


Figura 3.36.- Registro de dirección del servidor correo

3.6.10.1.3 Agregar al Registro de Direcciones web master

Agregar al web master al registro de Direcciones

1. En el menú *Firewall,* seleccionar *Address*.
2. Seleccionar la pestaña *Address*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   Address Name, Web_Master.

   Type, Subnet/IP Range

   Subnet / IP Range 192.168.20.150, dirección IP asignada para el web master.
5. Clic en *OK*.

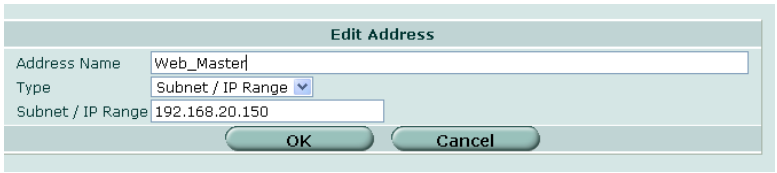


Figura 3.37.- Registro de dirección del web master

3.6.10.1.4 Políticas de uso para el servidor web

Configurar políticas para el servidor web.

Wan1 → DMZ.

Agregar una política para usar desde el Internet (wan1), para acceder al sitio web

en la red DMZ.

Agregar una política para acceder al servidor web

1. En el menú *Firewall,* seleccionar *Policy*.
2. Seleccionar la pestaña *Address*.
3. Clic en *Create New* .
4. Ingresar la siguiente información:

   Source *Interface/Zone,* wan1.
   Address Name, all.
   Destination *Interface/Zone,* dmz
   Address Name, serverWEB_VIP.
   Schedule, always.
   Service, HTTP.
   Action, ACCEPT.
5. Clic en *OK*.

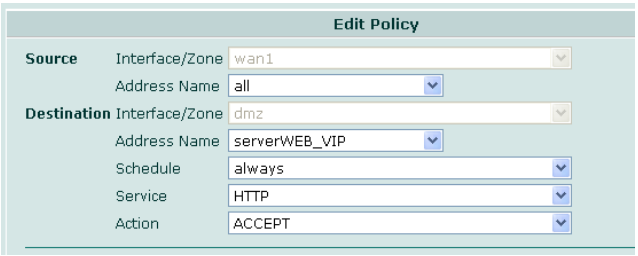


Figura 3.38.- Registro de dirección del web master

Internal → DMZ.

Agregar una política para que el desarrollador web suba las actualizaciones correspondientes al sitio web del servidor.

Agregar una política para que acceda el web master al servidor

1. En el menú *Firewall,* seleccionar *Policy*.
2. Seleccionar la pestaña *Address*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   Source *Interface/Zone,* internal.
   Address Name, Web_Masterl.
   Destination *Interface/Zone,* dmz

Address Name, serverWEB

Schedule, always.

Service, FTP.

Action, ACCEPT.

5. Clic en *OK*.

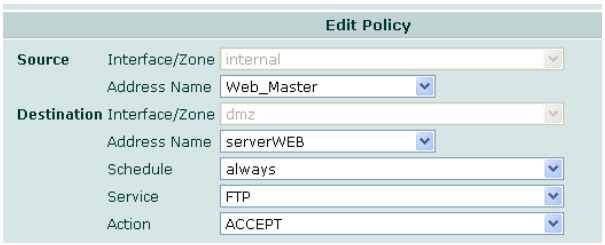


Figura 3.39.-- Políticas de acceso del web master

3.6.10.2 Servidor Correo

El correo electrónico, se puede decir que es el servicio más utilizado de todos los que existen actualmente de arquitectura cliente-servidor.

3.6.10.2.1 Virtual IP

Configuración unidad FortiGate con una Virtual IP

Con el servidor de correo localizado en la red DMZ, se necesita configurar una dirección virtual IP (VIP), para que los requerimientos al correo sean enrutados correctamente. La virtual IP puede ser incluida después en las políticas wan1 → DMZ.

1. En el menú *Firewall,* seleccionar *Virtual IP*.
2. Clic en *Create New*
3. Ingresar la siguiente información:

   Name serverMAIL_VIP

   External Interface, wan1

   Type, *Static* NAT.

   External IP Address/Range, 172.31.42.180

   Map to IP Address/Range, 20.20.20.20.
4. Clic en *OK.*

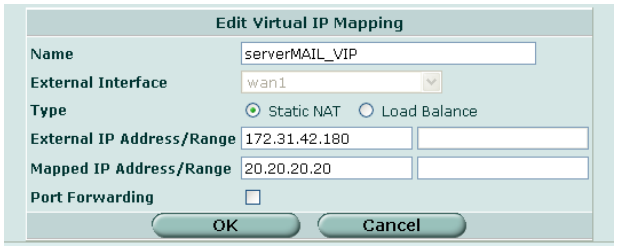


Figura 3.40.- Configuración VIP del servidor correo

3.6.10.2.2 Agregar al Registro de Dirección

Agregar el servidor correo al registro de Direcciones

1. En el menú *Firewall,* seleccionar *Address*.
2. Seleccionar la pestaña *Address*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   Address Name, serverMAIL.

   Type, Subnet/IP Range

   Subnet / IP Range 20.20.20.20
5. Clic en *OK*.

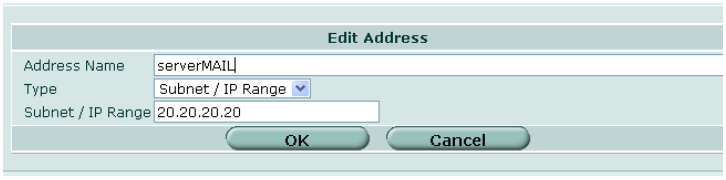


Figura 3.41.- Registro de dirección del servidor de correo

3.6.10.2.3 Políticas para el servidor de correo

Configurar políticas para el servidor de correo.

DMZ → wan1.

Agregar una política que permita al servidor enviar correos afuera

Agregar una política para envío de mensajes

1. En el menú *Firewall,* seleccionar *Policy*.
2. Seleccionar la pestaña *Address*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

Source *Interface/Zone,* dmz.
Address Name, serverMAIL.
Destination *Interface/Zone,* wan1
Address Name, all.
Schedule, always.
Service, SMTP.
Action, ACCEPT.

5. Clic en *OK*.

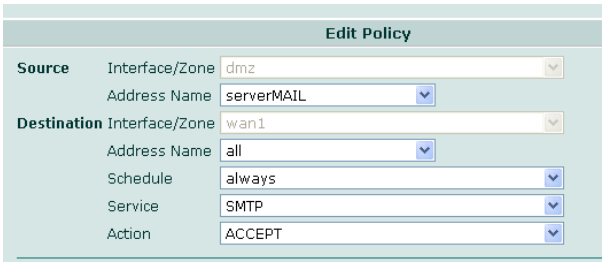


Figura 3.42.- Política para envió de mensajes

Wan1 → DMZ.

Agregar una política que permita desde los servidores de correo del Internet lleguen los mensajes al servidor.

Agregar una política para recibir correos de afuera

1. En el menú *Firewall,* seleccionar *Policy*.
2. Seleccionar la pestaña *Address*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

Source *Interface/Zone,* wan1.
Address Name, all.
Destination *Interface/Zone,* dmz
Address Name, serverMAIL_VIP
Schedule, always.
Service, SMTP.
Action, ACCEPT.

5. Clic en *OK*.

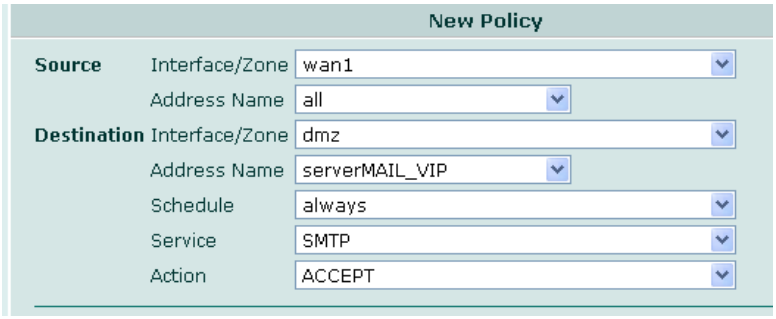


Figura 3.43.- Política para permitir correos desde servidores externos

Internal → DMZ.

- Agregar una política para que los usuarios de la intranet envíen mensajes hacia fuera; al servidor (SMTP).
- Agregar una política para que los usuarios de la intranet lean los mensajes dentro (POP3).
- Agregar una política para que los usuarios de la intranet envíen mensajes hacia fuera (IMAP).

Agregar una política para correos internos

1. En el menú *Firewall,* seleccionar *Policy*.
2. Seleccionar la pestaña *Address*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   Source *Interface/Zone,* internal.
   Address Name, all.
   Destination Interface/Zone, dmz
   Address Name, serverMAIL
   Schedule, always.
   Service, SMTP.
   Action, ACCEPT.
5. Clic en *OK*.

6. Clic en *Create New*
7. Ingresar la siguiente información:

   Source *Interface/Zone,* internal.

Address Name, all.

Destination Interface/Zone, dmz

Address Name, serverMAIL

Schedule, always.

Service, POP3.

Action, ACCEPT.

8. Clic en *OK*.

9. Clic en *Create New*
10. Ingresar la siguiente información:

Source *Interface/Zone,* internal.

Address Name, all.

Destination Interface/Zone, dmz

Address Name, serverMAIL

Schedule, always.

Service, IMAP.

Action, ACCEPT.

11. Clic en *OK*.

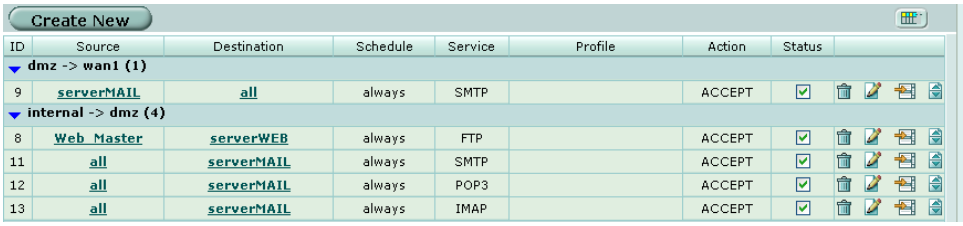


Figura 3.44.- Políticas para permitir correos internos

3.6.11 VPN (VIRTUAL PRIVATE NETWORK)

Una red privada virtual nos permite mantener una conexión segura a través del internet, para la demostración se pretende conectar con el servidor de base de datos que se encuentra en la intranet.

La configuración de la VPN será definida como Dialup VPN

Al configurar la unidad FortiGate como un servidor VPN Dial-up permite a un cliente remoto utilizar el software FortiClient Host Security para conectarse a la red interna de la unidad FortiGate.

En una configuración dialup-cliente, los clientes VPN remotos incluyendo la aplicación FortiClient Host Security se asignan direcciones IP dinámicas antes de iniciar una conexión a una unidad local FortiGate. Los clientes Dialup suelen obtener direcciones IP dinámicas del ISP a través del Dynamic Host Configuration Protocol (DHCP) o de Point-to-Point Protocol over Ethernet (PPPoE)

3.6.11.1 Configuración Dial-up VPN en Firewall FortiGate

3.6.11.1.1 Registro de Direcciones

Agregar la subred al registro de Direcciones

1. En el menú *Firewall,* seleccionar *Address*.
2. Seleccionar la pestaña *Address*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   Address Name, lti_Rinterna.

   Type, Subnet/IP Range

   Subnet / IP Range 192.168.20.0/255.255.255.0
5. Clic en *OK*.

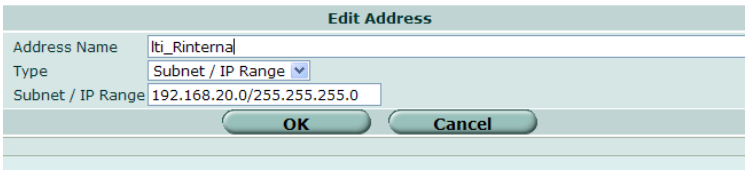


Figura 3.45.- Registro de un rango de direcciones

3.6.11.1.2 Configuración usuario local del equipo FortiGate

Agregar un usuario local en el Firewall

1. En el menú *User,*
2. Seleccionar la pestaña *Local*.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   User Name, user42.

   Password <contraseña>
5. Clic en *OK*.

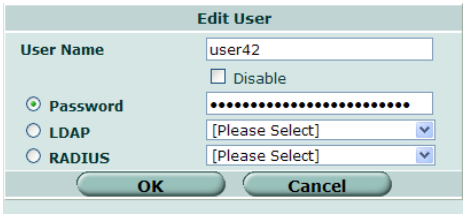


Figura 3.46.- Registro de nuevo usuario local de ForiGate

3.6.11.1.3 Agregar el usuario a un grupo de usuarios

Agregar un usuario local en un grupo

1. En el menú *User,*
2. Seleccionar la pestaña User Group.
3. Clic en *Create New*
4. Ingresar la siguiente información:

   Group Name, grupo_vpn

   Type: *Firewall*

   Protection Profile *unfiltered*

   Agregar el usuario <user42> con la flecha → e incluirlo en Members de Local Users
5. Clic en *OK*.

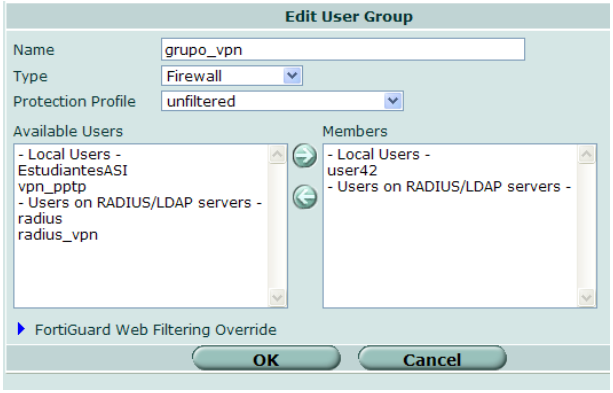


Figura 3.47.- Registro del usuario en un grupo

3.6.11.1.4 IPSEC Phase 1

Configurar IPSec phase1

1. En el menú *VPN,* seleccionar *IPSEC*.
2. Seleccionar la pestaña *Auto Key((IKE)*
3. Clic en *Create Phase1* (Figura 3.48).

4. Ingresar la siguiente información:

   Gateway Name, dial

   Remote Gateways, dialup User

   Local Interface *wan1*

   Mode, Aggressive

   Authentication Method, Preshared Key

   Pre-shared Key, ********* (clave conocida solo por el administrador)

   Peer Options, Accept peer ID in dialup group <grupo_vpn>

5. Clic en *OK*.

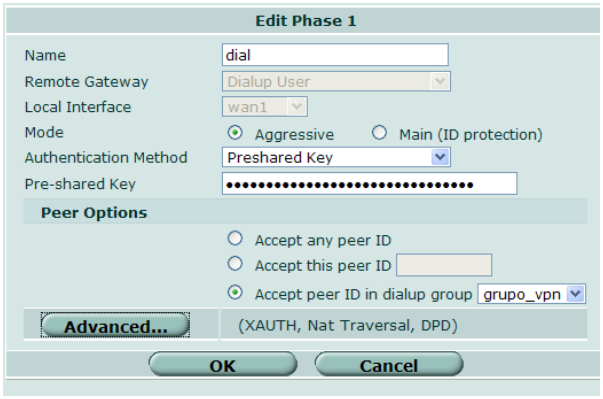


Figura 3.48.- Configuración Phase1

3.6.11.1.5 IPSEC Phase 2

Configurar IPSec phase2

1. En el menú *VPN,* seleccionar *IPSEC*.
2. Seleccionar la pestaña *Auto Key((IKE)*
3. Clic en *Create Phase2* (Figura 3.49).
4. Ingresar la siguiente información:

   Name, dialTunel

   Phase1, dial, (nombre generado en la phase1)

5. Clic en *OK*.

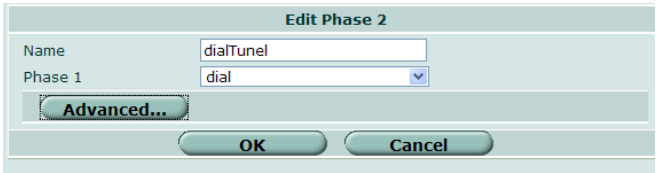


Figura 3.49.- Configuración Phase2

3.6.11.1.6 Creación de un rango de direcciones para los usuarios dialup

Rango de direcciones para los usuarios dial up

1. En el menú *Firewall*
2. Seleccionar la pestaña *Address*
3. Clic en *Create New*
4. Ingresar la siguiente información:

   Address Name, dial_vpn

   Type, Subnet/IP Range

   Subnet/IP Range 192.168.20[5-10]
5. Clic en *OK*.

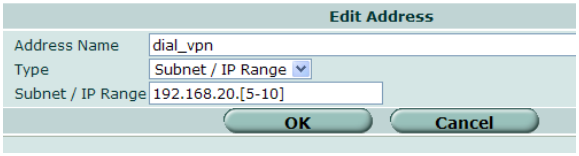


Figura 3.50.- Configuración de rango de direcciones para usuarios dial up

3.6.11.1.7 Políticas de firewall para la VPN

Las políticas se aplican específicamente para mantener una conexión segura entre el usuario remoto (usuario dialup) y la red interna.

Configurar políticas para VPN

1. En el menú *Firewall,* seleccionar *Policy*.
2. Clic en *Create New*
3. Ingresar la siguiente información:

   Source *Interface/Zone,* internal

   Address Name, lti_Rinterna

   Destination Interface/Zone, wan1

   Address Name, dial_vpn.

   Schedule, always.

   Service, ANY

   Action, IPSEC

   VPN Tunnel, dial

   Marcar *Allow inbound*

Allow outbound

4. Clic en *OK*.

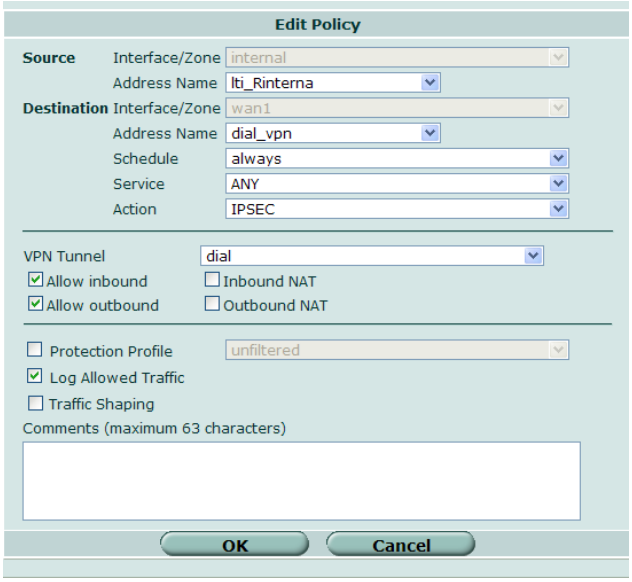


Figura 3.51.- Política para VPN

3.6.11.2 Instalación de FortiClient en el cliente VPN

Fortinet dentro de sus productos de seguridad ofrece el software FortiClient para obtener conexiones seguras para clientes que usan Windows

Es necesario como requisito necesario tener instalado Windows XP

Instalación de FortiClient

1. Ejecutar el programa FortiClient,

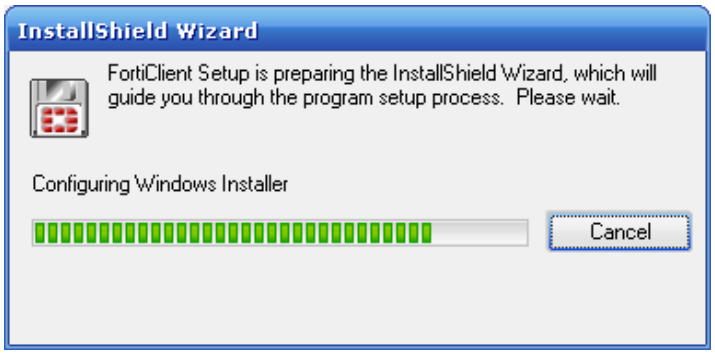


Figura 3.52.- Ejecución del programa FortiClient

2. Leer y aceptar la licencia del programa FortiClient; para continuar clic en Next.

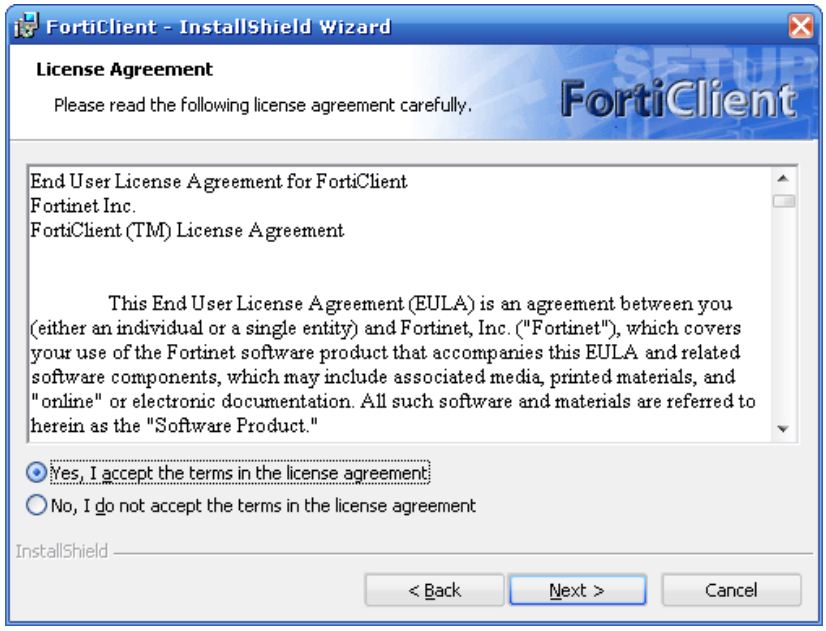


Figura 3.53.- Licencia y términos de uso para el usuario FortiClient

3. Seleccionar el modo IPSec VPN and Firewall puesto que es la aplicación que se necesita para realizar la VPN, clic en Next

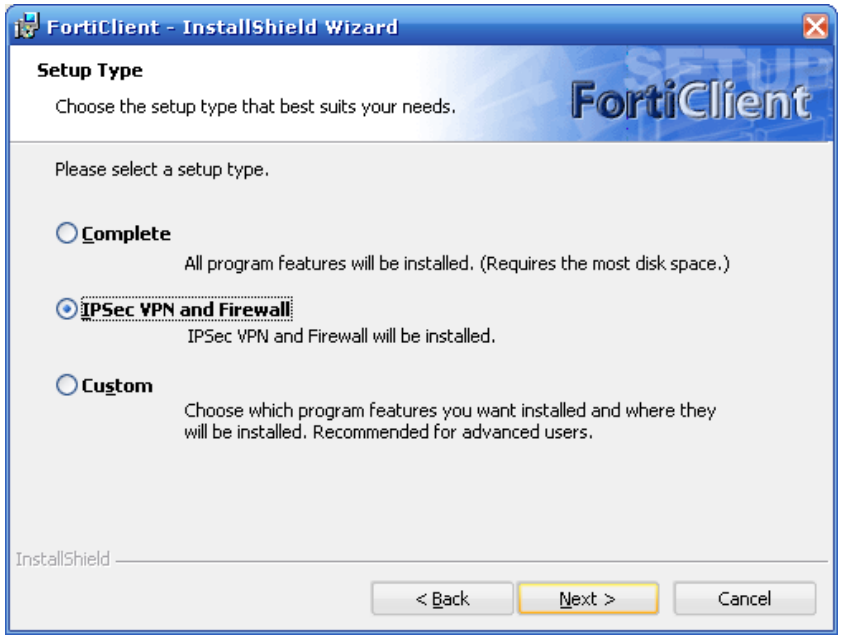


Figura 3.54.- Tipo de instalación de IPSec VPN y Firewall

4. Marcar Install para iniciar la instalación de FortiClient en la máquina del usuario remoto.

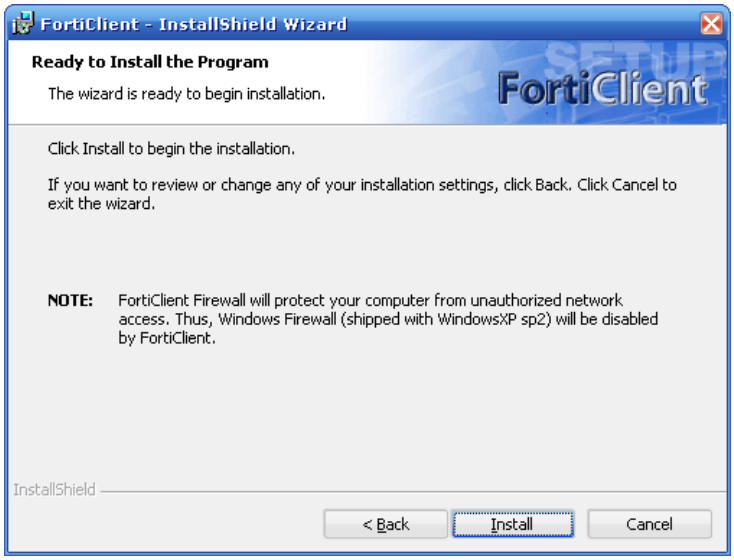


Figura 3.55.- Inicio de la instalación

5. Finalmente la instalación ha terminado satisfactoriamente, clic en Finish.

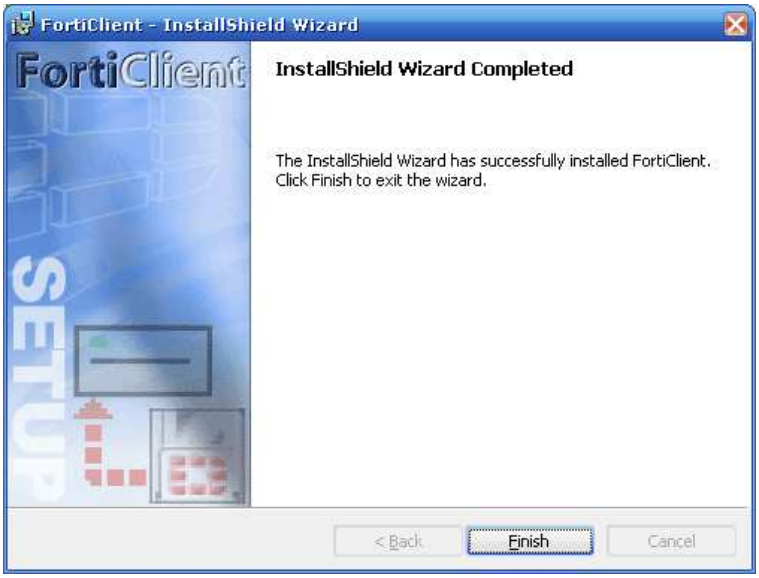


Figura 3.56.- Finalización del programa

3.6.11.3 Configuración de FortiClient

Despúes de realizar la instalación se procede a configurar los parámetros necesarios para utilizar FortiClient como un usuario de VPN

Configuración de FortiClient

1. Abrir FortiClient para el usuario dialup

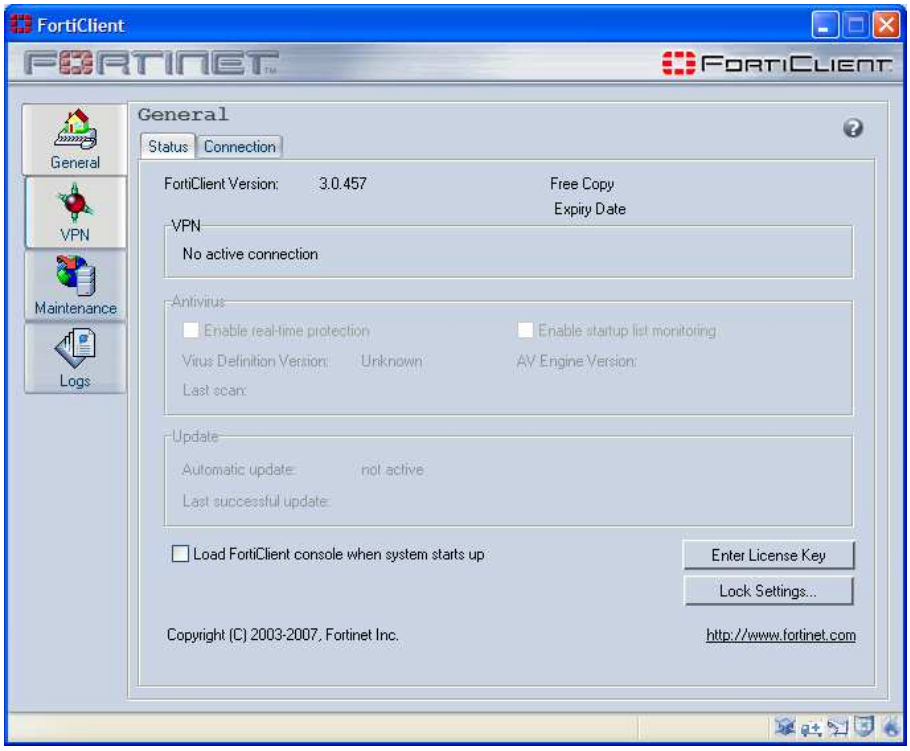


Figura 3.57.- Página principal de Forticlient

2. Clic en *VPN*, seleccionar la pestaña *Connections*
3. Seleccionar *Add* .
4. Ingresar la siguiente información:

Connection Name,	*vpn_user*
Configuration	*Manual*
Remote Gateway,	172.31.42.7 (Dirección IP de la interfaz wan1)
Remote Network,	0.0.0.0 / 0.0.0.0
Authentication method,	Preshared Key.
Preshared Key,	******** (clave ingresada en phase1).

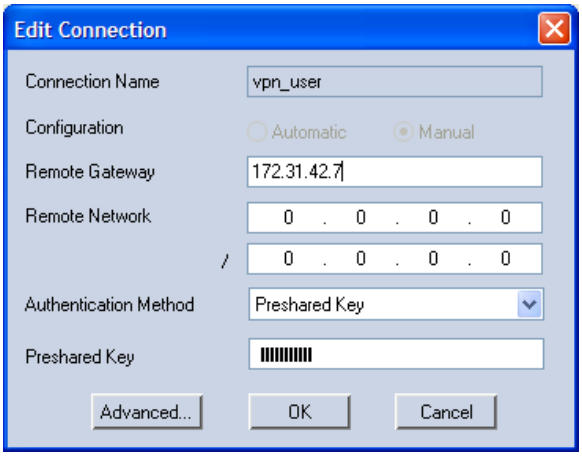


Figura 3.58.- Configuración usuario en FortiClient

5. Clic en *Advanced:*

   Remote Network 0.0.0.0 0.0.0.0

   Agregar <IP_dinámica asignada por el ISP> <mascara>

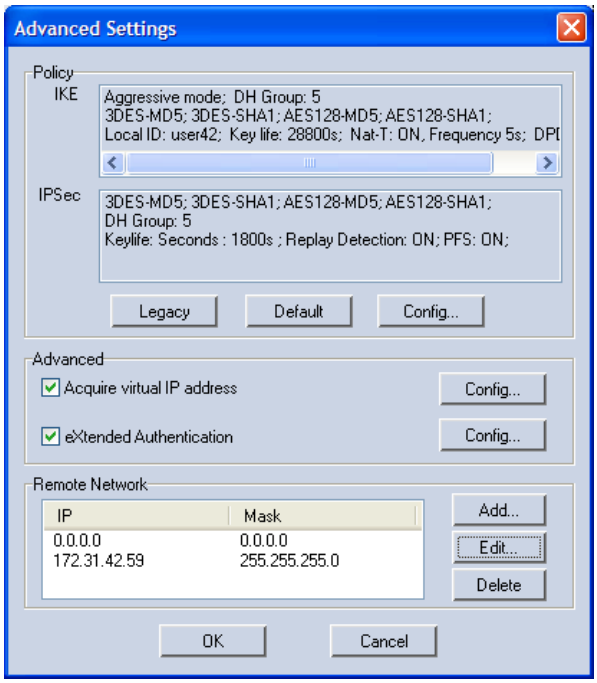


Figura 3.59.- Menú de configuración avanzadas FortiClient

6. Clic en Config en la sección Policy (Figura 3.59)

   Mode Aggresive

   Local ID user42

NOTA: El tipo de modo debe ser igual al que se selecciono en la configuración de la phase1

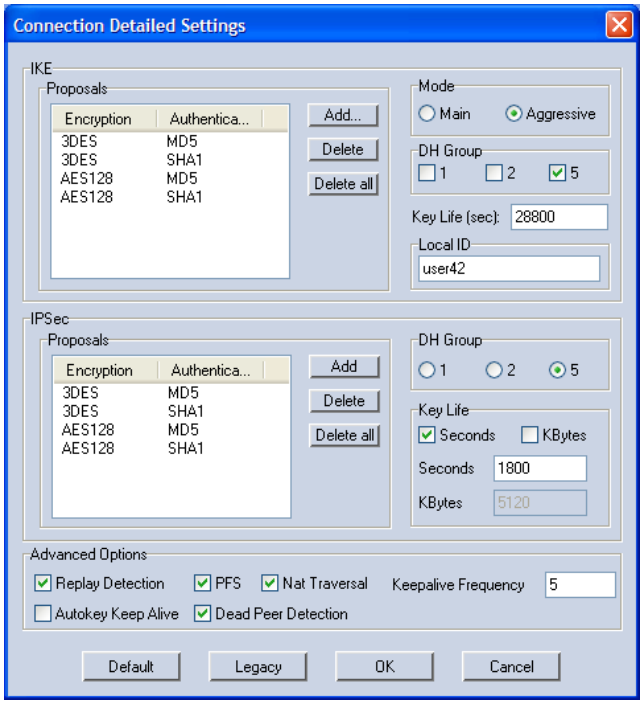


Figura 3.60.- Configuración avanzada de FortiClient

7. Clic *OK*
8. Marcar con un visto *Acquire Virtual IP address*. (Figura 3.59) y clic en *Config* que se encuentra junto a la selección realizada.
9. Seleccionar Manually Set (si no se tiene un servidor DHCP sobre IPSec.)

   IP 192.168.20.8

   Subnet Mask 255.255.255.0

   DNS Server 172.31.4.2

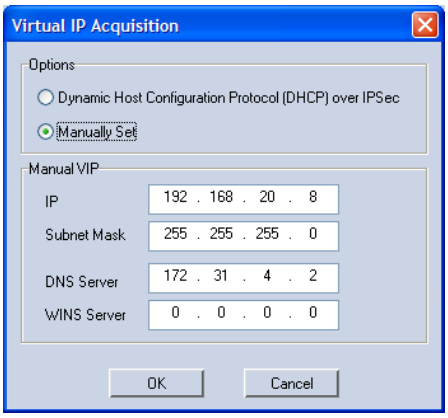


Figura 3.61.- Configuración manual de Virtual IP

10. Clic *OK*
11. Marcar con un check eXtended Authentication (Figura 3.59) y clic en

Config que se encuentra junto a la selección realizada

12. Seleccionar Prompt to login. (si no desea digitar el usuario y la contraseña al iniciar la sesión)

Figura 3.62.- Configuración de inicio de sesión del cliente VPN

13. Clic *OK*
14. Clic OK las veces que sean necesarias hasta volver a la ventana principal (Figura 3.57)
15. Clic en Connect. El estado del túnel debe ser Up
16. Ingresar el comando ipconfig /all; desde la computadora del cliente (FortiClient) y observar la configuración virtual.

Figura 3.63.- Comprobación de conectividad con la interfaz internal

3.6.11.4 Instalación de MySQL Tools en el cliente VPN

Se puede realizar una conexión segura a un servidor MySQL remotamente mediante SSH utilizando MySQL Tools 5.0 para clientes Windows.

Instalación de MySQL Tools 5.0

1. Ejecutar el programa mysql-gui-tools-5.0-r17-win32, clic en Next.

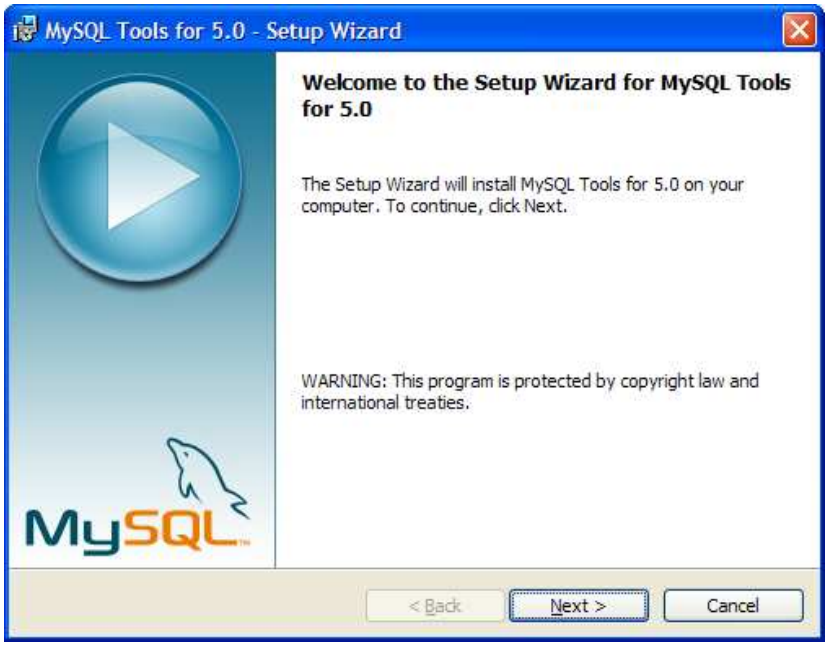


Figura 3.64.- Setup de MySQL Tools

2. Leer y aceptar la licencia, clic en *Next*.

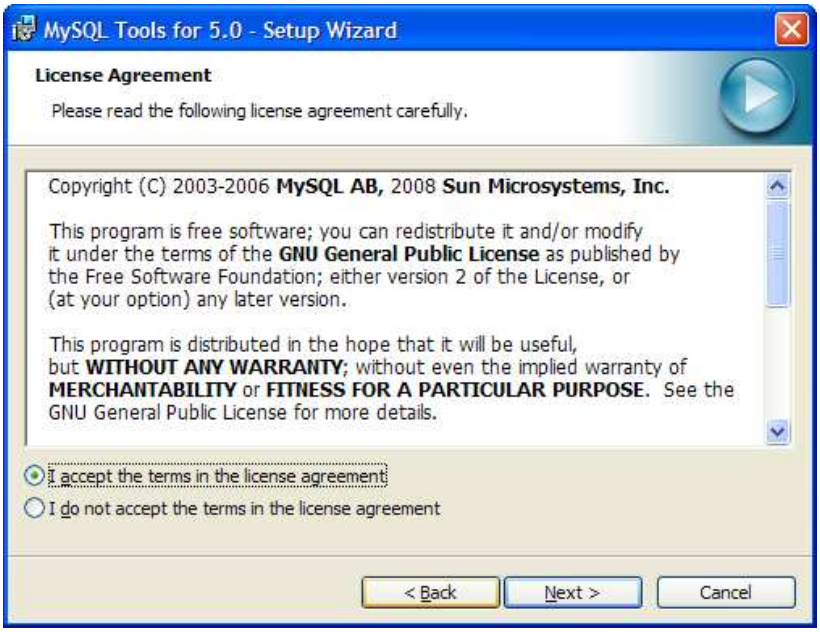


Figura 3.65.- Licencia y términos de uso de MySQL Tools

3. Indicar la ubicación donde se guardará los archivos de este programa, clic *Next*.

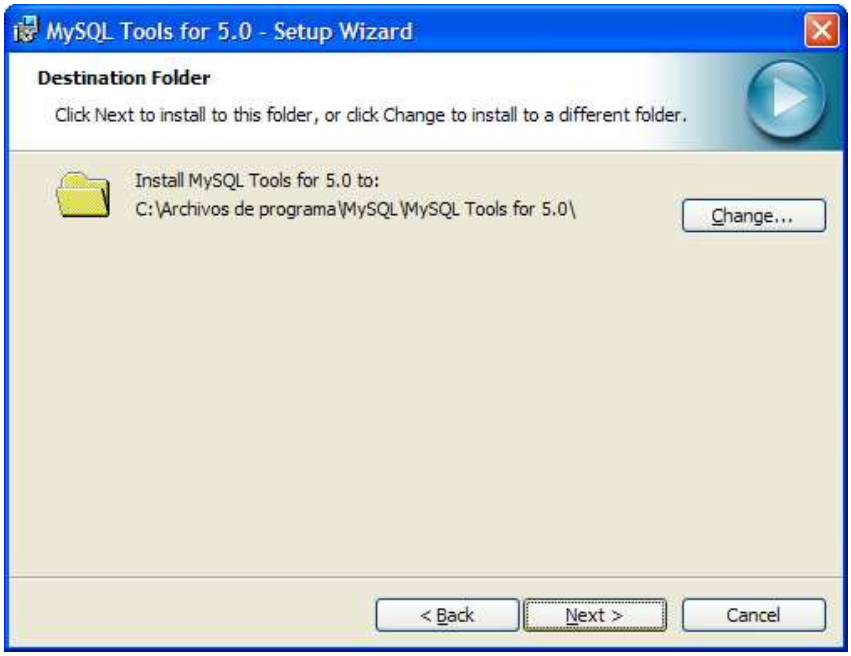


Figura 3.66.- Destino de la carpeta de instalación de MySQL Tools

4. Seleccionar el tipo de instalación. En este caso escoger la instalación completa para una mejor administración, clic en *Next.*

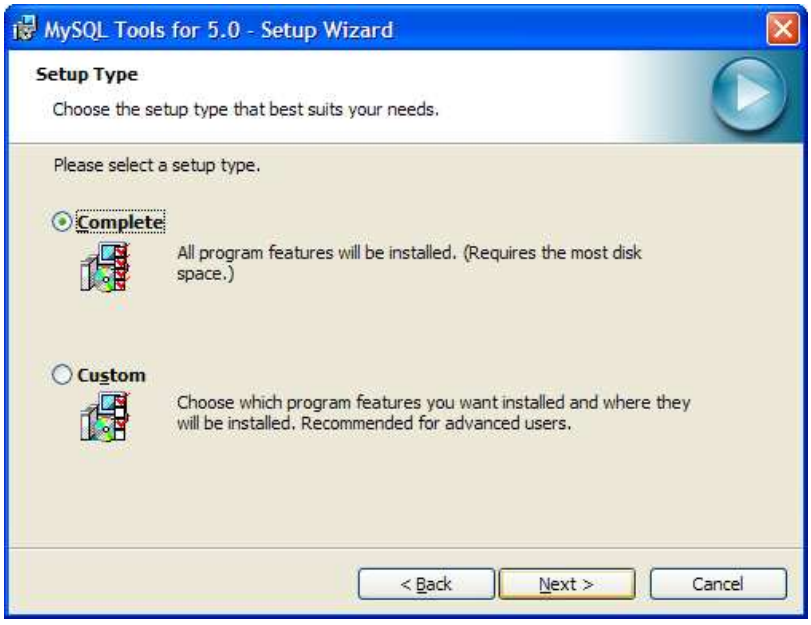


Figura 3.67.- Tipo de instalación según las necesidades

5. Seleccionar *Install* para iniciar la instalación.

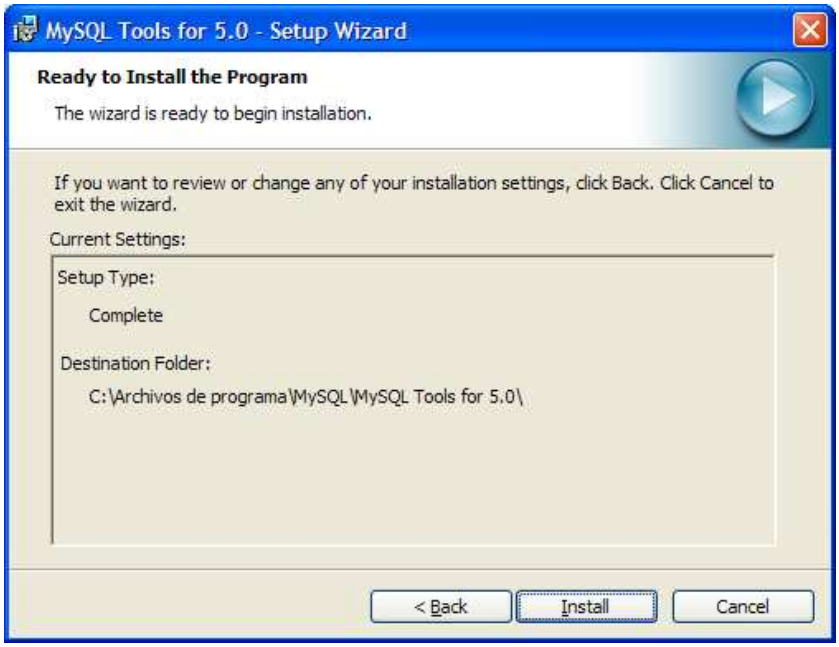


Figura 3.68.- Inicio de la instalación MySQL Tools

6. Finalmente la instalación ha sido realizada satisfactoriamente.

3.6.11.5 Configuración del cliente SSH MySQL

1. Clic en Inicio en la computadora del cliente VPN
2. Seleccionar todos los programas.
3. Seleccionar MySQL
4. Seleccionar MySQL Administrador
5. Ingresar al servidor remotamente indicando los siguientes parámetros.

Dirección IP del Servidor:	192.168.20.114
Puerto	3306
Usuario:	xavier
Contraseña:	********

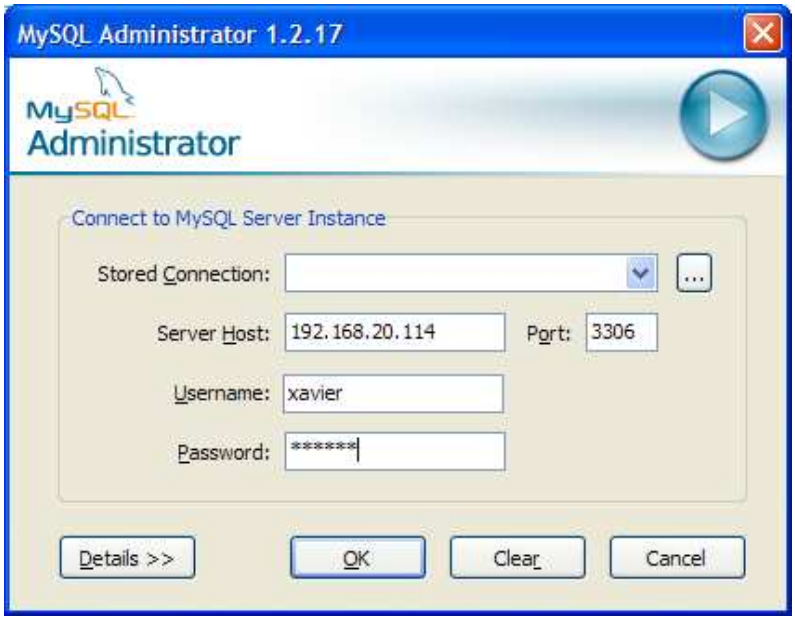


Figura 3.69.- Conexión desde el cliente VPN hacia el servidor Base de Datos

En MySQL para realizar una conexión remota se necesita conectar a través del **puerto 3306**

3.7 PRUEBA DE ACTIVIDAD DE LA DMZ

No se ha configurado un servidor de DNS por lo cual el ingreso a los servidores se realiza a través de su dirección IP pública

3.7.1 SERVICIO WEB

Ingreso a la página principal

Digitar la dirección IP del servidor http://172.31.42.65

Figura 3.70.- Ingreso a la página de inicio

3.7.2 SERVICIO DE CORREO

Envío de correo

Digitar la dirección IP del servidor http://172.31.42.180/webmail. Ingresar la cuenta de usuario que previamente se creo en el servidor

Figura 3.71.- Ingreso a cuenta de correo

Escribir un correo y enviar a otra cuenta de correo.

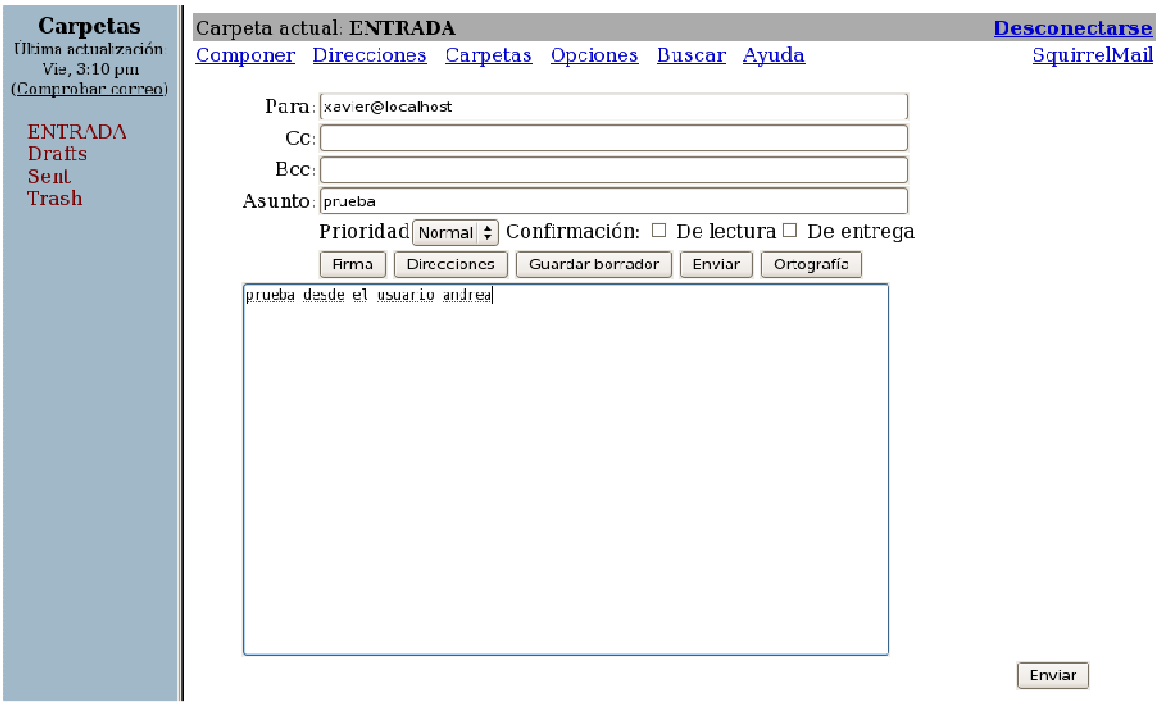


Figura 3.72.- Envío de mensaje de correo

Prueba de recepción de correo

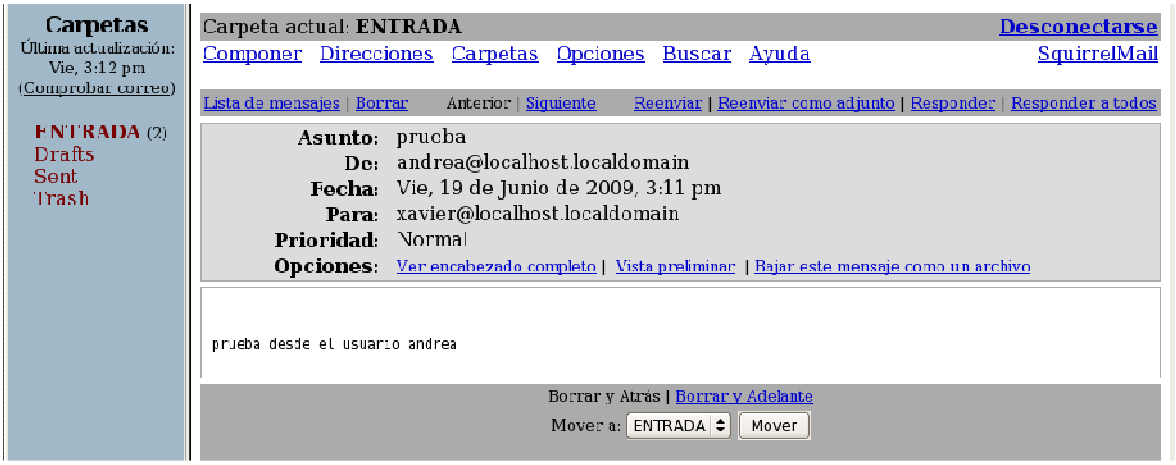


Figura 3.73.- Recepción de mensajes

3.8 PRUEBA DE SEGURIDAD DMZ

Las pruebas permiten conocer si la Zona Desmilitarizada está cumpliendo con su función, para aquello se realizará telnet a los servidores y la red interna

Telnet al Firewall

El firewall puede ser administrado desde el Internet, es por está razón que el

puerto 80 está abierto.

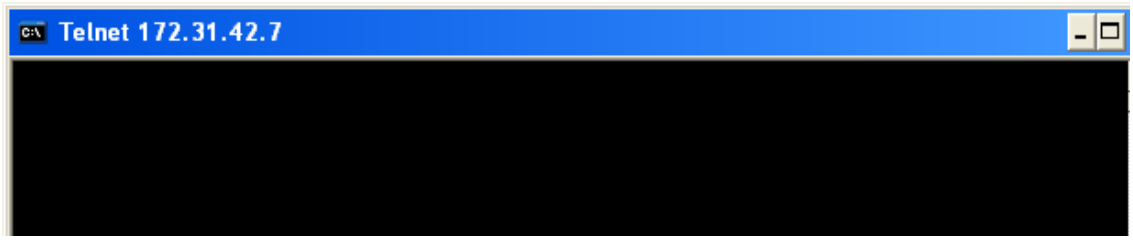


Figura 3.74.- Telnet al Firewall por el puerto 80

Telnet desde la red Internal

Dirección IP de usuario1

Figura 3.75.- Dirección IP del usuario1 de la red Internal

Telnet hacia el servidor de Correo al puerto 21 no es posible por políticas de seguridad.

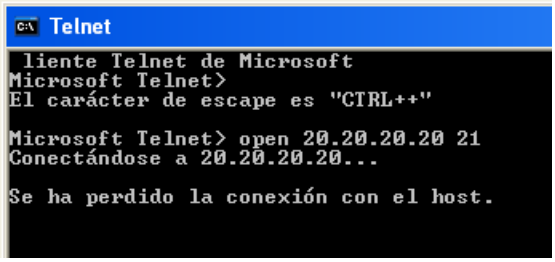


Figura 3.76.- Telnet desde un usuario al puerto 21 al servidor de Correo

Telnet hacia el servidor Web al puerto 21 no es posible por políticas de seguridad; puesto que el único que tiene acceso a realizar actualizaciones desde la red internal es el WebMaster.

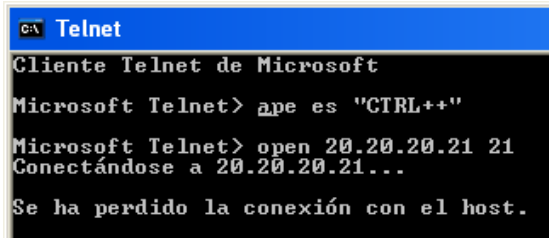


Figura 3.77.- Telnet desde un usuario al puerto 21 al servidor Web

Telnet hacia el servidor de Base de Datos por el puerto 3306 es posible porque el servidor MySQL utiliza este puerto para comunicarse remotamente.

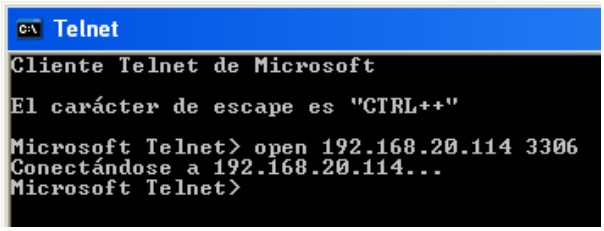


Figura 3.78.- Telnet desde un usuario al puerto 3306 al servidor Base de Datos

Telnet desde la WAN

Dirección IP de usuario

Figura 3.79.- Dirección IP del usuario1 de la red Internal

Telnet hacia el servidor de Correo y al servidor Web al puerto 21 no es posible por políticas de seguridad.

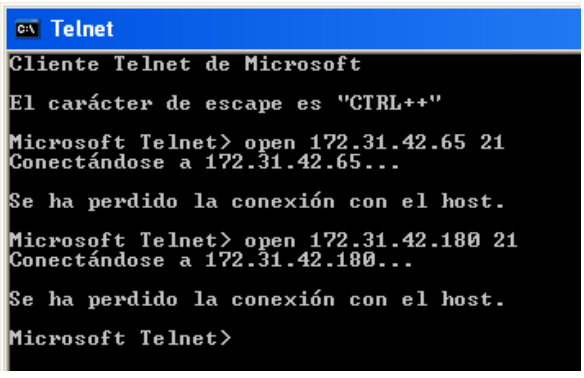


Figura 3.80.- Telnet al servidor de correo y al servidor Web por el puerto 21

Telnet hacia el servidor de Base de Datos por el puerto 3306 no es posible porque la red Internal no es visible al Internet

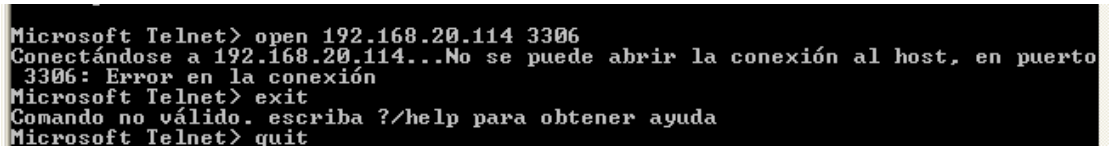


Figura 3.81.- Telnet al servidor de Base de Datos al puerto 21

Telnet hacia el servidor de Correo y al servidor Web al puerto 80 es posible porque el puerto está abierto en las políticas de seguridad.

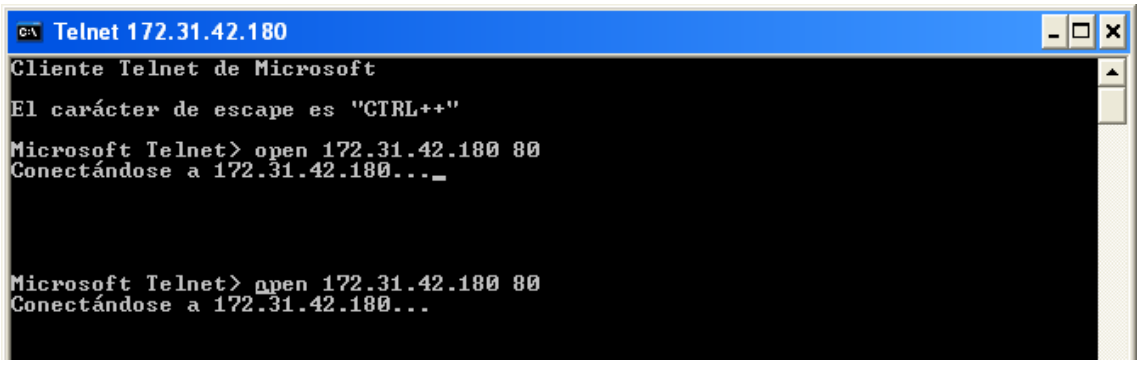


Figura 3.82.- Telnet al servidor de Correo y Web al puerto 80

3.9 PRUEBA DE ACTIVIDAD DE VPN

3.9.1 CONEXIÓN DEL HOST

- Dentro de la aplicación de FortiClient incluye una sección de monitoreo en donde se puede observar cómo se encuentra la conexión

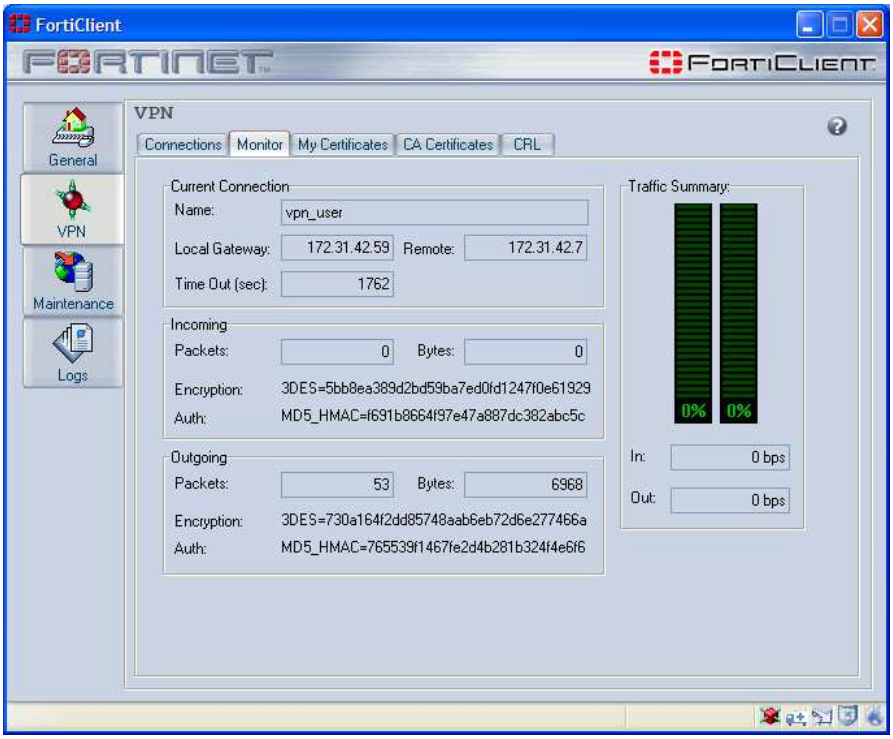


Figura 3.83.- Monitoreo de la conexión desde PC FortiClient

- Realizar un ping a la interfaz internal porque el objetivo de la VPN es ingresar al servidor de correo

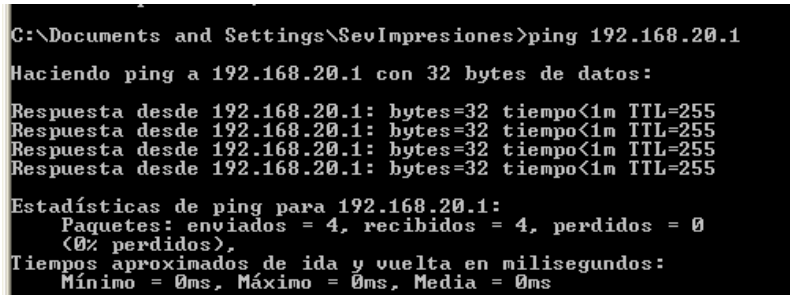


Figura 3.84.- Ping hacia la interfaz Internal

- Monitorear la conexión con el cliente VPN, desde el equipo FortiGate.

  Clic sobre *VPN*

  Seleccionar *IPSEC*, clic sobre la pestaña *Monitor*

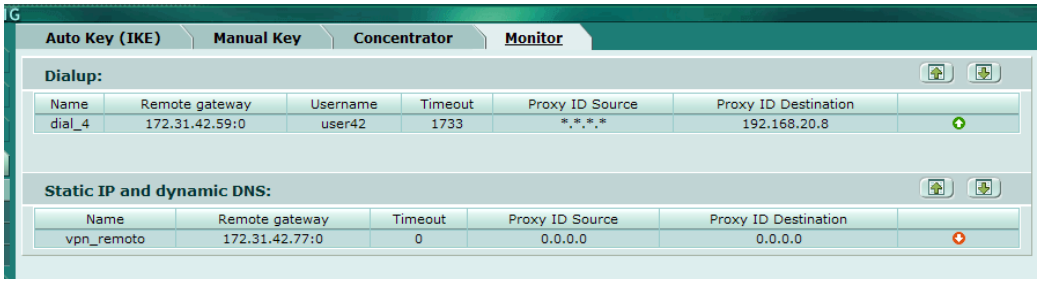


Figura 3.85.- Monitoreo de la conexión desde el Firewall FortiGate

- Abrir la aplicación MySQL Administrador y seleccionar la base que se desea modificar

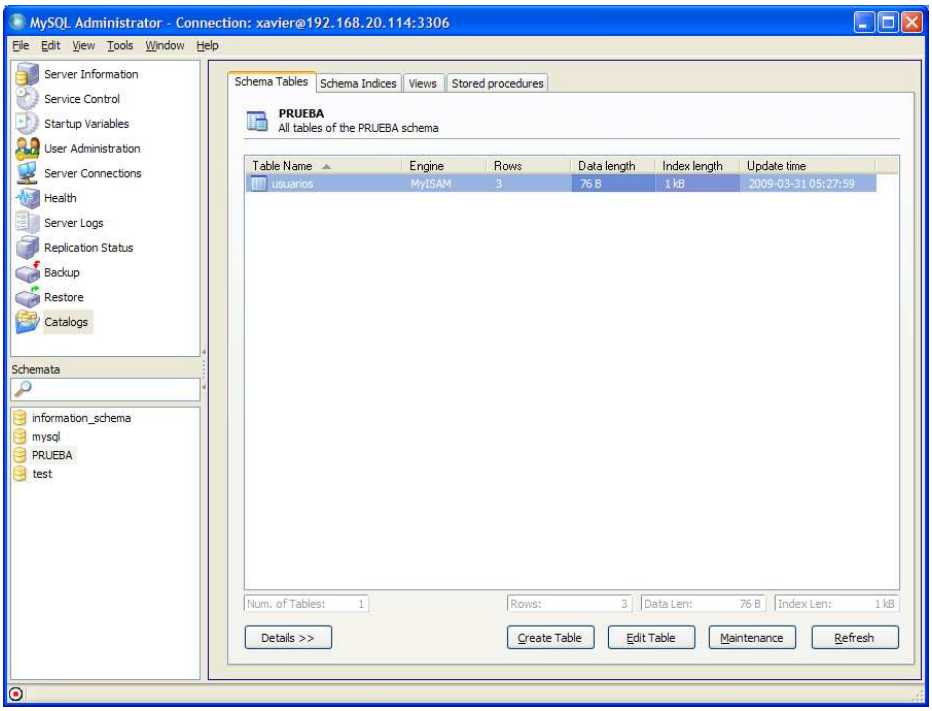


Figura 3.86.- Selección de Base de Datos a modificar en el cliente

- Insertar un nuevo campo en la base de datos PRUEBA

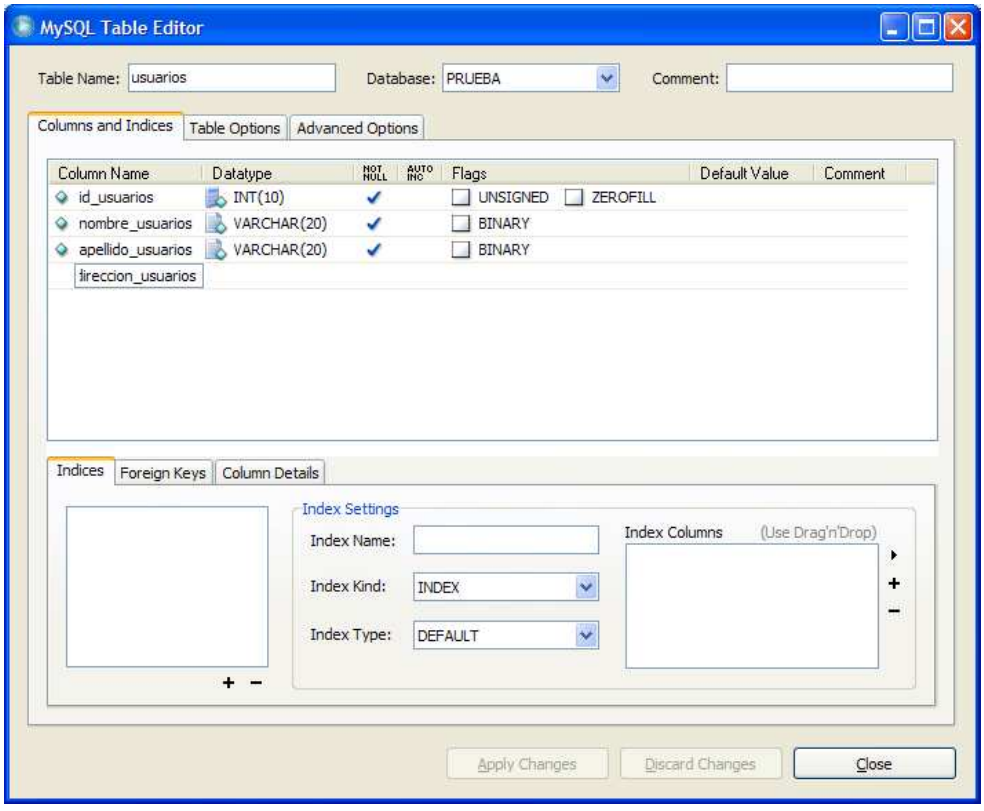
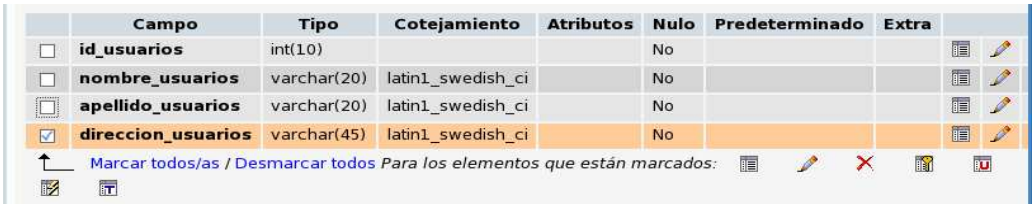


Figura 3.87.- Inserción de nuevo campo en la base de datos PRUEBA

- Revisar si el cambio que se realizó desde el cliente VPN se ve reflejado en el servidor



	Campo	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra	
☐	id_usuarios	int(10)			No			
☐	nombre_usuarios	varchar(20)	latin1_swedish_ci		No			
☐	apellido_usuarios	varchar(20)	latin1_swedish_ci		No			
☑	direccion_usuarios	varchar(45)	latin1_swedish_ci		No			

Marcar todos/as / Desmarcar todos *Para los elementos que están marcados:*

Figura 3.88.- Revisión de los cambios en el servidor

CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Una red perimetral o DMZ permite proteger los servicios privados puesto que éstos son un punto vulnerable dentro de una organización.
- La implementación de una VPN permite realizar una conexión a bajo costo de forma segura, permitiendo al administrador realizar cambios en el servidor de modo remoto y fiable.
- El conjunto completo que forma FortiGate 60 permite además proteger la red de ataques provenientes del Internet (hackers) al establecer políticas de seguridad en cuanto al acceso y uso de la red ofreciendo un mejor rendimiento para el lugar de trabajo.

4.2 RECOMENDACIONES

- Las políticas que se establecen en el firewall deben ser analizadas para así evitar conflictos con las necesidades de los usuarios de la organización.
- Después de realizar alguna actualización en la configuración del firewall FortiGate 60 y en el cliente VPN a través de FortiClient es necesario obtener un respaldo para proteger futuros cambios erróneos.
- No olvidar las claves que se generan tanto para el servidor como para el cliente VPN.
- La renovación de la licencia del firewall FortiGate 60 es necesaria para su buen funcionamiento.
- Antes de adquirir el equipo se debe verificar que lo que ofrece el fabricante, se ajuste a las necesidades de la organización.

GLOSARIO

A

AD HOC: en redes de comunicación, una red ad hoc es aquella (especialmente inalámbrica) en la que no hay un nodo central, sino que todos los ordenadores están en igualdad de condiciones. Ad hoc es el modo más sencillo para el armado de una red.

ADSL: son las siglas de Asymmetric Digital Subscriber Line ("Línea de Abonado Digital Asimétrica"). ADSL es un tipo de línea DSL. Consiste en una línea digital de alta velocidad, tecnología de acceso a Internet de banda ancha.

Aggresive Mode: Es una manera de establecer un canal de seguridad durante la fase uno del IPSec cuando el par (peer) VPN usa su identificación como parte del proceso de autentificación. Se llama también Modo principal (main mode)

ALL-IP: es un amplio término que se refiere a la evolución de la actual infraestructura de redes de telecomunicación y acceso telefónico con el objetivo de lograr la congruencia de los nuevos servicios multimedia (voz, datos, video...) en los próximos 5-10 años.

B

Backbone: La palabra backbone se refiere a las principales conexiones troncales de Internet.. El término backbone también se refiere al cableado troncal o subsistema vertical en una instalación de red de área local que sigue la normativa de cableado estructurado.

Bastion Host: en español anfitrión bastión, es un ordenador en una red que ofrece un único punto de entrada y salida a Internet desde la red interna y viceversa.

BGP: es un protocolo mediante el cual se intercambian prefijos los ISP registrados en Internet.

Bootear: se refiere a modificar el orden de arranque de los dispositivos jlmacenamiento (DVD, CD, Disco Duro, Disquetes, etc).

Bugtraq: es una lista de correo electrónico dedicada a temas sobre la seguridad informática. Los temas tratados son los nuevos debates acerca de las vulnerabilidades, métodos de explotación, y cómo solucionarlos.

C

CA, CERTIFICADO DE AUTORIDAD: (Certificate Authority) Sirve para las compañías que publican certificados digitales para validar la identidad de una persona o de una entidad en un intercambio en línea.

CH

Chargen: (Generador de carácteres) es un programa informático para sistemas operativos basados en Unix que actúa de servidor de caracteres ofrecido por Inetd en el puerto 19 con los protocolos TCP y UDP. Es utilizado para comprobar el estado de algunas conexiones de red.

D

Datagrama: es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el equipo receptor, de manera independiente a los fragmentos restantes.

DDOS: (Distributed Denial Of Service Attack) o Ataque de Denegación de Servicio Distribuido es un tipo especial de DoS consistente en la realización de un ataque conjunto y coordinado entre varios equipos (que pueden ser cientos o miles) hacia un servidor víctima

Daemon: es un tipo especial de proceso informático que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario (es un proceso no interactivo).

DHCP: Dynamic Host Configuration Protocoles un protocolo de red que permite a

los nodos de una red IP obtener sus parámetros de configuración automáticamente.

DMZ: En seguridad informática, una zona desmilitarizada (DMZ) o red perimetral es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

DNAT: (Destination Network Address Translation), emplea para efectuar traducciones de direcciones de red de destino que significa que se emplea para reescribir la dirección IP de destino de un paquete.

DNS: Sistema de Nombre de Dominio (Domain Name System).

E

E-Mail Bombing: En Internet, e-mail bombing (bomba de correo electrónico) es una forma de red de abuso que consiste en el envío de grandes volúmenes de correo electrónico a una dirección en un intento de desbordar el buzón de correo o saturar el servidor que la dirección de correo electrónico está alojado en una denegación de servicio ataque.

Ethernet: es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos.

F

Firmware: o Programación en Firme, es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria tipo ROM, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo

Floodear: significa escribir varios Post (envios) seguidos, repetir líneas iguales por más de tres veces, todo lo que implica inundación. Realmente, el Post múltiple (ya sean dos post seguidos, tres, cuatro o un millón), sería flood con independencia del tiempo que transcurra entre ambos.

FTP: Protocolo de Transferencia de Datos (File Transfer Protocol)

G

Gateway.- es un equipo que permite interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos.

GNOME: es un entorno de escritorio para sistemas operativos de tipo Unix bajo tecnología X Window. Forma parte oficial del proyecto GNU. Nació como una alternativa a KDE.

H

Hacker: es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Se suele llamar hackeo y hackear a las obras propias de un hacker.

HEAD END (CABECERA DE CABLE): Lugar en un sistema de cable o red de banda ancha coaxial donde se origina la programación y comienza la red de distribución.

Host: El término host (equipo anfitrión) en informática o computación puede referirse a un dispositivo de la red que ofrece servicios a otros ordenadores conectados a dicha red

HTTP: (HyperText Transfer Protocol) o Protocolo de Transferencia de Hipertexto es un conjunto de reglas que rigen la transferencia de datos, este protocolo es usado en la Web.

I

ICMP: (Internet Control Message Protocol) es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar

mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado

IKE: (Internet Key Exchange) Es un método automático de intercambiar llaves (keys) de autentificación y de encriptación de IPsec entre dos servidores seguros.

IMAP: Protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet.

IPsec: es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

IP Spoofing: Es una técnica usada para obtener acceso no autorizado a las computadoras, en donde el 'intruso' envía mensajes a una computadora con una dirección IP indicando que el mensaje viene de una computadora confiable

IRC: (Internet Relay Chat) es un protocolo de comunicación en tiempo real basado en texto, que permite debates y que está clasificado dentro de la Mensajería instantánea

J

JITTER: Es la variación de los retardos (delay), es un parámetro crítico en las aplicaciones de tiempo real, (Telefonía IP / video)

K

Kernel: Es la parte fundamental de un sistema operativo. Es el software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema

KDE: Entorno de Escritorio K, es un entorno de escritorio e infraestructura de desarrollo para sistemas Linux., KDE llena la necesidad de un escritorio amigable similar a los escritorios de Windows.

L

L2TP: (Layer 2 Tunneling L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado.

M

Malware: es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware.

MTA es una sigla en inglés que significa Mail Transport Agent (Agente de Transporte de Correos).

Multidifusión (inglés multicast) es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen.

N

NAT: (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por rotures IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados

Netfilter: es un servicio completo de Administración de Accesos y Filtrado de Contenido de Internet, que elimina páginas de pornografía, drogas y violencia garantizando un alto nivel de seguridad a sus usuarios.

NEWSGROUP: Los grupos de noticias (newsgroups en inglés) son un medio de comunicación dentro del sistema Usenet en el cual los usuarios leen y envían

mensajes textuales a distintos tablones distribuidos entre servidores con la posibilidad de enviar y contestar a los mensajes.

NFS: es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local

NODO: En informática, un nodo es "Punto de intersección o unión de varios elementos que confluyen en el mismo lugar". Ejemplo: en una red de ordenadores cada una de las máquinas es un nodo, y si la red es Internet, cada servidor constituye también un nodo.

P

PAYLOAD: La palabra "payload" en inglés significa contador, pagador, pago de carga, etc. En términos de virus informáticos, payload son el o los efectos nocivos o hasta irreparables, que ocasionan cualquier especie viral a los sistemas de los equipos que infectan, sean estos servidores, estaciones de red o computadoras domésticas.

PEER TO PEER: Una red peer-to-peer (P2P) o red de pares, es una red de computadoras en la que todos o algunos aspectos de esta funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre si. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red.

POP3: Post Office Protocol en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto es para recibir correo y no para enviar y sus predecesores permite que los usuarios con conexiones intermitentes (tales como las conexiones módem), descarguen su correo electrónico cuando se encuentren conectados de tal manera que puedan ver y manipular sus mensajes sin necesidad de permanecer conectados.

PPPoE: (Protocolo Punto a Punto sobre Ethernet) es un protocolo de red para la

encapsulación PPP sobre una capa de Ethernet.

PPP: protocolo punto a punto una de las formas más habituales de conectarse a Internet de un particular con su proveedor de acceso a través de un MODEM telefónico. Ocasionalmente también es utilizado sobre conexiones de banda ancha.

PPTP: Microsoft, conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN.

Q

QoS: Calidad de Servicio (Quality of Service,) son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio.

R

RDSI: (Red Digital de Servicios Integrados) es un sistema de conexiones telefónicas digitales que se ha diseñado para el envío de voz, vídeo y datos simultáneamente durante digital ordinario o líneas de teléfono

RFC 2373: Esta especificación define la arquitectura de abordar el período de investigación de la versión 6 de protocolo [IPV6]. El documento incluye el tratamiento de Ipv6, las representaciones de texto de direcciones IPv6, la definición de Ipv6, direcciones unicast, anycast y direcciones multicast.

RFC 2374: Esta especificación sustituye a RFC 2073, "Un IPv6 Unicast-base”
Los principales cambios incluyen la eliminación del registro bits, ya que no son necesarios para la vía de agregación, el apoyo de EUI-64 interfaz basada en identificadores, el apoyo del proveedor y el intercambio basado en la agregación, separación del público y de la topología de sitio, y las nuevas terminología basada en la agregación.

Router: Los Rotures son dispositivos electrónicos encargados de encaminar y

transmitir paquetes de información entre diferentes redes informáticas. Los cuales establecen comunicaciones externas y de convertir los protocolos utilizados en las LAN en protocolos de WAN y viceversa, estos dispositivos trabajan a nivel de capa 3

RTP: (Real Time Protocol - Protocolo de Tiempo Real). Protocolo empleado para transmitir información en tiempo real como audio y video para una videoconferencia.

S

SCRIPT: En informática, un script es un guión o conjunto de instrucciones. Permiten la automatización de tareas creando pequeñas utilidades. Es muy utilizado para la administración de sistemas UNIX. Son ejecutados por un intérprete de línea de órdenes y usualmente son archivos de texto. También un script puede considerarse una alteración o acción a una determinada plataforma.

SIP: Session Initiation Protocol (SIP o Protocolo de Inicio de Sesiones) es un protocolo, con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos online y realidad virtual

Smurf, es un ataque de denegación de servicio que utiliza mensajes de ping al broadcast con spoofing para inundar flood un objetivo (sistema atacado).

Spam: correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor es la parte fundamental de un sistema operativo.

Spamming: El spamming es el abuso de cualquier tipo de sistema de mensajes electrónicos y, por extensión, cualquier forma de abuso en otros medios como spam en mensajería instantánea, en foros, en blogs, en buscadores, en mensajes en teléfonos móviles, etc.

Spyware: es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

SSH: (Secure Shell) Es una aplicación que permite a los usuarios registrar en una computadora remota y ejecutar comandos con seguridad.

SSL/TLS: Secure Sockets Layer (SSL) y Transport Layer Security (TLS) Seguridad de la Capa de Transporte, su sucesor, son protocolos criptográficos que proporcionan comunicaciones seguras en Internet.

Switch: es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI

T

TCP: es uno de los protocolos fundamentales en Internet. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

Telnet: (TELecommunication NETwork) es el nombre de un protocolo de red (y del programa informático que implementa el cliente) que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. El puerto que se utiliza generalmente es el 23.

U

UDP: (User Datagram Protocol) es uno de los dos protocolo de transporte más utilizado sobre IP, es un protocolo basado en el intercambio de datagrama a través de la red sin que se haya establecido previamente una conexión

UIT: Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.

UNIs ETHERNET: En una interfaz de usuario a red (UNI, User-to-Network Interfaces). El cual es un método de señalización estándar para que se comuniquen las estaciones finales y los conmutadores ATM.

Unix: es un sistema operativo portable, multitarea y multiusuario.

UPnP: Universal Plug and Play Conectar y Usar Universal, es una arquitectura softwarenix: es un sistema operativo portable, multitarea y multiusuario.

UP LINK: El uplink de un concentrador de red (hub), boca destinada a la conexión de dos concentradores por medio de un cable directo.

V

VPN: red privada virtual se puede interpretar como un servicio de acceso remoto a la red y recursos de la empresa.

Voip: o Telefonía IP, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Internet Protocol).

BIBLIOGRAFÍA

Libros o Manuales

Tema: Configuración Inicial FortiGate 60

Fortinet, Guía de Instalación FortiGate 60, FortiGate-60 Installation Guide, Enero 2005

Tema: VPN

Fortinet, Guía de Administración FortiGate 60, FortiGate-60 Administration Guide, Julio 2004

Tema: DMZ

Fortinet, Ejemplos de Configuración FortiGate SOHO y SMB, FortiGate Configuration Example –SOHO and SMB, Diciembre 2004.

Tesis

Tema: Configuración Inicial FortiGate 60

Fiallos Carina, Toro Susana. “DISEÑO E IMPLEMENTACIÓN DE UNA RED SEGURA PARA EL LABORATORIO DE TECNOLOGÍAS DE LA INFORMACIÓN”, Abril 2007

Tema: DMZ

Chipantiza, Verónica. DISEÑO E IMPLEMENTACIÓN DE UNA DMZ EN EL LABORATORIO DE TECNOLOGÍAS DE LA INFORMACIÓN “LTI”, Abril 2008