PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

SEDE AMBATO

ESCUELA DE INGENIERIA EN SISTEMAS

Tema:

"ESTUDIO E IMPLEMENTACIÓN DE DISPOSITIVOS DE SEGURIDAD EN LA RED DEL CAMPUS UNIVERSITARIO DE LA PUCESA"

Autores:

ORTIZ PAREDES WILLIAN FRANKLIN
VILLALBA MORALES WILLIAN RAUL

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
BIBLIOTECA

Asesor:

ING. VICTOR CHUNCHA

Ambato – Ecuador

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
BIBLIOTECA

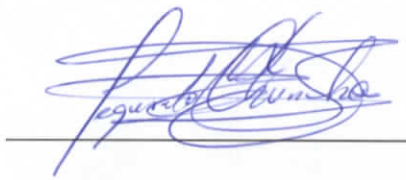
PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
SECRETARIA
ESCUELA DE INGENIERIA DE SISTEMAS
06-11-07

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE AMBATO

ESCUELA DE INGENIERIA DE SISTEMAS

DISERTACION DE GRADO PREVIA A LA OBTENCION DEL TITULO DE INGENIERIA DE SISTEMAS

"ESTUDIO E IMPLEMENTACIÓN DE DISPOSITIVOS DE SEGURIDAD EN LA RED DEL CAMPUS UNIVERSITARIO DE LA PUCESA"

DIRECTOR: 

Ing. Víctor Chuncha

ORTIZ PAREDES WILLIAN FRANKLIN
VILLALBA MORALES WILLIAN RAUL

DECLARACIÓN DE AUTENTICIDAD

Y RESPONSABILIDAD

Yo, Ortiz Paredes William Franklin portador de la cédula de ciudadanía No. *180346974-9* declaro que los resultados obtenidos en la investigación que presento como informe final, previo la obtención del título de Ingeniero en Sistemas son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola y exclusiva responsabilidad legal y académica.

Ortiz Paredes William Franklin
CI. 180346974-9

DECLARACIÓN DE AUTENTICIDAD

Y RESPONSABILIDAD

Yo, Villalba Morales William Raúl portador de la cédula de ciudadanía No. *180348590-1* declaro que los resultados obtenidos en la investigación que presento como informe final, previo la obtención del título de Ingeniero en Sistemas son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola y exclusiva responsabilidad legal y académica.



Villalba Morales William Raúl
CI. 180348590-1

Resumen

El tema de Disertación lleva como título "Estudio e implementación de Dispositivos de seguridad en al red del Campús Universitario de la PUCESA" y esta conformado por cuatro capítulos.

Capítulo I: se encuentra el proyecto de la investigación, en el que se explican los objetivos a conseguir, basados en el problema de la red, y también se indica la estructura de la Tesis

Capítulo II: Marco teórico, en él se estudian, la Seguridad Informática, Redes, y el Firewall. Conocimientos que son necesarios para la implementación del Firewall dentro de la red.

Capítulo III: Desarrollo del proyecto, en donde se presenta un estudio de la red, y los requerimientos indispensables para la funcionalidad del Proyecto.

Capítulo IV: Conclusiones, Recomendaciones y Anexos. Finalmente las conclusiones a las que se llegan luego de realizar el estudio, Recomendaciones para la funcionalidad, como también se incluye el Manual de usuario para un uso apropiado del dispositivo

Abstract

The title of the dissertation is: "Study and Implementation of dispositives of Security in the PUCESA Campus Network" It's divided into four chapters:

Chapter I: We present the research project and the objectives we want to accomplish in relation to the problem the University Network has. On this chapter we also present the thesis structure.

Chapter II: The Theory Framework to study the computing security, network and firewall. This information is necessary for the correct implementation of the firewall in the network.

Chapter III: The project focus on the study of the network itself, and the necessary requirements for the project functionality

Chapter IV: Conclusions, recommendations and appendices. In this chapter we include the conclusion we have drawn once the present study finished, the recommendation for functionality as well as the user's manual for the appropriate use of the dispositive.

TABLA DE CONTENIDOS

CAPITULO I

PROYECTO DE LA INVESTIGACIÓN

1. Introducción ---------- 1
2. Planteamiento del Problema ---------- 1
2.1. Problema ---------- 1
2.2. Ploblematización ---------- 1
3. Delimitación ---------- 2
4. Importancia y Justificación ---------- 2
4.1. Importancia ---------- 2
4.2 Justificación ---------- 2
5. Objetivos ---------- 2
5.1. Objetivo General ---------- 2
5.2. Objetivos Especificos ---------- 2
6. Marco Teórico ---------- 3
7. Hipótesis ---------- 3
8. Aspectos Metodólogicos ---------- 3
8.1. Fundamentos Teóricos ---------- 3
8.2. Métodos de Investigación ---------- 4

CAPITULO II

MARCO TEORICO

Seguridad Informática

2.1. Seguridad Informática ---------- 5
2.1.1. Concepto ---------- 6
2.1.1.1. Caracteristicas de un Sistema seguro ---------- 7
2.1.1.2. Objetivos de la seguridad Informática ---------- 7
2.1.1.2.1. Hardware ---------- 7
2.1.1.2.2. Software ---------- 8
2.1.2. ¿Qué queremos Proteger ---------- 8
2.1.2.1. Tópicos errónios comunes aceca de la Seguridad ---------- 8

2.1.2.2. Importancia de la Seguridad ---------- 9
2.1.2.3. Seguridad en Internet ---------- 9
2.1.2.4. Puntos que son causantes de daños dentro de la Red ---------- 10
2.1.2.4.1. Hoax ---------- 10
2.1.2.4.2. Spam ---------- 10
2.1.2.4.3. ¿Qué es el Bulo? ---------- 10
2.1.3. Seguridad del entorno de operaciones ---------- 10
2.1.3.1. Acceso físico 10
2.1.3.2. Desastres naturales 11
2.1.3.3. Desastres del entorno 11
2.1.3.5. Protección de los datos ---------- 12
2.1.3.5.1. Backups ---------- 12
2.1.4. Métodos y herramientas de ataque ---------- 12
2.1.4.1. Atacantes 13
2.1.4.2. Vulnerabilidades 13
2.1.4.3. Amenazas y vulnerabilidades ---------- 13
2.1.4.3.1. Malware ---------- 14
2.1.4.3.2. Virus ---------- 14
2.1.4.3.3. Los gusanos informáticos ---------- 15
2.1.4.3.4. Un cabballo de Troya ---------- 15
2.1.4.3.5. EL spyware ---------- 15
2.1.4.3.6. Exploit ---------- 15
2.1.4.3.7. Rootkit ---------- 16
2.1.4.4. Ataques Potenciales ---------- 16
2.1.4.4.1. Ingeniería social 16
2.1.4.4.2. Shoulder Surfing 16
2.1.4.4.3. Masquerading 16
2.1.4.4.4. Basureo 17
2.1.4.5. Actos Delictivos ---------- 17
2.1.4.5.1. Hackers ---------- 17
2.1.4.6. Tipos de ataques a la red ---------- 18
2.1.4.6.1. Ataques de escaneo: 18
2.1.4.6.2. Ataques de Modificación-daño 18

2.1.4.6.3. Ataques por vulnerabilidades 19
2.1.4.6.4. Ataque por Fragmentación: 19
2.1.4.6.5. Ataques de autentificación 20
2.1.4.6.6. Ataques DoS (denegación de servicio) 21
2.1.5. Seguridad de la red ----------21
2.1.5.1. General !Cuidados con los Clics¡ ----------22
2.1.5.2. Privacidad ----------22
2.1.5.3. Protección ----------23
2.1.6. Vulnerar Para Proteger 23
2.1.6.1. Access Control Lists (ACL) 23
2.1.6.2. Wrappers 24
2.1.6.3. Detección de Intrusos en Tiempo Real 24
2.1.6.4. Call Back 25
2.1.6.5. Sistemas Anti-Sniffers 25
2.1.7. Amenazas internas 25
2.1.8. Amenazas externas 25
2.1.8.1. Defensa en profundidad 26
2.1.9. Politicas de uso aceptable 26

2.2. Redes

2.2.1.1. Ventajas de las redes informáticas 28
2.2.1.2. Tipos de Redes informáticas según el protocolo 29
2.2.1.2.1. Protocolos de bajo nivel 29
2.2.1.2.2. Protocolos de red 29
2.2.1.2.3. Comunicaciones en red 32
2.2.2. Modelo OSI 32
2.2.2.1. Estructura del Modelo OSI 34
2.2.2.2. Estructura multinivel 34
2.2.2.3. Puntos de accseso 35
2.2.3. Nivel Físico 36
2.2.4. Nivel de Enlace de Datos 36
2.2.5. Nivel de Red 39
2.2.6. Nivel de Transporte 40

BIBLIOTECA

2.2.7. Nivel de Sesión 42
2.2.8. Nivel de Presentación 43
2.2.9. Nivel de Aplicación 44
2.2.10. Relaciones entre los niveles del modelo OSI 44
2.2.11. Paquetes de datos y el modelo OSI 46
2.2.12. Dispositivos de Red 47
2.2.12.1. Router 47
2.2.12.2. Firewall 47
2.2.12.3. Switch 48
2.2.13. Enrutamiento 48
2.2.13.1. Ventajas y Desventajas de enrutar 49
2.2.13.2. Clases de Enrutamientos 49
2.2.13.2.1. Procedimiento de enrutamiento 49
2.2.13.2.2. Tablas de enrutamiento 51
2.2.14. Direccionamiento de paquetes 51
2.2.14.1. Cómo dirigir los paquetes 52

2.3. Firewall (Corta Fuegos)

2.3.1. Características Principales ----- 53
2.3.2. Firewall, la muralla defensiva de un PC ----- 54
2.3.3. Como funcionan los Firewall ----- 55
2.3.4. Tipos de peligros que pueden evitar un Firewall ----- 55
2.3.5. Arquitecturas del Firewall ----- 55
2.3.5.1. Host Doble conexión (Dual-Homed Gateway) ----- 55
2.3.5.2. Filtrado de Host (Screened Host) ----- 56
2.3.5.3. Filtrado de Subred (Screened Subnet) ----- 57
2.3.6. Tecnologías de Firewall ----- 58
2.3.7.1. Tipos de Firewall ----- 59
2.3.7.1. Firewall de software ----- 60
2.3.7.2. Firewall de Hardware ----- 61
2.3.7.3. Firewall a Nivel de Red ----- 61
2.3.7.4. Firewall a Nivel de Aplicación ----- 62
2.3.7.5. Firewall a Nivel de Circuito ----- 63

2.3.8. Resumen de los tres tipos de firewall ---------- 654
2.3.9. Beneficios de un firewall en Internet ----------65
2.3.10. Configuración de Firewall ----------65

Capitulo III

Desarrollo del Proyecto

3.1. Análisis de la Implementación----------66
3.1.1. Análisis y estudio de la Red actual de la PUCESA ----------66
3.1.2. Análisis de reqisitos sobre la implementación----------69
3.1.3. Análisis de requerimentos del Hardware----------69
3.1.4. Funcionalidad del Proyecto----------69
3.1.5. Restriciones----------71
3.1.6. Diagrama de la red luego de la implementación ----------72

Capitulo IV

VALIDACIÓN Y VERIFICACIÓN DE RESULTADOS

Conclusiones y recomendaciones----------75
Bibliografía----------77
Glosario----------79
Anexos----------81

TABLA DE GRAFICOS

Figura 2.1 Esquema de los objetos que actúan en la Seguridad Informática ---- 5
Figura 2.2 Esquema de los elementos que actuan en la Seguridad Informática ---- 6
Figura 2.3 Esquema de los elementos de ataque ---- 12
Figura 2.4 Esquema de una Red de Ordenadores ---- 27
Figura 2.5 Esquema de la Estructura Multinivel del Modelo OSI ---- 34
Figura 2.6 Esquema de la Capa de Enlace de Datos ---- 37
Figura 2.7 Esquema de las Sub capas de la capa de enlace de Datos ---- 38
Figura 2.8 Esquema de las funciones de las Capas del Modelo OSI ---- 45
Figura 2.9 Esquema de los Paquetes de Datos del Modelo OSI ---- 46
Figura 2.10 Esquema del Camino que un Paquete Sigue hacia su destino ---- 49
Figura 2.11 Esquema del Firewall en la Red ---- 52
Figura 2.12 Esquema general del Firewall ---- 54
Figura 2.13 Arquitectura del Host de Doble Conexión ---- 56
Figura 2.14 Arquitectura del Filtrado de Host ---- 56
Figura 2.15 Arquitectura del filtrado de Sub_Red ---- 57
Figura 2.16 Esquema del Firewall de Software ---- 60
Figura 2.17 Esquema del Firewall de Hardware ---- 61
Figura 2.18 Firewall a Nivel de Red utilizando un Ruteador ---- 61
Figura 2.19 Firewall a Nivel de Aplicación ---- 62
Figura 2.20 Firewall a Nivel de Circuito ---- 63
Figura 2.21 Sistema de Firewall de una Empresa ---- 64

INDICE DE TABLAS

Tabla 2.1 Principales Ventajas y Desventajas de Enrutar ----------49
Tabla 2.2 Arquitecturas de Firewall ----------58
Tabla 2.3 Tipos de Firewall----------63

CAPITULO I

PROYECTO DE LA INVESTIGACIÓN

1. Introducción

Con el propósito de obtener seguridad estable en el servidor y por ende en toda la red del campus universitario de la PUCESA, se prevé de un estudio de implementación de dispositivos, como es un Firewall Físico con las características necesarias para obtener una convicción eficaz. Para así poder contrarrestar los ataques de virus y códigos malintencionados, teniendo en cuenta, que el 80% de información que llega a nuestros correos electrónicos es basura, publicidad y virus. Los productos ofrecidos por los fabricantes de Hardware de seguridad pueden resultar no eficaces dentro de una organización sin un correcto estudio de implementación, que es lo que pretendemos brindar en la PUCESA con nuestro trabajo. El estudio que se realice permita seleccionar la alternativa más adecuada y de esta manera implementar dispositivos de seguridad, los cuáles se podrá filtrar contenidos, bloquear URLS y comprobar palabras clave, así como también la gestión de configuración basada en Web y monitorización en tiempo real.

2. Planteamiento del problema.

2.1. Problema

Carencia de un estudio e implementación de Dispositivos de seguridad en la red de la Pontificia Universidad Católica del Ecuador Sede Ambato, la cuál está expuesta a continuos ataques de programas maliciosos que afectan al servidor provocando daños y pérdidas de información.

2.2. Problematización

- Ausencia de una guía práctica para la implementación de dispositivos de seguridad en la red de la PUCESA
- Inexistencia de un dispositivo Físico que contrarreste los ataques de Hackers y virus al servidor de la PUCESA.
- Falta de seguridad en la navegación en Internet en la red del campus universitario.
- Carencia de un filtrado de todos los contenidos como el bloqueo de URLS

3. Delimitación

El estudio e implementación de dispositivos de seguridad en la Pontificia Universidad Católica, Brindará una solución de protección de los equipos de la red contra ataques de virus, hackers, filtrando contenidos, y bloqueo de URLS la cual será implementada en el Centro de Computo en el primer semestre del año académico 2006-2007.

4. Importancia y justificación:

4.1. Importancia

La seguridad es una de las preocupaciones principales del administrador de red. Hay muchas páginas inseguras en Internet y la mayor parte de los usuarios desconocen lo que realmente pasa durante la transmisión de datos, o si éstos pueden venir acompañados de virus o intrusos. Así pues, es necesario realizar un estudio sobre todos los programas y dispositivos necesarios para tener una protección a la red interna, de la otra red, la Internet, mediante el uso de filtros equipados para evitar automáticamente que un usuario no-autorizado ataque al equipo.

La realización del proyecto se enfoca en el servicio de Internet de la Pontificia Universidad Católica del Ecuador, para brindar protección contra programas malignos, y bloqueo de URLS, lo que representa un alto grado de importancia, ya que los continuos ataques al servidor y por ende a la red se reducirán notablemente.

4.2. Justificación

Para la realización de este tema contamos con el tiempo necesario para poder cumplir con todas los objetivos trazados dentro del plan, como también tenemos el conocimiento, la información y la asesoria técnica indispensable para no tener dificultades en el transcurso del desarrollo del proyecto. Además los costos de los dispositivos de seguridad que vamos a necesitar para la implementación del proyecto son accesibles.

5. Objetivos:

5.1. Objetivo general

Realizar un estudio e implementación de un dispositivo de seguridad en la red de la Pontificia Universidad Católica del Ecuador Sede Ambato, contra ataques de

programas maliciosos que permitan proteger al servidor y por ende la información vulnerable de la red.

5.2. Objetivos específicos

- Realizar una Guía Práctica para la implementación de dispositivos de seguridad en la red de la PUCESA
- Implementar un dispositivo físico para lograr que el servidor y la red de la PUCESA esté libre de ataques de virus, Hackers y programas maliciosos
- Bloquear URLS y comprobar palabras Clave.
- Obtener un filtrado de contenidos que llega al servidor de la PUCESA.

6. Marco teórico

Para la realización de este proyecto se analizarán los siguientes temas:

- Seguridad Informática
- Redes
- Configuración de Firewalls

7. Hipótesis

Con el estudio e implementación de un dispositivo de seguridad Físico (Firewall) se logrará obtener una protección para el servidor y toda la red de la PUCESA y así evitar daños a los equipos y pérdida de información.

8. Aspectos metodológicos

8.1. Fundamentos teóricos

Este proyecto de disertación utiliza los siguientes paradigmas:

- Racionalista, ya que este proyecto cuenta con el conocimiento e instrumentos necesarios, es posible llevar a cabo.
- Crítico, ya que transmitir mensajes por medio de los resultados obtenidos y consiguiendo de esta manera resultados positivos en la protección de ataques desde la red a la PUCESA.

8.2. Métodos de investigación

En el proceso de investigación se utilizará el método de la investigación aplicada, también conocida como activa o dinámica, correspondiente al estudio y aplicación de la investigación al problema de protección contra virus y código malicioso que llega al servidor y por ende se expande por toda la red.

Entre los tipos de investigación aplicada utilizaremos la descriptiva, ya que nuestro objeto fundamental será interpretar la realidad de los resultados obtenidos por la Implementación del Firewall.

También utilizaremos la Experimentación Científica ya que utilizaremos experimentación, bajo condiciones estrictamente comprobadas con el objeto de describir los resultados y brindar recomendaciones.

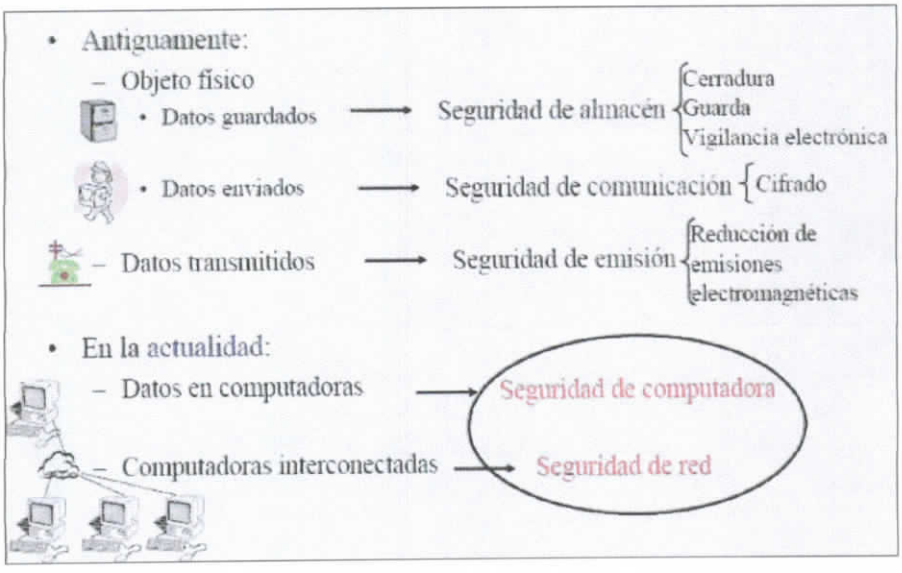
CAPITULO II

MARCO TEORICO

2.1. Seguridad Informática

Se está viviendo la era de la informática y de las comunicaciones. Antes la informática estaba reservada a unos pocos "sabios" el resto de las personas se veían afectadas de manera muy limitada. Con el desarrollo de los computadores personales, la vertiginosa evolución de Internet, la implantación del comercio electrónico y el impulso de la denominada "Sociedad de la Información", todo el mundo habla, sabe y se preocupa de la seguridad en estos ámbitos

Figura 2.1 Esquema de los objetos que actúan en la Seguridad Informática



La facilidad de transmisión de datos, generó nuevas necesidades que siempre estarán presentes en el mundo de las redes informáticas y son básicamente, garantizar la privacidad de los datos, así como también de protegerlos y asegurar su autenticidad al momento de enviarlos a través del Internet. Por lo tanto las necesidades son las que obligan a poner seguridades debido a que el Internet es un servicio que posee millones de usuarios y que crece a un ritmo acelerado, siempre han existido usuarios que en algunos casos por curiosidad les gusta adquirir mayores conocimientos sobre el funcionamiento interno de un sistema, de una computadora, o de una red de computadores y que, con frecuencia se propone como reto poner a prueba la seguridad de los sistemas pero sin buscar su propio beneficio ni el perjuicio de otros.

Mientras que en otros casos existen personas maliciosas con fines de lucro o simplemente con la finalidad de causar daños. Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de sus red a los Expertos de Internet

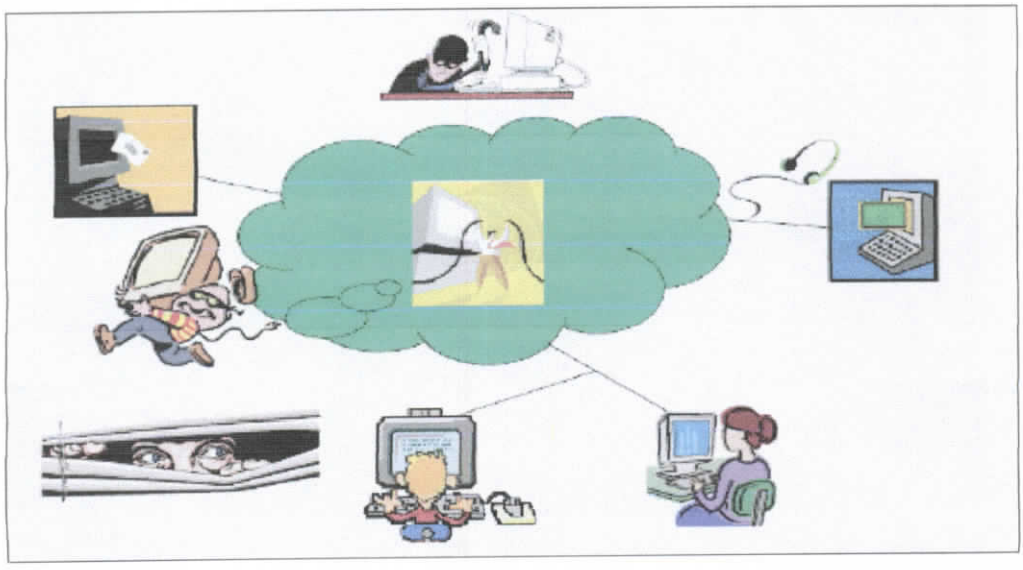
2.1.1. Concepto

La Seguridad Informática es un conjunto de estrategias y técnicas que impiden que ocurran cosas malas. En términos generales, la seguridad puede entenderse como reglas técnicas y actividades destinadas a prevenir, proteger y resguardar lo que es considerando como robo, perdida o daño, ya sea de manera personal, o grupal.

Seguridad es la protección de la información mediante:

- Prevención: Tomar medida para impedir que los elementos sean vistos, dañados o robados
- Detección.- Tomar medidas para detectar cuándo, cómo o quien ha dañado un elemento
- Reacción.-Tomar medidas para recuperar los elementos o recuperar del daño

Figura 2.2 Esquema de los elementos que actúan en la Seguridad Informática



2.1.1.1. Características de un Sistema seguro:

a) Integridad

La integridad se refiere a la seguridad, cuando una información no ha sido alterada, borrada, reordenada, copiada, etc., durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

b) Confidencialidad

La confidencialidad se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de medios, presenta múltiples oportunidades para ser interceptada y copiada: las líneas "pinchadas" la intercepción o recepción electromagnética no autorizada, o la simple intrusión directa en los equipos donde la información está físicamente almacenada

c) Disponibilidad

La disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

2.1.1.2. Objetivos de la Seguridad Informática

En el mundo de la Informática se utiliza habitualmente una división en dos grandes áreas que denominamos Hardware y Software.

2.1.1.2.1. Hardware

Los objetos de nuestra atención son fundamentalmente en:

i. **Los servidores.-** son los que se encuentran situados en dependencias específicas como centros de procesos de datos. El acceso a dichas instalaciones debe estar controlado y auditado con reflejo del personal y material que entra y sale del mismo.

ii. **Los clientes.-** son equipos remotos que interactúan entre sí o con los servidores, han tenido un desarrollo enorme en los últimos tiempos. Pasar de los denominados "terminales tontos" a computadores personales.

iii. **Las líneas de comunicaciones.-** son segmentaciones de la red que permite mejorar su funcionamiento y ayudará enormemente a su seguridad. La eliminación de los cuellos de botella y el estudio de las razones que ocurra.

2.1.1.2.2. Software

Los objetos de nuestra atención son fundamentalmente en:

i. **Sistemas Operativos.-** es la base del funcionamiento lógico del mismo, todo lo que esté alojado en el sistema estará íntimamente condicionado a la elección de un sistema operativo y su configuración personalizada.

ii. **Base de datos.-** es la parte más importante, además de contar con salvaguardas recientes, el contar con réplicas de la misma, a tiempo real lo que permite minimizar el impacto de una base explotada.

iii. **Aplicaciones.-** son a aquellos programas que de una u otra manera nos permiten explotar las funcionalidades de nuestro sistema.

2.1.2. ¿Qué queremos proteger?

Las redes de las universidades necesitan, protección contra amenazas, tanto internas como externas. En muchos casos, la violación de la seguridad es consecuencia de la falta de conocimiento o entrenamiento de los usuarios en prácticas informáticas seguras. En otros casos, el problema reside en estudiantes que intentan invadir los servidores que contienen información para poder manipular la información dentro de las universidades.

2.1.2.1. Tópicos erróneos comunes acerca de la seguridad

i. Mi sistema no es importante para un hacker.

ii. Estoy protegido pues no abro archivos que no conozco.

iii. Como tengo antivirus estoy protegido.

iv. Como dispongo de un firewall no me contagio.

2.1.2.2. Importancia de la Seguridad

La seguridad Informática es muy importante ya que existen personas ajenas a la información, también conocidas como piratas informáticos o hackers, que buscan tener acceso a la red para modificar, sustraer o borrar datos voluntaria o involuntariamente. Tales personajes pueden, incluso, formar parte del personal administrativo o de sistemas.

2.1.2.3. Seguridad en Internet

La Seguridad significa guardar algo seguro. "Algo" puede ser un objeto, tal como un secreto, mensaje, aplicación, archivo, sistema o una comunicación interactiva. «Seguro» los medios son protegidos desde el acceso, el uso o alteración no autorizada.

Para guardar objetos seguros, es necesario lo siguiente:

i. La autenticación (promesa de identidad), es decir la prevención de suplantaciones, que se garantice quien firma un mensaje es realmente quien dice ser.
ii. La autorización (se da permiso a una persona o grupo de personas de poder realizar ciertas funciones, al resto se le niega el permiso y se les sanciona si las realizan).
iii. La privacidad o confidencialidad, es el más obvio de los aspectos y se refiere a que la información solo puede ser conocida por individuos autorizados.
iv. La integridad de datos, La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., durante el proceso de transmisión o en su propio equipo de origen.
v. La disponibilidad de la información, se refiere a la seguridad, que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación o situaciones fortuitas o de fuerza mayor.
vi. No rechazo (la protección contra alguien que niega que ellos originaron la comunicación o datos).
vii. Controles de acceso, esto es quien tiene autorización y quien no para acceder a una parte de información determinada.

2.1.2.4. Puntos que son causantes de daños dentro de la red

2.1.2.4.1. Hoax.

Es una palabra inglesa que significa "engaño". Un Hoax es ligeramente diferente de un SPAM. No tiene fines comerciales. Tienen fines más mórbidos, y mucho menos amigables, en el peor de los casos. El Hoax utiliza a los receptores, para reenviar el mensaje.

2.1.2.4.2. Spam.

Es un correo electrónico que tiene por finalidad difundir, o publicitar un producto o servicio con fines comerciales, el SPAM sólo suele circular en un sentido (desde el emisor hacia el receptor).

2.1.2.4.3. Bulo

Un bulo es una noticia o una información falsa. Normalmente llega por correo electrónico y tiene un mensaje con contenido falso: por ejemplo que debemos borrar tal o cual fichero de nuestro sistema porque se trata de un virus.
Los bulos se sirven de la propia mentira para propagarse a sí mismos: recomiendan que ese mensaje sea enviado a tantas personas como sea posible.

2.1.3. Seguridad del entorno de operaciones

La seguridad de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención de las amenazas a los recursos y la información confidencial. Más claramente, por 'seguridad física' podemos entender todos aquellos mecanismos generalmente de prevención de los recursos de los sistemas; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

2.1.3.1. Acceso físico

Es cuando un atacante puede llegar con total libertad hasta una estación, por ejemplo abrir la CPU y llevarse un disco duro; sin necesidad de privilegios en el sistema, sin importar la robustez de nuestros cortafuegos, sin ni siquiera una clave de

usuario, el atacante podrá seguramente modificar la información almacenada. destruirla o simplemente leerla.

2.1.3.2. Desastres naturales

Son problemas que no suelen ser tan habituales, pero que en caso de producirse puede acarrear gravísimas consecuencias, es el derivado de los desastres naturales y su falta de prevención.

2.1.3.3. Desastres del entorno

i. Electricidad

En el entorno de trabajo los problemas más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo, son los que a diario amenazan la integridad tanto de nuestro hardware como los datos que almacena o que circulan por él

ii. Ruido eléctrico

Este problema no es una incidencia directa de la corriente en nuestros equipos, sino una incidencia relacionada con la corriente de otros computadores que pueden afectar al funcionamiento nuestro. El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede ser por otros computadores o por multitud de aparatos.

iii. Incendios y humo

Una causa casi siempre relacionada con la electricidad son los incendios, y con ellos el humo; aunque la causa de un fuego puede ser un desastre natural, lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga de la red debido al gran número de aparatos conectados al tendido.

iv. Temperaturas extremas

Las temperaturas extremas, ya sea un calor excesivo o un frió intenso, perjudican gravemente a todos los equipos. Para controlar la temperatura

ambiente en el entorno de operaciones se debe tener un acondicionador de aire, que influirá positivamente en el rendimiento de los usuarios.

2.1.3.5. Protección de los datos

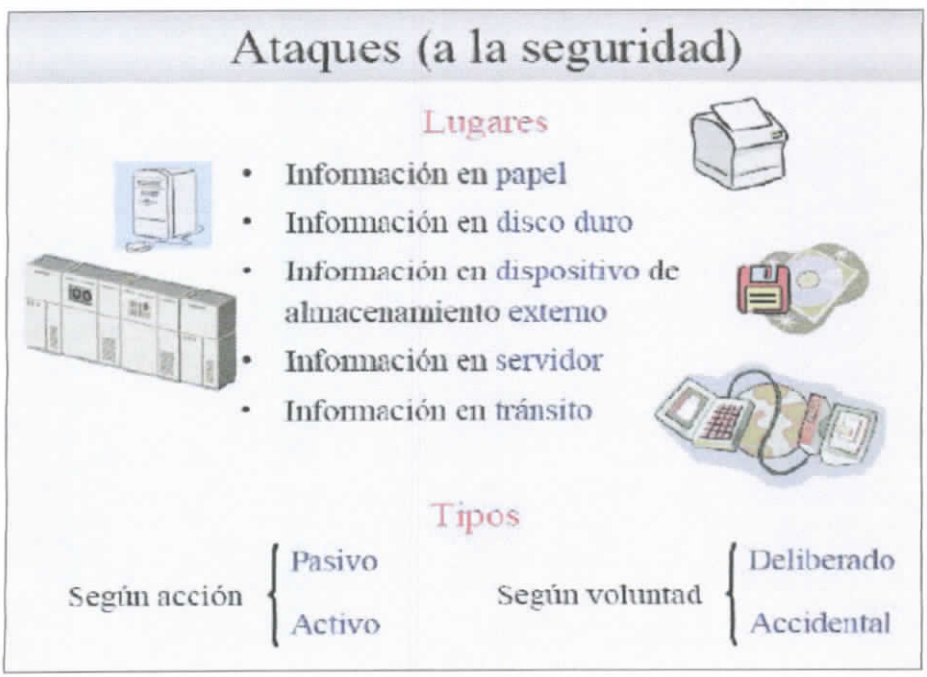
En lo que son los datos, existen ataques cuyo objetivo no es destruir el medio físico del sistema, sino simplemente conseguir la información almacenada en dicho medio. Existen varios métodos para dar una mejor protección a los datos:

2.1.3.5.1. Backups

Es la protección física de la información almacenada en backups, esto es, la protección de los diferentes medios donde residen las copias de seguridad. Se debe tener siempre presente que si las copias contienen toda la información se tiene que protegerlas igualmente a los sistemas.

2.1.4. Métodos y herramientas de ataque

Figura 2.3 Esquema de los elementos de ataque



El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia. La manipulación fraudulenta de los computadores con fines de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información puede afectar la esfera de la privacidad, son algunos de

los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

2.1.4.1. Atacantes

i. Personas llevadas por desafío intelectual o por aburrimiento
ii. (Ex) Empleados vengativos
iii. Personas (Empleados, clientes, delincuentes) que buscan beneficio económico
iv. Delincuencia organizada que quiere ocultar actividades ilegales
v. Espías de compañías o países rivales con fines económicos, políticos o militares.
vi. Terroristas o naciones que intentan influir en la política de un estado
vii. Fenómeno de la naturaleza (huracán, terremoto,....) que causa catástrofes

2.1.4.2. Vulnerabilidades

i. Software (con fallos)
ii. Contenido activo (malicioso): macros, scripts, etc.
iii. Puertos abiertos: Telnet, correo, etc.
iv. Configuración de recursos (incorrecta): permisos, etc.
v. Puertas traseras (agujeros de seguridad deliberados)
vi. Comunicación (sin cifrado)
vii. Contraseñas (mal elegidas) localización física (no segura)
viii. Administradores y usuarios (mal adiestrados)

2.1.4.3. Amenazas y vulnerabilidades

Por vulnerabilidad entendemos la exposición latente a un riesgo. En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, toca enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Estos fenómenos pueden ser causados por:

i. **Un operador.**-es la causa del mayor problema ligado a la seguridad de un sistema informático.

ii. **Programas maliciosos:** son programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.

iii. **Un intruso:** persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido. (cracker).

iv. **Un siniestro** (robo, incendio, inundaciones): una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.

Los métodos y herramientas de ataque involucraban poca sofisticación técnica. Los insiders (empleados disconformes o personas externas con acceso a sistemas dentro de la empresa) utilizaban sus permisos para alterar archivos o registros.

Los outsiders (personas que atacan desde afuera de la ubicación física de la organización) ingresaban a la red simplemente averiguando una password válida.

2.1.4.3.1. Malware

La palabra **malware** proviene de una agrupación de las palabras (**mal**icious soft**ware**). Existen muchísimos tipos de Malware, aunque algunos de los más comunes son los virus, los gusanos, los troyanos, los programas de spyware. Estos programas tienen como objetivo recopilar información sobre un usuario, un PC, etc., o con los peores fines.

2.1.4.3.2. Virus

Un virus informático es un programa que puede infectar a otros programas, modificándolos de tal manera que causen daño, borrando o dañando archivos que puedan afectar su rendimiento o seguridad. Este software constituye una amenaza muy seria; se propaga más rápido de lo que se tarda en solucionarlo.

Existe una gran variedad de virus cuyos efectos van desde los simplemente molestos, hasta los que destruyen información específica o bien todo el contenido en el disco duro. Lo característico de los virus es que una vez que se instalan en el ordenador pasan largo tiempo sin provocar ningún efecto, aparte de infectar a todos los demás programas que se ejecuten. Después de este período el virus actúa sobre el equipo en que estaba instalado.

2.1.4.3.3. Los gusanos informáticos.

Son similares a los virus, pero los gusanos no dependen de archivos portadores para poder contaminar otros sistemas. Estos pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema.

La diferencia entre un gusano y un virus informático radica en que el gusano opera de forma más o menos independiente a otros archivos, mientras que el virus depende de un portador para poderse replicar.

2.1.4.3.4. Un caballo de troya

Es un programa que hace algo oculto y que el usuario no ha aprobado, como abrir una conexión para que alguien externo tenga acceso a nuestra información. Finalmente, mucha gente usa el término "Troyano" para referirse solamente a un programa malicioso que no se copia a si mismo, a diferencia de los llamados "gusanos" que estos si se copian y propagan rápidamente.

Los troyanos son programas que permiten a extraños intervenir en un ordenador remoto que está conectado a Internet, es lo que se conoce como "hackear" o más correctamente "nukear" un computador remoto.

2.1.4.3.5. El spyware.

Es todo aquel software que recolecta y envía información de los usuarios. Normalmente trabajan y contaminan sistemas como lo hacen los caballos de troya.

2.1.4.3.6. Exploit.

Es aquel software que ataca una vulnerabilidad particular de un sistema operativo. Los exploits no son necesariamente maliciosos, son generalmente creados por

investigadores de seguridad informática para demostrar que existe una vulnerabilidad. Y por esto son componentes comunes de los programas maliciosos como los gusanos informáticos.

2.1.4.3.7. Rootkit.-

Son programas que son insertados en una computadora después de que algún atacante ha ganado el control de un sistema. Los rootkit generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los log de entradas o encubrir los procesos del atacante. Los rootkit pueden incluir puertas traseras, permitiendo al atacante obtener de nuevo acceso al sistema o también pueden incluir exploits para atacar otros sistemas.

2.1.4.4. Ataques potenciales

2.1.4.4.1. Ingeniería social

La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían aunque a nadie le gusta ser manipulado, en algunos casos no es excesivamente perjudicial (por ejemplo un vendedor puede aplicar ingeniería social para conocer las necesidades de un cliente y ofrecer así mejor sus productos), si las intenciones de quien la pone en práctica no son buenas se convierte quizás el método de ataque más sencillo, menos peligroso para el atacante y por desgracia en uno de los más efectivos. El atacante puede aprovechar el desconocimiento de unas mínimas medidas de seguridad por parte de personas relacionadas de una u otra forma con el sistema para poder engañarlas en beneficio propio.

2.1.4.4.2. Shoulder Surfing

Es otro tipo de ataque relacionado con la ingenuidad de los usuarios del sistema (pero también con el control de acceso físico) es el denominado *shoulder surfing*. Consiste en 'espiar' físicamente a los usuarios, para obtener generalmente claves de acceso al sistema.

2.1.4.4.3. Masquerading

El ataque denominado de masquerading o mascarada consiste simplemente en suplantar la identidad de cierto usuario autorizado de un sistema informático o su

entorno; esta suplantación puede realizarse electrónicamente, un usuario utiliza para acceder a una máquina un login y password que no le pertenecen.

2.1.4.4.4. Basureo

La técnica del basureo (en inglés, scavenging) está relacionada tanto con los usuarios como con la seguridad física de los sistemas; consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo. El basureo puede ser físico, como buscar en cubos de basura, listados de impresión o copias de documentos, o lógico, como analizar buffers de impresoras, memoria liberada por procesos, o bloques de un disco que el sistema acaba de marcar como libres, en busca de información

2.1.4.5. Actos delictivos

La información con la que se trabaja en la mayor parte de entornos hace poco probable que alguien amenace o chantajee a un operador para conseguir ciertos datos; al tratarse de información poco sensible, en la mayoría de situaciones los atacantes no llegan a estos extremos para acceder al sistema, sino que utilizan procedimientos menos arriesgados como la ingeniería social o la captura de datos que viajan por la red.

2.1.4.5.1. Hackers

Son piratas y para ellos ya no existen los barcos ni los tesoros escondidos debajo del mar. Los piratas se presentan con un cerebro desarrollado, curioso y con muy pocas armas: una simple computadora y una línea telefónica. Hackers es una palabra que aún no se encuentra en los diccionarios pero que ya suena en todas las personas que alguna vez se interesaron por la informática o leyeron algún diario. Proviene de "hack", el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionen. Hoy es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida. Los crackers (crack=destruir) son aquellas personas que siempre buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus, etc.

Se diferencian con los Hackers porque no poseen ningún tipo de ideología cuando realizan sus "trabajos". En cambio, el principal objetivo de los Hackers no es convertirse en delincuentes sino "pelear contra un sistema injusto" utilizando como arma al propio sistema.

2.1.4.6. Tipos de ataques a la red

2.1.4.6.1. Ataques de escaneo:

Los ataques de escaneo se realizan para la recopilación de información sobre posibles puertas de acceso a la red. Consisten en recopilar la información de que puertos están escuchando en la red para posteriormente acceder a los recursos a través de ellos.

Un puerto se podría definir como el punto de enlace entre dos procesos, sean locales (en una misma pc) o remotos (desde una red local o Internet). Es un punto de conexión y de organización de la información que circula. Los puertos tienen un límite y están numerados del 0 al 65535. El rango de puertos más conocidos es del 0 al 1023. De las páginas Web Los números de puerto están divididos en tres rangos: Los Puertos Bien Conocidos, los Puertos Registrados, y los Puertos Dinámicos y/o Privados.

- Los Puertos Bien Conocidos son aquellos del 0 hasta el 1023.
- Los puertos registrados son aquellos del 1024 al 49151.
- Los puertos Dinámicos y/o Privados son aquellos desde el 49152 al 65535.

Explorar todos los puertos posibles involucraría explorar más de 130.000 puertos. La exploración puede tomar mucho tiempo. Para explorar los 64.000 puertos TCP. El problema con los puertos UDP es que no responden cuando el puerto está abierto.

2.1.4.6.2. Ataques de Modificación-daño

Este tipo de ataques son los más peligrosos porque actúan sobre los datos o los programas instalados, modificando o borrando los archivos. Los ataques necesitan de los anteriores para obtener la información necesaria de la red y normalmente realizar el objetivo final de un intruso.

Estos ataques se efectúan sobre el software o datos del sistema con la finalidad de sustituir el software original por otro malicioso y los archivos de datos de la victima por otros que pueden llevar incorporados virus, troyanos etc.

a) **Tampering o Data Diddling**

Con este tipo de ataques se puede hacer mucho daño a entidades como bancos, ya que al acceder al sistema, si se han conseguido los permisos oportunos, deja libre al atacante para crear por ejemplo cuentas falsas o modificar las existentes y desviar dinero de una a otra.

b) **Borrado de huellas:**

El atacante cuando accede a un sistema lo hace aprovechando las vulnerabilidades del sistema, estas acciones se pueden ver reflejadas en los logs del sistema, monitores de red, o si la red posee un firewall en los logs del firewall

2.1.4.6.3. Ataques por vulnerabilidades

Las vulnerabilidades son puntos débiles de los sistemas que son aprovechados parar acceder y realizar alguna acción maliciosa. El software que es utilizado es sometido a numerosas pruebas para detectar y corregir las vulnerabilidades, pero esto no garantiza al 100% que no este libre de ser vulnerable.

Los desarrolladores de software cuando detectan alguna vulnerabilidad, la corrigen con los famosos parches.

2.1.4.6.4. Ataque por Fragmentación:

Como su nombre indica, consiste en fragmentar los paquetes de ataques SYN y FIN para que los filtros de la red no puedan detectarlos. Es poco efectivo ya que genera tal cantidad de pequeños paquetes que son enviados a la victima, que pueden llegar a bloquear tanto los recursos del atacante como saturar las colas de los posibles filtros de la red (firewalls).

a) **Snnifing:**

El ataque Snnifing se considera un ataque pasivo, porque realmente solo recopila y almacena la información que circula por la red. Estas herramientas se pueden instalar tanto en quipos de la red como en equipos.

b) **Snooping**

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Este tipo de ataque también es pasivo, también escucha en la red todo el trafico, pero a diferencia del anterior, este ataque permite acceder a datos e incluso descargar los mismos para una manipulación posterior.

c) **Tampering o data diddling**

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada.

2.1.4.6.5. Ataques de autentificación

Los ataques de autentificación consisten en introducirse en un sistema suplantando la identidad de un usuario o del propio administrador. O bien se aprovecha una sesión establecida por el usuario, o bien con los datos obtenidos de los ataques de escaneo.

a) **Spoofing**

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails. El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso,

llamado Looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante.

b) Jamming o flooding

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla. Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión.

2.1.4.6.6. Ataques DoS (denegación de servicio)

Los ataques DoS se ejecutan típicamente usando herramientas DoS que envían muchos paquetes con peticiones a un servidor de Internet (generalmente servidor Web, FTP o de correo), lo cual agota los recursos del servidor, haciendo el sistema inutilizable. Cualquier sistema que esté conectado a Internet y equipado con servicios de red TCP está expuesto a un ataque.

2.1.5. Seguridad de la red

Muchas organizaciones dependen en gran medida de seguridad de red para proteger sus estaciones de trabajo y servidores, de las amenazas de Internet. Este enfoque se conoce como "duro por fuera, blando por dentro". Otro enfoque proporciona un tipo de seguridad "duro por dentro y por fuera" más adecuado. El hecho de que se hayan detectado gusanos que hayan logrado franquear los servidores de seguridad de las organizaciones.

Los atacantes crean gusanos y virus que pueden destruir los datos almacenados en los equipos cliente, o provocar la pérdida o el robo de la información que contienen. Estos ataques pueden causar la pérdida de información privada y secretos empresariales, impedir que los equipos puedan iniciarse e incluso servir de plataforma para el lanzamiento de ataques a otros equipos. En consecuencia, constituyen una amenaza muy real para los equipos conectados a Internet.

La seguridad, está tomando mayor importancia día a día, puesto que cada vez hay más conexiones a Internet y más prolongadas, y los servidores caseros, que están permanentemente conectados a la red, proliferan como setas. Y eso sin contar con los grandes servidores, aunque eso ya es otra historia puesto que muchos de ellos están detrás de un firewall implementado directamente en hardware. A estos se les suele llamar firewalls perimetrales, puesto que normalmente son los que cubren los primeros accesos de la red, a causa de su mayor robustez, por lo que muchas veces el peligro está dentro.

2.1.5.1. General - ¡Cuidado con los Clics!

Con la generalización del ambiente gráfico de Windows y del uso del Mouse, surgieron los famosos "clics" como medio de comunicación entre el hombre y el computador. Los "clics" se convierten en una especie de llaves que nos van abriendo las puertas a medida que nos sumergimos en el ciberespacio, permitiéndonos disfrutar de sus múltiples beneficios en forma más cómoda

Pero no es todo, un clic inconsciente o sin suficiente análisis, mientras estamos conectados a la red, puede ser muy peligroso en la medida que, o bien puede abrir la puerta de su vida privada al público, obligarlo a cumplir un contrato que no se intento celebrar o exponer la seguridad de su computador y de sus finanzas

2.1.5.2. Privacidad

La privacidad es un derecho renunciable y una de las formas de renunciar a ella, es a través de un clic. Por ejemplo, cuando se registra en un sitio de Internet y suministra datos personales, es posible que los datos sean compartidos o vendidos a otras empresas que posteriormente le enviarán publicidad a su correo electrónico sin usted solicitarla. También suele suceder que el sitio web al que se ingrese le introduzca "cookies" en su disco duro para determinar cuales son sus preferencias.

En cuanto a los cookies, estos son archivos de texto que son escritos en el disco duro por el navegador a solicitud de un servidor Web. Los archivos contienen información como el nombre del sitio que la origina, qué páginas fueron visitadas por el internauta, las preferencias de una búsqueda, los nombres colocados en algún formulario e incluso los números de la tarjeta de crédito usadas para alguna

transacción en línea. Las cookies no siempre representan un peligro para la privacidad ya que en algunos casos su único objetivo es facilitar la navegación al usuario dentro de un sitio Web determinado.

2.1.5.3. Protección

"Esto es lo que llamamos Criptograma, en el cual el sentido está oculto bajo letras embarulladas a propósito y que, convenientemente dispuestas, formarían una frase inteligible. La palabra Criptografía proviene etimológicamente del griego Kruiptoz (Kriptos-Oculto) y Grajein (Grafo-Escritura) y significa "arte de escribir con clave secreta o de un modo enigmático"

La Criptografía es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es (mediante claves que sólo el emisor y el destinatario conocen), para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.

2.1.6. Vulnerar Para Proteger

Una vez conocidas las vulnerabilidades y ataques a las que está expuesto un sistema es necesario conocer los recursos disponibles para protegerlo. Mientras algunas técnicas son evidentes (seguridad física por ejemplo).

Los intrusos utilizan diversas técnicas para infringir los sistemas de seguridad de una red. Básicamente buscan los puntos débiles del sistema para poder filtrarse en ella. El trabajo de los administradores no difiere mucho. En lo que se diferencia, y por completo, es en los objetivos: mientras que un intruso penetra en las redes para distintos fines (investigación, daño, robo, etc.) un administrador lo hace para poder mejorar los sistemas de seguridad

2.1.6.1. Access Control Lists (ACL)

Las Listas de Control de Accesos proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas Operativos. Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo pueden definirse sobre un Proxy una lista de todos los usuarios (o grupos de ellos) a quien se le permite el acceso a Internet. También podrán definirse otras características como limitaciones de anchos de banda y horarios.

Ejemplo de ACL

Para acceder a determinados servicios de una máquina, es necesario definir permisos sobre el modo de acceso, el origen y los servicios a los que se permite acceder de esa máquina; esto se consigue mediante la orden access-lis.

Si por ejemplo queremos habilitar un acceso HTTP desde cualquier lugar de Internet, y además acceso POP3 desde un determinado segmento externo (por ejemplo, 196.33.22.128/25) a la máquina 158.42.22.41, lo haremos mediante una lista de control de acceso.

2.1.6.2. Wrappers

i. Un Wrapper es un programa que controla el acceso a un segundo programa. El Wrapper literalmente cubre la identidad de este segundo programa, obteniendo con esto un más alto nivel de seguridad. Los Wrappers son usados dentro de la seguridad en sistemas UNIXs. Estos programas nacieron por la necesidad de modificar el comportamiento del sistema operativo sin tener que modificar su funcionamiento.

2.1.6.3. Detección de Intrusos en Tiempo Real

La integridad de un sistema se puede corromper de varias formas. La forma de evitar esto es con la instalación de sistemas de Detección de Intrusos en Tiempo Real, quienes:

i. Inspeccionan el tráfico de la red buscando posibles ataques.
ii. Controlan el registro de los servidores para detectar acciones sospechosas (tanto de intrusos como de usuarios autorizados).
iii. Mantienen una base de datos con el estado exacto de cada uno de los archivos (Integrity Check) del sistema para detectar la modificación de los mismos.
iv. Controlan el ingreso de cada nuevo archivo al sistema para detectar Caballos de Troya o semejantes.
v. Controlan el núcleo del Sistema Operativo para detectar posibles infiltraciones en él, con el fin de controlar los recursos y acciones del mismo.

Cada una de estas herramientas permite mantener alejados a la gran mayoría de los intrusos normales. Algunos pocos, con suficientes conocimientos, experiencia y paciencia serán capaces de utilizar métodos sofisticados como para voltear el perímetro de seguridad (interna + externa)

2.1.6.4. Call Back

Este procedimiento es utilizado para verificar la autenticidad de una llamada vía MODEM. El usuario llama, se autentifica contra el sistema, se desconecta y luego el servidor se conecta al número que en teoría pertenece al usuario.

La ventaja reside en que si un intruso desea hacerse pasar por el usuario, la llamada se devolverá al usuario legal y no al del intruso, siendo este desconectado. Como precaución adicional, el usuario deberá verificar que la llamada-retorno proceda del número a donde llamó previamente.

2.1.6.5. Sistemas Anti-Sniffers

Esta técnica consiste en detectar Sniffers en el sistema. Generalmente estos programas se basan en verificar el estado de la placa de red, para detectar el modo en el cual está actuando (recordar que un Sniffer la coloca en Modo Promiscuo), y el tráfico de datos en ella.

2.1.7. Amenazas internas

En las amenazas internas debemos tener en cuenta a un estudiante como hacker, el simple acceso a un equipo de la red que esté por detrás del firewall dará la oportunidad de introducir virus, gusanos o otros códigos dañinos. Estudiantes que dispongan de ese mismo tipo de acceso pueden violar archivos que contienen información confidencial y así ver o modificar sus notas.

2.1.8. Amenazas externas

Los problemas de seguridad informática no pueden ser tratados aisladamente ya que la seguridad de todo sistema es igual a la de su punto más débil. Al asegurar nuestra casa no sacamos nada con ponerle una puerta blindada con sofisticada cerradura si dejamos las ventanas sin protección. De manera similar el uso de sofisticados

algoritmos y métodos criptográficos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo.

Las vulnerabilidades que el software presenta pueden poner el sistema en peligro si no se aplican los parches necesarios. El tiempo que transcurre desde la detección de cualquier vulnerabilidad y la explotación de los fallos de seguridad por los hackers es cada vez más corto. Pese a ello, la principal amenaza externa a la seguridad sigue siendo los virus, que en la actualidad tienen una capacidad de diseminación muy rápida.

2.1.8.1. Defensa en profundidad

No existe ningún método válido para todos los casos que pueda proteger redes, de las amenazas internas y externas presentes en un ambiente tan imprevisible como el de la actualidad. La defensa en profundidad implica la creación de varias capas de tecnologías de seguridad complementarias en torno de las computadoras y datos confidenciales en estaciones de trabajo, gateway y servidores.

De esta forma, firewalls y software antivirus pueden proteger la red en el gateway de amenazas externas, pero es necesario contar con controles adicionales que impidan acciones no autorizadas de usuarios internos. El software de filtrado de contenido aporta otra capa al programa de seguridad que evitará que los usuarios tengan acceso a contenidos inadecuados de la Web.

2.1.9. Políticas de uso aceptable

El uso generalizado de computadoras conectadas a Internet exige que los administradores de las redes de las universidades, bibliotecarios, profesores, y estudiantes se aseguren de utilizar los equipos de manera apropiada y segura. Los programas de seguridad informática eficaces incluyen la concienciación y apoyo de los usuarios para que se reduzcan los riesgos. La definición de políticas y procedimientos preparan el escenario de la informática segura. Es necesario educar a los usuarios ya que, de lo contrario, podrían convertirse involuntariamente en el origen de las brechas en la seguridad.

Veamos a continuación algunos componentes típicos de las políticas de uso aceptable:

i. Descripción de lo que se considera uso aceptable y no aceptable de Internet, indicando por ejemplo transferencias de archivos, uso de mensajería instantánea, etc.

ii. Declaración de uso con fines educativos y ventajas de disponer de Internet en el aula.

iii. Filosofía y estrategias institucionales que se verían apoyadas por el acceso a Internet.

iv. Prácticas informáticas seguras al llevar a casa computadoras y discos pertenecientes a la escuela.

v. Responsabilidad de los profesores, padres y estudiantes en lo que respecta al uso de Internet, que puede incluir prácticas informáticas seguras tales como no revelar la contraseña, no abrir anexos de correo electrónico que no sean conocidos, a quién informar en caso de problemas de seguridad potenciales, etc.

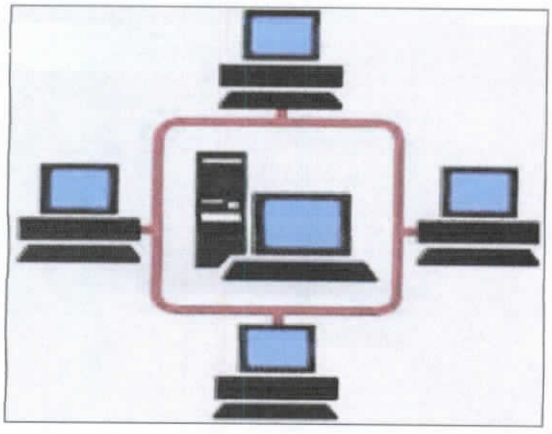
vi. Recordatorio de que el acceso a Internet y el uso de redes de computadoras son un privilegio, no un derecho.

vii. Especificación de las consecuencias de violar la política.

viii. Formulario de consentimiento y exención para profesores, padres y estudiantes indicando su intento de respetar las políticas establecidas.

2.2. Redes

Figura 2.4 Esquema de una Red de Ordenadores



Las redes son el pilar en el uso compartido de la información en empresas, así como en grupos gubernamentales y científicos. Esta información puede adoptar distintas

formas, sea como documentos, datos a ser procesados por otro ordenador, ficheros a ser enviados, e incluso formas más exóticas de datos.

La mayoría de estas redes se instalaron a finales de los años 60 y 70, cuando el diseño de redes se consideraba como la piedra filosofal de la investigación informática y la tecnología punta. Dio lugar a numerosos modelos de redes como la tecnología de conmutación de paquetes, redes de área local con detección de colisión, redes jerárquicas, y muchas otras de elevada calidad.

Desde comienzos de los '70, otro aspecto de la tecnología de redes cobró importancia: el modelo de pila de protocolo, que permite la interoperabilidad entre aplicaciones. Toda una gama de arquitecturas fue propuesta e implementada por diversos equipos de investigación y fabricantes de ordenadores.

El resultado de todos estos conocimientos prácticos es, que hoy en día cualquier grupo de usuarios puede hallar una red física y una arquitectura adecuada a sus necesidades específicas, desde líneas asíncronas de bajo coste, pasando por funciones completas de redes de área extensa (pública o privada) con protocolos fiables como redes públicas de conmutación de paquetes o redes privadas, hasta las redes de área local, de alta velocidad pero distancia limitada.

2.2.1.1. Ventajas de las redes informáticas

Las redes de computadoras permiten compartir recursos e información, con el objeto de abaratar costes, facilitar el trabajo en grupo. En particular:

i. compartir archivos y programas
ii. compartir impresoras
iii. compartir un acceso a Internet
iv. enviar y recibir correo electrónico
v. usar bases de datos compartidas
vi. gestionar eficazmente la seguridad de los equipos
vii. realizar copias de seguridad centralizadas

2.2.1.2. Tipos de redes informáticas según su protocolo

Los protocolos se clasifican en dos grupos: protocolos de bajo nivel, y los protocolos de red.

2.2.1.2.1 Protocolos de bajo nivel

Los protocolos de bajo nivel son: Ethernet, Token Ring, FDDI, ATM, LocalTalk, etc. Aunque los más usados para implementaciones similares son: Ethernet, Token Ring

a) **Ethernet**

Es el método de conexión más adecuado que permite un buen equilibrio entre velocidad, costo y facilidad de instalación. Ethernet es la tecnología ideal para la mayoría de las instalaciones de LAN. Esta tecnología obtiene velocidades de conexión de 10 Mbits/s aunque existen especificaciones de velocidades superiores como es el caso de Fast Ethernet que llega a conseguir hasta 100 Mbits/s.

b) **Token Ring**

Es un sistema bastante usado aunque mucho menos que Ethernet. Llega a conseguir velocidades de hasta 16 Mbits/s aunque también existen especificaciones para velocidades superiores. La topología lógica que usa es en anillo aunque en la práctica se conecta en una topología física en estrella, a través de concentradores llamados MAU (Multistation Access Unit).

2.2.1.2.2. Protocolos de red.

Los protocolos de red organizan la información (controles y datos) para su transmisión por el medio físico a través de los protocolos de bajo nivel. Veamos algunos de ellos:

a) **IPX/SPX**

IPX (Internetwork Packet Exchange) es un protocolo de Novell que interconecta redes que usan clientes y servidores Novell Netware. **IPX/SPX**, cuyas siglas provienen de **Internetwork Packet Exchange/Sequenced Packet**

Exchange (Intercambio de paquetes interred/Intercambio de paquetes secuenciales), es un protocolo de red utilizado por los sistemas operativos Novell Netware.

SPX es un protocolo de la capa de transporte (nivel 4 del modelo OSI) utilizado en redes Novell. La capa SPX se sitúa encima de la capa IPX (nivel 3) y proporciona servicios orientados a conexión entre dos nodos de la red. SPX se utiliza principalmente para aplicaciones cliente/servidor.

Mientras que el protocolo IPX es similar a IP, SPX es similar a TCP. Juntos, por lo tanto, proporcionan servicios de conexión similares a TCP/IP. IPX se sitúa en el nivel de red del modelo OSI y es parte de la pila de protocolos IPX/SPX. IPX/SPX fue diseñado principalmente para redes de área local (LANs), y es un protocolo muy eficiente para este propósito (típicamente su rendimiento supera al de TCP/IP en una LAN).

b) NetBIOS

NetBIOS (Network Basic Input/Output System) es un programa que permite comunicarse entre aplicaciones en diferentes ordenadores dentro de una LAN. Desarrollado originalmente para las redes de ordenadores personales IBM, fue adoptado posteriormente por Microsoft. NetBIOS, se usa en redes con topologías Ethernet y Token Ring. No permite un mecanismo de enrutamiento por lo que no es adecuado para redes de área extensa (MAN), en las que se deberá usar otro protocolo para el transporte de los datos (por ejemplo, el TCP). Resumiendo, de forma sencilla, NetBIOS, permite a las aplicaciones 'hablar' con la red. Su intención es conseguir aislar los programas de aplicación de cualquier tipo de dependencia del hardware. También evita que los desarrolladores de software tengan que desarrollar rutinas de recuperación ante errores o de enrutamiento o direccionamiento de mensajes a bajo nivel. En una red local con soporte NetBIOS, los ordenadores son conocidos e identificados con un nombre. Cada computador de la red tiene un único nombre.

Cada PC de una red local NetBIOS se comunica con los otros bien sea estableciendo una conexión (sesión), usando datagramas NetBIOS o mediante broadcast. Las sesiones permiten, como en el protocolo TCP, mandar mensajes

más largos y gestionar el control y recuperación de errores. La comunicación será punto a punto.

c) **AppleTalk**

AppleTalk identifica varias entidades de red, cada una como un nodo. Un nodo es simplemente un dispositivo conectado a una red AppleTalk. AppleTalk fue diseñada como un cliente/servidor o sistema de red distribuido, en otras palabras, los usuarios comparten recursos de red como archivos e impresoras con otros usuarios. Las interacciones con servidores son transparentes para el usuario, ya que, la computadora por sí misma determina la localización del material requerido, accediendo a él sin que requiera información del usuario.

Existen tres variantes de este protocolo:

i. **Local Talk.** -La comunicación se realiza a través de los puertos serie de las estaciones. La velocidad de transmisión es pequeña pero sirve por ejemplo para compartir impresoras.

ii. **Ether talk**. -Es la versión para Ethernet. Esto aumenta la velocidad y facilita aplicaciones

iii. **Token talk**. -Es la versión de Apple talk para redes TokenRing.

d) **TCP/IP**

Es el mas conocido y utilizado TCP (Transmission Control Protocolo) e IP (Internet Protocol o protocolo Internet). Dicha conjunto o familia de protocolos es el que se utiliza en Internet.

TCP/IP es el protocolo común utilizado por todas las redes conectadas a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta queeln Internet se encuentran conectado a redes, de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Este protocolo se encargará que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware

2.2.1.3. Comunicaciones en red

La actividad de una red incluye el envío de datos de un equipo a otro. Este proceso complejo se puede dividir en tareas secuenciales discretas. El equipo emisor debe:

i. Reconocer los datos.
ii. Dividir los datos en porciones manejables.
iii. Añadir información a cada porción de datos para determinar la ubicación de los datos y para identificar al receptor.
iv. Añadir información de temporización y verificación de errores.
v. Colocar los datos en la red y enviarlos por su ruta.

El software de cliente de red trabaja a muchos niveles diferentes dentro de los equipos emisores y receptores. Cada uno de estos niveles, o tareas, es gestionado por uno o más protocolos. Estos protocolos, o reglas de comportamiento, son especificaciones estándar para dar formato a los datos y transferirlos. Cuando los equipos emisores y receptores siguen los mismos protocolos se asegura la comunicación. Debido a esta estructura en niveles, a menudo es referido como pila del protocolo.

2.2.2. Modelo OSI

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).

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. 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.

La tarea del subcomité ISO fue definir el conjunto de niveles y los servicios proporcionados por cada nivel. Los principios aplicados para establecer un nivel fueron los siguientes:

i. Diferentes niveles deben corresponder a diferentes niveles de abstracción en el manejo de los datos (por ejemplo diferencias en la morfología, la sintaxis, la semántica).
ii. Cada nivel debe ejecutar una función bien definida.
iii. Aprovechar la experiencia de protocolos anteriores. Las fronteras de niveles deben situarse donde la experiencia ha demostrado que son convenientes.
iv. Establecer las divisiones de los niveles de forma que se minimice el flujo de información entre ellos.
v. El número de niveles debe ser suficiente para que no agrupen funciones distintas, pero no tan grande que haga la arquitectura inmanejable.
vi. Permitir que las modificaciones de funciones o protocolos que se realicen en un nivel no afecten a los niveles contiguos.
vii. Cada nivel debe interaccionar únicamente con los niveles contiguos a él (superior e inferiormente).

El modelo OSI es la guía mejor conocida y más ampliamente utilizada para la visualización de entornos de red. Los fabricantes se ajustan al modelo OSI cuando diseñan sus productos para red. Éste ofrece una descripción del funcionamiento conjunto de hardware y software de red por niveles para posibilitar las comunicaciones. El modelo también ayuda a localizar problemas proporcionando un marco de referencia que describe el supuesto funcionamiento de los componentes.
Los equipos presentan diferencias en:

- Procesador Central.
- Velocidad.
- Memoria.
- Dispositivos de Almacenamiento.
- Códigos de caracteres.
- Sistemas Operativos.

Estas diferencias propician el problema de comunicación entre computadoras no tenga una solución simple. Dividiendo el problema general de comunicación, en problemas específicos, facilitamos la obtención de una solución a dicho problema. Formalizar los diferentes niveles de interacción para la conexión de computadoras habilitando así la comunicación del sistema de cómputo independientemente del:

i. Fabricante.
ii. Arquitectura.
iii. Localización.
iv. Sistema Operativo.

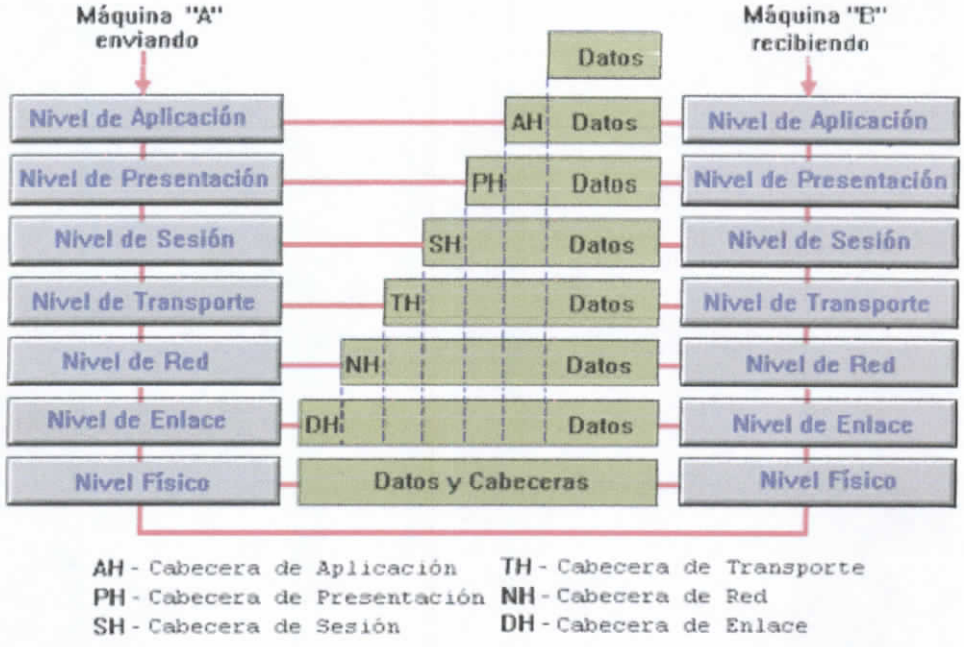
2.2.2.2. Estructura del Modelo OSI de ISO

El objetivo perseguido por OSI establece una estructura que presenta las siguientes particularidades:

2.2.2.2.1. Estructura multinivel

Se diseñó una estructura multinivel con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación. Esto es, cada nivel ejecuta funciones específicas. El nivel superior utiliza los servicios de los niveles inferiores: Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora. La comunicación ínter nivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1. En la figura 2.5 se muestra una representación de los niveles OSI y la forma de establecer un diálogo entre diferentes dispositivos.

Figura 2.5 Esquema de la Estructura Multinivel del Modelo OSI



Para simplificar, estructurar y normalizar los protocolos utilizados en las redes de comunicaciones se establecen una serie de niveles paralelos diferenciados por funciones específicas. Cada uno de estos niveles proporciona un conjunto de servicios al nivel superior, a partir de otros servicios más básicos proporcionados por los niveles inferiores.

Los niveles paralelos de las máquinas que participan en la comunicación mantienen una conversación virtual a través de los niveles inferiores. Las reglas y convenciones utilizadas en esta conversación son lo que se denomina protocolo de nivel **n**.

El modelo de siete niveles se ha convertido en un estándar internacional. Cada uno de los niveles del modelo define una sección específica del total de la arquitectura. Diferentes organismos de estandarización (ISO, IEEE, ANSI...) han definido diversos protocolos sobre esos niveles para adaptar las implementaciones finales a variados entornos y requisitos.

2.2.2.2.2. Puntos de acceso:

Entre los diferentes niveles existen interfaces llamadas "puntos de acceso" a los servicios.

i. **Dependencias de Niveles**: Cada nivel es dependiente del nivel inferior y también del superior.

ii. **Encabezados:** En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información. Cualquier nivel dado, puede incorporar un encabezado: Encabezado e Información. Entonces, la incorporación de encabezados es necesaria aunque representa un lote extra de información, lo que implica que un mensaje corto pueda ser voluminoso. Sin embargo, como la computadora destino retira los encabezados en orden inverso a como fueron incorporados en la computadora origen, finalmente el usuario sólo recibe el mensaje original.

iii. **Unidades de información:** En cada nivel, la unidad de información tiene diferente nombre y estructura.

2.2.3. Nivel Físico:

La capa física comunica directamente con el medio de comunicación y tiene dos responsabilidades: enviar bits y recibir bits. Un dígito binario o bit es la unidad básica de información en comunicación de datos. Un bit sólo puede tener dos valores, 1 ó 0, representados por distintos estados en el medio de comunicación. Otras capas se responsabilizan del agrupamiento de los bits de forma que representen datos de un mensaje. Los bits se representan por cambios en las señales del medio de la red. Algunos cableados representan los unos y los ceros con distintos voltajes, otros utilizan tonos de audio distintos y otros utilizan métodos más sofisticados, por ejemplo transiciones de estado (cambios de alto a bajo voltaje y viceversa).

Se utiliza una gran variedad de medios en la comunicación de datos; entre otros, cables eléctricos, fibras ópticas, ondas de luz o de radio y microondas. Estos definen el medio de comunicación utilizado para la transferencia de información

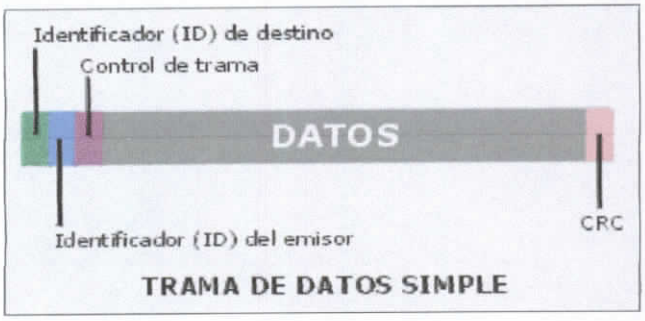
Los medios de control especifican bits mediante:

i. Definir conexiones físicas entre computadoras.
ii. Describir el aspecto mecánico de la interfase física.
iii. Describir el aspecto eléctrico de la interfase física.
iv. Describir el aspecto funcional de la interfase física.
v. Definir la Técnica de Transmisión.
vi. Definir el Tipo de Transmisión.
vii. Definir la Codificación de Línea.
viii. Definir la Velocidad de Transmisión.
ix. Definir el Modo de Operación de la Línea de Datos.

2.2.4. Nivel Enlace de Datos

Los dispositivos que pueden comunicarse a través de una red suelen denominarse nodos (en ocasiones se denominan estaciones y dispositivos). La capa de enlace de datos es responsable de proporcionar la comunicación nodo a nodo en una misma red de área local.

Figura 2.6 Esquema de la Capa de Enlace de Datos



La capa de enlace de datos proporciona un mecanismo de direcciones que permita entregar los mensajes en los nodos correctos y debe traducir los mensajes de las capas superiores en bits que puedan ser transmitidos por la capa física.

Cuando la capa de enlace de datos recibe un mensaje, le da formato para transformarlo en una trama de datos (denominada igualmente paquete). Las secciones de una trama de datos se denominan campos. Los campos del ejemplo son los siguientes:

Indicador de inicio. Un patrón de bits que indica el inicio de una trama de datos.
Dirección de origen. La dirección del nodo que realiza el envío se incluye para poder dirigir las respuestas al mensaje.
Dirección de destino. Cada nodo queda identificado por una dirección. La capa de enlace de datos del remitente añade la dirección de destino a la trama. La capa de enlace de datos del destinatario examine la dirección de destino para identificar los mensajes que debe recibir.
Control. En muchos casos es necesario incluir información adicional de control. Cada protocolo determine la información específica.
Datos. Este campo contiene todos los datos enviados a la capa de enlace de datos por las capas superiores del protocolo.
Control de errores. Este campo contiene información que permite que el nodo destinatario determine si se ha producido algún error durante la transmisión. El sistema habitual es la verificación de redundancia cíclica (CRC), que consiste en un valor calculado que resume todos los datos de la trama. El nodo destinatario calcula nuevamente el valor y, si coincide con el de la trama, entiende que la trama se ha transmitido sin errores.

La entrega de tramas resulta muy sencilla en una red de área local. Un nodo remitente se limita a transmitir la trama. Cada nodo de la red ve la trama y examina su dirección de destino. Cuando coincide con su dirección, la capa de enlace de datos del nodo recibe la trama y la envía a la siguiente capa de la pile.

Se encuentra por encima del nivel físico y transforma los 1 y 0 que le llegan en una secuencia de bits libre de errores para enviarlos al nivel de red. Este nivel proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red. También organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información. Para:

i. *Detectar errores en el nivel físico.*

ii. Establecer esquema de detección de errores para las retransmisiones o *reconfiguraciones de la red.*

iii. Establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes. Realizar la transferencia de datos a través del enlace físico.

iv. Enviar bloques de datos con el control necesario para la sincronía.

v. En general controla el nivel y es la interfaces con el nivel de red, al comunicarle a este una transmisión libre de errores.

La capa de enlace puede considerarse dividida en dos sub capas:

Figura 2.7 Esquema de las Sub Capas de la Capa de Enlace de Datos



Control lógico de enlace LLC: define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.

Control de acceso al medio MAC: Esta sub capa actúa como controladora del hardware subyacente (el adaptador de red). De hecho el controlador de la tarjeta de red es denominado a veces "MAC driver", y la dirección física contenida en el hardware de la tarjeta es conocida como dirección. Su principal consiste en arbitrar la utilización del medio físico para facilitar que varios equipos puedan competir simultáneamente por la utilización de un mismo medio de transporte. El mecanismo **CSMA/CD** ("Carrier Sense Multiple Access with Collision Detection") utilizado en Ethernet es un típico ejemplo de esta subcapa

2.2.5. Nivel de Red:

Las redes más pequeñas normalmente constan de una sola red de área local, pero la mayoría de las redes deben subdividirse. Una red que consta de varios segmentos de red suele denominarse inter_red (no confundir con Internet).

Las subdivisiones de una inter_red pueden planificarse para reducir el tráfico de los segmentos o para aislar las redes remotas conectadas a través de medios de comunicación más lentos. Cuando las redes se subdividen, no es posible dar por sentado que los mensajes se entregan en la red de área local. Es necesario recurrir a un mecanismo que dirija los mensajes de una red a otra.

Para entregar mensajes en una inter_red, cada red debe estar identificada de manera única por una dirección de red. Al recibir un mensaje de las capas superiores, la capa de red añade una cabecera al mensaje que incluye las direcciones de red de origen y destino. Esta combinación de datos sumada a la capa de red se denomina paquete. La información de la dirección de red se utiliza para entregar el mensaje a la red correcta. A continuación, la capa de enlace de datos puede utilizar la dirección del nodo para realizar la entrega del mensaje.

El proceso de hacer llegar los paquetes a la red correcta se denomina encaminamiento, y los dispositivos que encaminan los paquetes se denominan encaminadores. Una inter _ red tiene dos tipos de nodos:

Los nodos finales proporcionan servicios a los usuarios. Utilizan una capa de red para añadir las direcciones de red a los paquetes, pero no llevan a cabo el

correcto. Para ello, la capa de transporte incluye un número de secuencia en la cabecera del mensaje.

Muchas computadoras son multitarea y ejecutan varios programas simultáneamente. Por ejemplo, la estación de trabajo de un usuario puede estar ejecutando al mismo tiempo un proceso para transferir archivos a otra computadora, recuperando el correo electrónico y accediendo a una base de datos de la red. La capa de transporte debe entregar los mensajes del proceso de una computadora al proceso correspondiente de la computadora de destino.

Aunque las capas de enlace de datos y de red pueden encargarse de detectar errores en los datos transmitidos, además esta responsabilidad suele recaer sobre la capa de transporte. La capa de transporte puede realizar dos tipos de detección de errores:

Entrega fiable. Entrega fiable no significa que los errores no puedan ocurrir, sino que los errores se detectan cuando ocurren. La recuperación puede consistir únicamente en notificar el error a los procesos de las capas superiores.

Entrega no fiable. No significa que los errores puedan producirse, sino que la capa de transporte no los verifica. Dado que la comprobación requiere cierto tiempo y reduce el rendimiento de la red, es frecuente que se utilice la entrega no fiable cuando se confía en el funcionamiento de la red. Este es el caso de la mayoría de redes de área local. La entrega no fiable es preferible cuando los mensajes constan de un alto número de paquetes. Con frecuencia, se denomina entrega de datagramas y cada paquete transmitido de este modo se denomina datagrama.

Este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados al procesamiento. Además, garantiza una entrega confiable de la información.

i. Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por el nivel 5 (Sesión).
ii. Este nivel define como direccionar la localidad física de los dispositivos de la red.

iii. Asigna una dirección única de transporte a cada usuario.

iv. Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.

v. Define la manera de habilitar y deshabilitar las conexiones entre los nodos.

vi. Determina el protocolo que garantiza el envío del mensaje.

vii. Establece la transparencia de datos así como la confiabilidad en la transferencia de información entre dos sistemas.

2.2.7. Nivel Sesión:

El control de los diálogos entre distintos nodos es competencia de la capa de sesión. Un diálogo es una conversación formal en la que dos nodos acuerdan un intercambio de datos.

La comunicación puede producirse en tres modos de diálogo

Simple (Simplex). Un nodo transmite de manera exclusiva mientras otro recibe de manera exclusiva.

Semidúplex (Half-duplex). Un solo nodo puede transmitir en un momento dado, y los nodos se turnan para transmitir.

Dúplex total (Full-duplex). Los nodos pueden transmitir y recibir simultáneamente. La comunicación dúplex total suele requerir un control de flujo que asegure que ninguno de los dispositivos envía datos a mayor velocidad de la que el otro dispositivo puede recibir.

Las sesiones permiten que los nodos se comuniquen de manera organizada. Cada sesión tiene tres fases:

1. **Establecimiento de la conexión.** Los nodos establecen contacto. Negocian las reglas de la comunicación incluyendo los protocolos utilizados y los parámetros de comunicación.
2. **Transferencia de datos.** Los nodos inician un diálogo para intercambiar datos.
3. **Liberación de la conexión.** Cuando los nodos no necesitan seguir comunicados, inician la liberación ordenada de la sesión.

Los pasos 1 y 3 representan una carga de trabajo adicional para el proceso de comunicación. Esta carga puede no ser deseable para comunicaciones breves. Por ejemplo, considere la comunicación necesaria para una tarea administrativa de la red. Cuando una red administra varios dispositivos, éstos envían periódicamente un breve informe de estado que suele constar de una sola trama. Si todos estos mensajes se enviaran como parte de una sesión formal, las fases de establecimiento y liberación de la conexión transmitirían más datos que los del propio mensaje.

Proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos:

i. Establece el inicio y termino de la sesión.
ii. Recuperación de la sesión.
iii. Control del diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.
iv. Referencia a los dispositivos por nombre y no por dirección.
v. Permite escribir programas que correrán en cualquier instalación de red.

2.2.8. Nivel Presentación:

La capa de presentación se responsabiliza de presentar los datos a la capa de aplicación. En ciertos casos, la capa de presentación traduce los datos directamente de un formato a otro. Las grandes computadoras IBM utilizan una codificación de caracteres denominada EBCDIC, mientras que las computadoras restantes utilizan el conjunto de caracteres ASCII. Por ejemplo, si se transmiten datos de una computadora EBCDIC a otra ASCII, la capa de presentación podría encargarse de traducir de un conjunto de caracteres al otro.

Una técnica habitual para mejorar la transferencia de datos consiste en convertir todos los datos a un formato estándar antes de su transmisión. Otras funciones que pueden corresponder a la capa de presentación son la encriptación/desencriptación y compresión/descompresión de datos.

La capa de presentación es la que se implementa con menor frecuencia de las capas OSI. Se han definido pocos protocolos para esta capa. En la mayoría de los casos, las aplicaciones de red desempeñan las funciones asociadas con la capa de presentación.

i. Traduce el formato y asignan una sintaxis a los datos para su transmisión en la red.
ii. Determina la forma de presentación de los datos sin preocuparse de su significado o semántica.
iii. Establece independencia a los procesos de aplicación considerando las diferencias en la representación de datos.
iv. Proporciona servicios para el nivel de aplicaciones al interpretar el significado de los datos intercambiados.
v. Opera el intercambio.
vi. Opera la visualización.

2.2.9. Nivel Aplicación:

La capa de aplicación proporciona los servicios utilizados por las aplicaciones para que los usuarios se comuniquen a través de la red. Algunos ejemplos de servicios, son:

Transporte de correo electrónico. Gran variedad de aplicaciones pueden utilizar un protocolo para gestionar el correo electrónico. Las aplicaciones que comparten una misma interfaz de correo pueden intercambiar mensajes utilizando el gestor de correo electrónico.

Acceso a archivos remotos. Las aplicaciones locales pueden acceder a los archivos ubicados en los nodos remotos.

Ejecución de tareas remotas. Las aplicaciones locales pueden iniciar y controlar procesos en otros nodos.

Directorios. La red puede ofrecer un directorio de recursos, incluyendo nombres de nodos lógicos. El directorio permite que las aplicaciones accedan a los recursos de la red utilizando nombres lógicos en lugar de identificaciones numéricas abstractas.

Administración de la red. Los protocolos de administración de la red permiten que varias aplicaciones puedan acceder a la información administrativa de la red.

2.2.10. Relaciones entre los niveles del modelo OSI

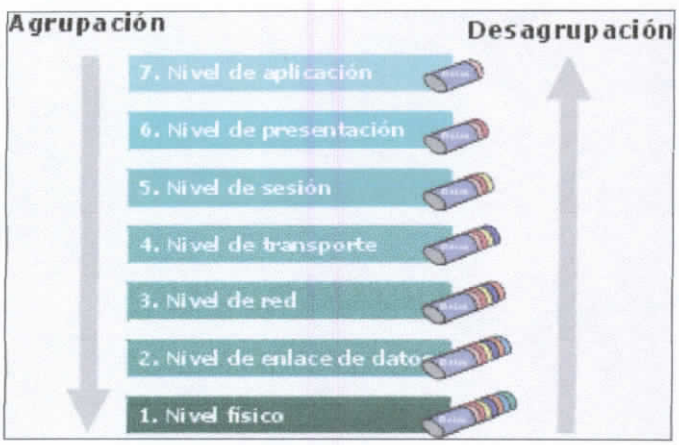
Cada nivel proporciona servicios al nivel inmediatamente superior y lo protege de los detalles de implementación de los servicios de los niveles inferiores. Al mismo

el equipo A, la información desciende hacia los niveles de enlace de datos y físico de la parte emisora, atraviesa el cable y asciende los niveles físico y de enlace de datos de la parte receptora hasta su destino final en el nivel de red del equipo B.

En un entorno cliente/servidor, un ejemplo del tipo de información enviada desde el nivel de red de un equipo A, hacia el nivel de red de un equipo B, debería ser una dirección de red, posiblemente con alguna información de verificación de errores agregada al paquete. La interacción entre niveles adyacentes ocurre a través de una interfaz. La interfaz define los servicios ofrecidos por el nivel inferior para el nivel superior y, lo que es más, define cómo se accede a dichos servicios. Además, cada nivel de un equipo aparenta estar en comunicación directa con el mismo nivel de otro equipo.

2.2.11. Paquetes de datos y el modelo OSI

Figura 2.9 Esquema de los Paquetes de Datos del Modelo OSI



El proceso de creación de paquetes se inicia en el nivel de aplicación del modelo *OSI*, donde se generan los datos. La información a enviar a través de la red comienza en el nivel de aplicación y desciende a lo largo de los siete niveles.

En cada nivel, se agrega a los datos información relevante de ese nivel. Esta información es utilizada por el correspondiente nivel del equipo receptor. El nivel de enlace de datos del equipo receptor, por ejemplo, leerá la información agregada en el nivel de enlace de datos del equipo emisor. En el nivel de transporte, el bloque de datos original se divide en los paquetes reales. El protocolo define la estructura de los paquetes utilizados por los dos equipos.

Cuando el paquete alcanza el nivel de transporte, se agrega una secuencia de información que guía al equipo receptor en la desagrupación de los datos de los paquetes. Cuando, finalmente, los paquetes pasan a través del nivel físico al cable, contienen información de cada uno de los otros seis niveles.

2.2.12. Dispositivos de Red

Existen una variedad de dispositivos de seguridad entre los mas importantes son los siguientes:

2.2.12.1 Router

Los routers, como dispositivos inteligentes, controlan la velocidad y congestión de las líneas y así elegirán la mejor ruta. Es un conmutador de paquetes que opera en el nivel de red del modelo OSI. Sus principales características son:

i. Permiten interconectar tanto redes de área local como redes de área extensa.

ii. Proporcionan un control del tráfico y funciones de filtrado a nivel de red, es decir, trabajan con direcciones de nivel de red, como por ejemplo, con direcciones IP.

iii. Son capaces de rutear dinámicamente, es decir, son capaces de seleccionar el camino que debe seguir un paquete en el momento en el que les llega, teniendo en cuenta factores como líneas más rápidas, líneas más baratas, líneas menos saturadas, etc.

2.2.12.2. Firewalls

Los Firewalls son barreras creadas entres redes privadas y redes públicas como por ejemplo, Internet. Originalmente, fueron diseñados por los directores de informática de las propias empresas, buscando una solución de seguridad. En la actualidad, los sistemas de seguridad proporcionados por terceras empresas, son la solución más escogida. Los Firewalls son simples en concepto, pero estructuralmente complejos. Examinan todo el tráfico de entrada y salida, permitiendo el paso solamente al tráfico autorizado.

2.2.12.3. Switch

Un switch (en castellano "conmutador") es un dispositivo electrónico de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).

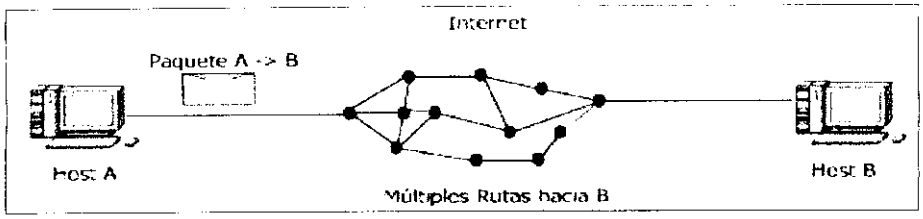
Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo se dirija únicamente desde el puerto origen al puerto que permite alcanzar el dispositivo destino. En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

2.2.13. Enrutamiento.

La función principal del nivel de Internet es hacer llegar los paquetes de una máquina a otra dando igual cual sea el medio físico que utilicen y los datos que estén transmitiendo

Proceso de descubrimiento de una ruta hacia el host de destino. Como se puede apreciar en la figura 2.10 el paquete enviado por el host A tiene como objetivo alcanzar el host B, para lo cual tendrá que ser ayudado por un dispositivo de red como por ejemplo un router que le permita decidir que ruta deberá tomar para cumplir con su propósito.

Figura 2.10 Esquema del Camino que un Paquete sigue hacia su Destino



El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host de destino.

2.2.13.1. Ventajas y Desventajas de Enrutar

Tabla 2.1 Principales Ventajas y Desventajas de Enrutar

Ventajas	Desventajas
• Optimiza el tiempo de entrega de los paquetes. • Disminuye la presencia de bucles. • Permite conocer parcial o totalmente la topología de las redes del entorno.	• Algunos protocolos de enrutamiento pueden llegar a consumir demasiados recursos de hardware. • Diseños estrictos de red cuando se maneja redes demasiado grandes.

2.2.13.2. Clases de Enrutamientos

2.2.13.2.1. El Procedimiento de Enrutamiento

a) Estático

Las tablas de enrutamiento son configuradas por el administrador de la red de una manera manual lo que implica que las rutas permanezcan sin cambios hasta que los requerimientos sean substituidos.

b) Cuasi-Estático

Es similar al estático con la particularidad de que se torna un poco mas adaptable ya que en vez de dar una sola ruta fija, se dan otras rutas alternativas en caso de que la principal falle.

c) Centralizado

En este tipo de enrutamiento un solo dispositivo de red (central o principal) es el encargado de calcular las tablas de enrutamiento para cada uno de los dispositivos secundarios enlazados a este.

d) Aislado

Se caracteriza porque el dispositivo de red reenvía un paquete que no le pertenece por todos los demás enlaces activos que posea con otras redes, sin hacer uso del enlace por el cual recibió el paquete.

e) Distribuidor

i. Estado de Enlace

Este tipo de enrutamiento está caracterizado por su gran adaptación a los cambios que puedan surgir en la topología de red y esto se debe a que cada dispositivo de control de tráfico elabora su propia tabla de enrutamiento en base al conocimiento total de la topología que posee, manteniendo siempre informados a todos los dispositivos que pertenezcan al entorno de su red únicamente cuando existan modificaciones lo cual da como resultado una rápida convergencia[1].

ii. Vector Distancia

Cada controlador de tráfico realiza actualizaciones constantes de su tabla de enrutamiento a todos sus vecinos, lo que implica una velocidad de convergencia más lenta que en el enrutamiento de estado de enlace. En este tipo de enrutamiento cada dispositivo conoce la topología de red desde el punto de vista de los vecinos. Es fácil de implementar. Su nombre deriva de

[1] Convergencia.- Tiempo que le toma a un grupo de dispositivos de red, para ponerse de acuerdo sobre el estado actual de la red después de un cambio en la topología.

las actualizaciones que realiza mediante vectores distancia de longitud variable que indican la distancia que existe a un determinado dispositivo de red.

2.2.13.2.2. Las Tablas de Enrutamiento Empleadas:

a) Enrutamiento Salto a Salto

Se fundamenta en el hecho de que cada dispositivo de red no necesita conocer la trayectoria completa que debe seguir un paquete hasta su destino, tan solo debe saber donde se encuentra el siguiente controlador de tráfico que a su vez se encargará de enviar el paquete por la mejor ruta al dispositivo adyacente y así sucesivamente. Este tipo de enrutamiento es complejo de administrar en los sistemas intermedios y conlleva a inconsistencias cuando se producen bucles[2] debido a que no se tiene una visión completa de la red.

b) Enrutamiento Fijado en Origen

Difiere totalmente del anterior ya que los dispositivos finales son los encargados de conocer la ruta que deben seguir los paquetes hasta su destino. Por lo que los controladores de tráfico intermedios se convierten en dispositivos que simplemente dejan pasar la información sin consultar en tablas de enrutamiento en caso de tenerlas. La gran ventaja que presenta este mecanismo de trabajo es que se eliminan los bucles.

2.2.14. Direccionamiento de paquetes

La mayoría de los paquetes de la red se dirigen a un equipo específico y, como resultado, obtienen la atención de un único equipo. Cada tarjeta de red ve todos los paquetes enviados en su segmento de cable, pero interrumpe el equipo sólo si la dirección del paquete coincide con la dirección individual de la tarjeta. De forma alternativa, se puede utilizar una dirección de tipo difusión múltiple. Los paquetes enviados con una dirección de tipo difusión múltiple pueden recibir la atención simultánea de varios equipos de la red.

---

[2]Bucle.- Ruta donde los paquetes nunca alcanzan su destino, sino que recorren repetidamente una serie constante de dispositivos de red.

2.2.14.1. Cómo dirigir los paquetes

Las componentes de red utilizan la información de direccionamiento de los paquetes para dirigir los paquetes a sus destinos o para mantenerlos alejados de las posiciones de la red a las que no pertenecen. Las dos funciones siguientes juegan un papel principal en la dirección apropiada de paquetes:

Reenvío de paquetes.

Los equipos envían un paquete al siguiente componente de red apropiado en base a la dirección del encabezado del paquete.

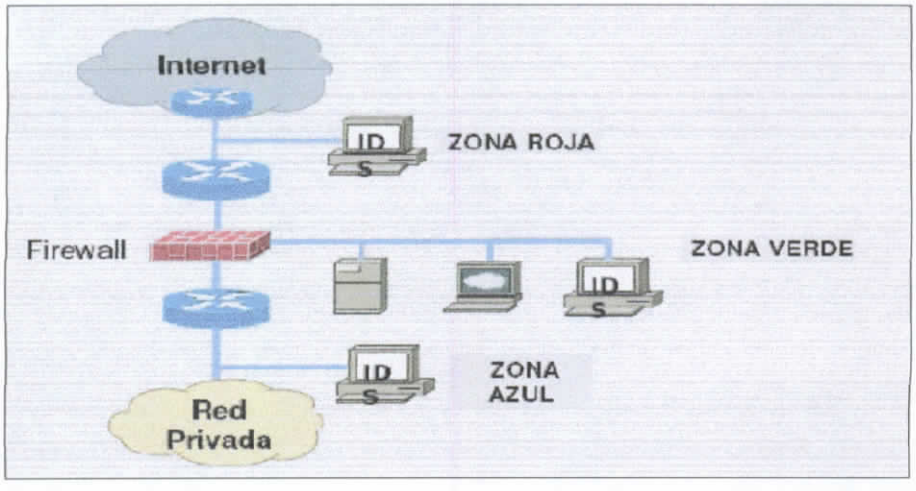
Filtrado de paquetes.

Los equipos utilizan criterios, como una dirección, para seleccionar los paquetes específicos

2.3. Firewall (Cortafuegos)

El Firewall en las redes es un dispositivo físico o lógico que protege una red privada del resto de la red (pública). Ahora hay dos redes distintas que comparten un computador. El computador que actúa de cortafuegos, al que de ahora en adelante llamaremos "cortafuegos", puede comunicarse tanto con la red protegida como con la Internet. La red protegida no puede comunicarse con la Internet, y la Internet no puede comunicarse con la red protegida, dado que hemos deshabilitado el reenvío IP en el único ordenador que las conecta.

Figura 2.11 Esquema del Firewall en la Red



El Firewall actúa como un filtro que controla el paso de información de una red a otra. Normalmente ubicado en la frontera de la red. Evita que intrusos tengan acceso a información confidencial. Puede ser un dispositivo de Hardware o Software. También protege a la red de diversas formas. Puede proporcionar servicios de encubrimiento que nieguen o garanticen los accesos basados en: el nombre del usuario, el nombre del host, y el protocolo TCP/IP, etc. Un cortafuegos puede suministrar también una variedad de servicios que dejen paso a los usuarios autorizados (si se implementa un PROXY) mientras excluyen a los no autorizados. Al mismo tiempo, asegura que todas las comunicaciones entre la red e Internet dan la impresión de finalizar en el cortafuegos, si se usa NAT (Network Address Translation), evitando que el mundo externo pueda vislumbrar en modo alguno la estructura de la red.

Un Firewall hace las veces de un portero en un edificio, verifica quien entra, quien sale y más importante aún que lleva consigo. Muchas de las amenazas a la perdida de información, como virus, gusanos y ataques combinados explotan vulnerabilidades como puertos abiertos para entrar en las redes.

Un firewall es un dispositivo que funciona como barrera defensiva entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local e Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Los firewalls fueron creados con la finalidad de ofrecer seguridad. Estos principalmente protegen de intrusos, que deseen acceder desde el Internet, a las redes privadas con la finalidad de manipular datos, sistemas o servicios existentes dentro de una red privada. Pero un firewall también sirve para salvaguardar la información dentro de la red privada de sus propios usuarios por ejemplo en una empresa una de las políticas podría ser que el departamento de Recursos Humanos no tenga acceso al departamento de contabilidad.

2.3.1. Características Principales

i. Es un filtro que controla el paso de información de una red a otra.
ii. Normalmente ubicado en la frontera de la red

iii. Evita que intrusos tengan acceso a información confidencial

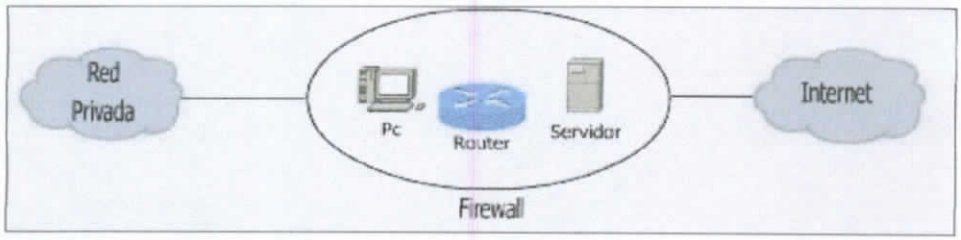
iv. Puede ser un dispositivo de Hardware o Software.

2.3.1.1. Los firewall básicamente hacen uso de:

i. Filtrado de paquetes

ii. Servidores proxy

Figura 2.12 Esquema General de un Firewall



Como se puede apreciar en la figura 2.12 un firewall puede estar alojado solamente en un computador de escritorio, en un ruteador o en un servidor de aplicaciones y servicios o ser una estructura un poco más compleja en la que el cortafuegos sea la unión de algunos de estos dispositivos, eso sí cualquiera que sea la arquitectura que se esté utilizando, estos dispositivos deben estar separados del resto de la red privada para que ninguna petición entrante pueda conseguir directamente recursos de la red privada.

2.3.2. Firewall, la muralla defensiva de un PC

Mientras se mantiene conectado a Internet, constantemente se está enviando y recibiendo información en pequeñas unidades, que contiene la dirección de quien envía el mensaje y del receptor. Pero al igual que con los correos electrónicos, no siempre se recibe en el ordenador todos los contenidos que se quisiera, ya que a veces, algunos son completamente innecesarios o peligrosos para el rendimiento del equipo. Para evitar en lo posible este tipo de intrusiones o ataques, surgieron los firewall, una especie de murallas defensivas contra los "cracker" que actúan en la Red.

Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, el correo o el IRC. Dependiendo del servicio decide si lo permite o no. Además, examina si la comunicación es entrante o saliente además depende que la dirección puede validarla o no.

2.3.3. Como funcionan los Firewall

Se manejan por zonas (seguras o no) o bien por niveles de seguridad, los que establece el usuario según el grado de permisividad que le imponga al equipo.

Se trata de aplicaciones destinadas a prevenir que penetren en la PC elementos no deseados vía Internet. Para eso concentran todo el flujo entrante y saliente entre la PC e Internet y bloquea los pedidos de enlaces no solicitados por el usuario potencialmente inseguro, instalaciones clandestinas de programas y algunos hasta bloquean pop ups, publicidades, etc.

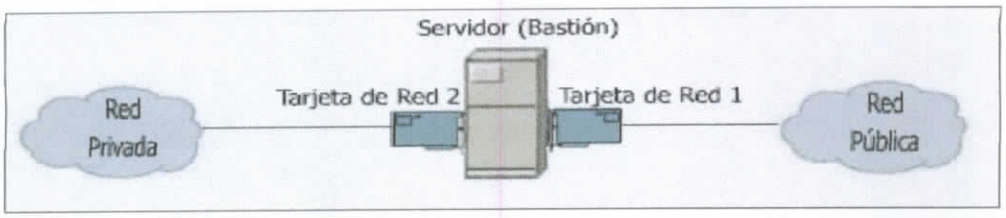
2.3.4. Tipos de peligros que puede evitar un firewall

i. Instalación y ejecución de programas instalados clandestinamente desde Internet, que pueden llegar a transferir datos personales de los usuarios a otros sitios.
ii. Acceso de terceros por fallas o errores de configuración de Windows (por ejemplo de NetBIOS).
iii. Instalación de publicidad (advertisers) o elementos de seguimiento (track) como las cookies.
iv. Troyanos: Aplicaciones ocultas que se descargan de la red y que pueden ser usadas por terceros para extraer datos personales
v. Reducción del ancho de banda disponible por el tráfico de banners, pop ups, sitios no solicitados, y otro tipo de datos innecesarios que ralentizan la conexión.
vi. Utilización de la línea telefónica por terceros por medio de Dialers (programas que cortan la actual conexión y utilizan la línea para llamadas de larga distancia)

2.3.5. Arquitecturas de Firewall

2.3.5.1. Host de Doble Conexión (Dual-Homed Gateway)

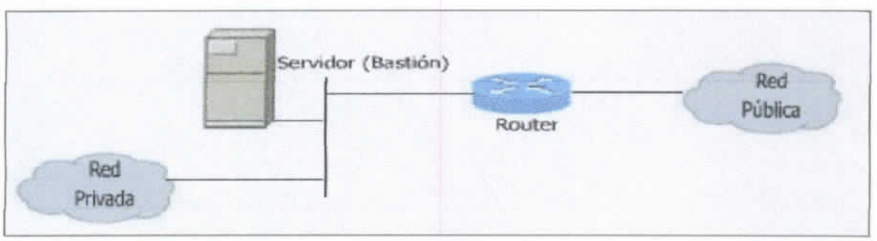
Figura 2.13 Arquitectura Host de Doble Conexión



Esta arquitectura como se puede apreciar en la figura 2.13 es muy fácil de implementar y no implica gastos elevados. El servidor utilizado para la construcción de este firewall debe poseer dos tarjetas de red cuyo objetivo es separar la red pública de la privada. Ambas redes se comunican la mayoría de las veces por el uso de software que ejecuta proxys. Algo que se debe tener muy en cuenta es la necesidad de inhabilitar la opción de enrutamiento para el caso de determinados sistemas operativos ya que de esta manera el servidor trabajará como un cortafuegos, caso contrario si dicho parámetro está activado se permitirá que el servidor funcione como un puente de red y por lo tanto existirá comunicación directa entre la red pública y la privada lo cual anula al firewall.

2.3.5.2. Filtrado de Host (Screened Host)

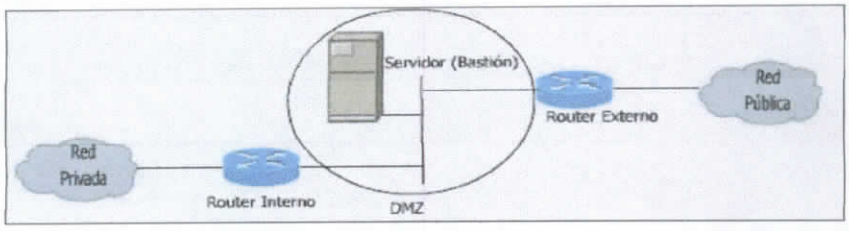
Figura 2.14 Arquitectura Filtrado de Host



El Filtrado de host es una topología más segura que la anterior ya que está conformada por un ruteador para el filtrado de paquetes, que bloquea el tráfico proveniente desde la red pública hacia la red privada, y por un servidor que soporta servicios mediante proxy mismo que es el único que si recibe información desde Internet a través del router. Es fácil de mantener y de implementar y su costo es de mayor valor que el de una arquitectura de doble conexión. Las dos arquitecturas mostradas anteriormente centran su seguridad en el servidor y por lo tanto poseen la gran desventaja de que si un usuario logra acceder desde la red pública al servidor podrá tomar el control de la red interna y causar daños indeseables.

2.3.5.3. Filtrado de Subred (Screened Subnet)

Figura 2.15 Arquitectura Filtrado de Subred



El filtrado de subred es la arquitectura que posee mayor seguridad con respecto a las dos anteriores, razón por la cual su implementación involucra mayor complejidad y costo.

Esta topología como se muestra en la fig. 2.15 está compuesta por un ruteador externo y otro interno que son los encargados de controlar el tráfico que tenga por destino la red local mientras que en la DMZ[1] (De-Militarized Zone) se coloca el o los servidores que soportan servicios mediante proxy que son los encargados de controlar el tráfico de entrada y salida hacia el Internet.

También se suele colocar en esta zona puntos de acceso inalámbricos y servidores de conexión dialup[2].

Como se puede apreciar si un atacante logra burlar al primer ruteador e ingresar al servidor en la DMZ aún tiene un ruteador por evadir.

Cabe señalar que las arquitecturas anteriores no son las únicas ya que pueden crearse nuevas realizando distintas combinaciones de todas las presentadas hasta el momento.

---

[1] DMZ (De-Militarized Zone).- En español Zona Desmilitarizada, se refiere a aquella zona donde se colocan sistemas que por sus características presentan altos riesgos de seguridad. Los sistemas que se colocan en esta zona son aquellos que ofrecen servicios hacia el exterior (cuyo tráfico debe ser aceptado por el firewall debido a requerimientos de la organización).

[2] Dial up.- Método ampliamente usado de acceder a la Internet. Una conexión "dialup" utiliza líneas telefónicas estándar para enlazar una computadora con otra, vía modem.

Tabla 2.2 Arquitecturas de Firewall

Tipo de Firewall	Descripción
Host de Doble Conexión	• Económico, fácil de implementar y administrar. • Utiliza dos tarjetas de red que separan la red privada de la pública. • La mayoría de las veces hace uso de programas que habilitan servicios de proxy que son los encargados de establecer comunicación entre la red pública y la privada.
Filtrado de Host	• Costo moderado, fácil de implementar y administrar. • Está conformada por un router y un servidor proxy.
Filtrado de Subred	• Es costo alto y complicado de implementar. • Su arquitectura comprende dos routers y un servidor proxy.

2.3.6. Tecnologías de Firewall

Veamos las 3 divisiones principales, aunque pueden haber implementaciones híbridas.

a) Filtrado de Paquetes - Primera generación

Es el firewall más sencillo, se basa en permitir o denegar el tráfico basado en el encabezado de cada paquete. Como no guarda los estados de una conexión, es decir no tiene el concepto de una sesión. Este tipo de implementación era popular antes de la aparición de los Firewalls y aún se encuentra ya que normalmente hace parte del sistema operativo (Linux o Windows)

b) Stateful Application inspection

A diferencia del anterior el Stateful Application permite abrir "Puertas" a cierto tipo de tráfico basado en una conexión y volver a cerrar la puerta cuando la conexión termina.

Adaptan las reglas básicas de firewall para acomodarse a las necesidades específicas de cada protocolo. El Stateful Firewall mantiene un registro de las conexiones, las sesiones y su contexto. Este módulo tiene su asiento entre la capa de Data Link y Network.

c) Full application inspection

También conocido como Application Gateway. Es un firewall que es capaz de inspeccionar hasta el nivel de aplicación. No solo la validez de la conexión sino todo el contenido de la trama. Es considerado como el más seguro. Todas las conexiones van a través del firewall.

i. Transparencia (Proxy Transparente)

Transparencia es uno de los desarrollos más grandes en la segunda generación de gateways de aplicación. Una de las desventajas de los firewalls típicos es que cada estación tenía que ser configurada para comunicarse con el Proxy y saber su ubicación.

ii. Detección de Intrusos (IDS)

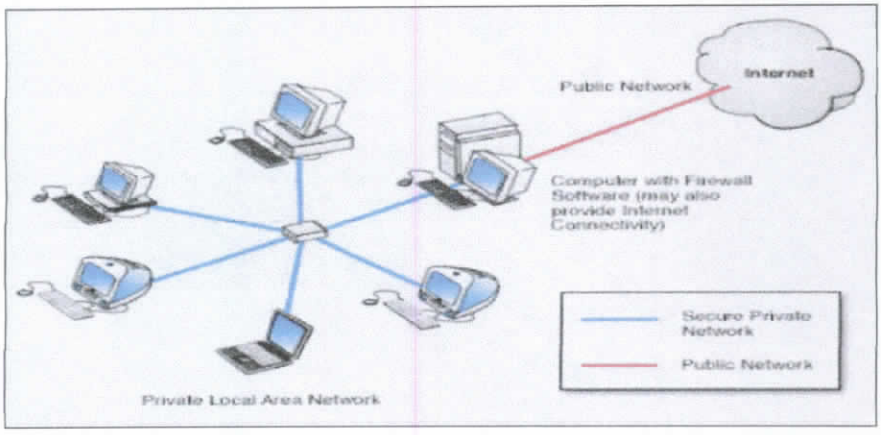
Normalmente un Firewall mantiene bitácoras con registros de actividad y guardan en ellos actividad anormal y registro de eventos. Muy pocos han integrado en sus capacidades la facilidad de alertar en tiempo real al administrador en caso de un evento. Esta capacidad se conoce como **IDS**. Detección de Intrusión y es una característica muy deseable de seguridad, ya que de nada sirve revisar bitácoras cuando la intrusión ya pasó, y el rastro esta frío.

2.3.7. Tipos de Firewall

Actualmente, podemos encontrar dos tipos de Firewall: de software y de hardware. Estos últimos son los más caros, pero también los mejores. Ambos, se basan en el filtrado de información.

2.3.7.1. Firewall de software

Figura 2.16 Esquema del Firewall de Software



En el Mercado existe mucha variedad de software y hardware que permite implementar o complementar soluciones de seguridad de red, variando sus precios en base a la calidad, tecnología, propiedad, certificaciones, mantenimiento y otros criterios que son válidos al momento de seleccionar y optar por una de las alternativas, tomando en cuenta los requerimientos y alcances de la organización.

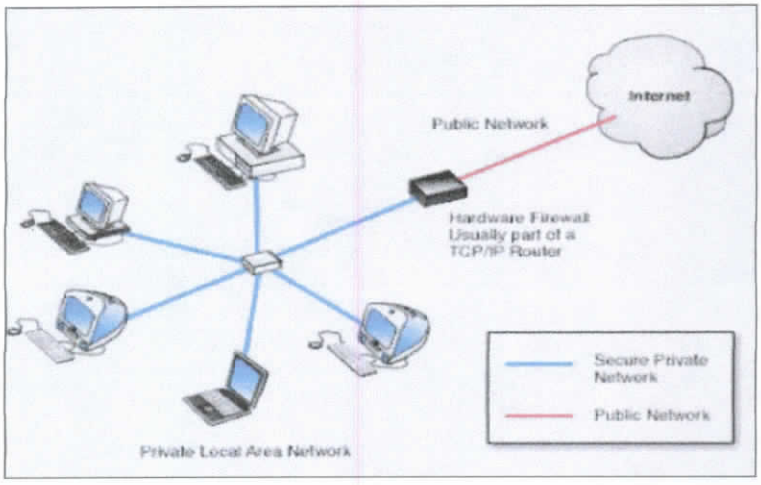
Estos programas son los más comunes en los hogares, ya que a parte de resultar mucho más económicos que el hardware, su instalación y actualización es más sencilla.

Actualmente, los sistemas operativos más modernos como Windows XP y Linux integran soluciones básicas de firewall, en algunos casos, como en el software libre, son muy potentes y flexibles, pero requieren un gran conocimiento en redes y puertos necesarios para las aplicaciones.

Windows Firewall (anteriormente denominado Internet Connection Firewall o ICF) es un cortafuego de filtrado basado en software para Microsoft Windows XP y Microsoft Windows Server 2003. Windows Firewall proporciona protección para los PC que se encuentran conectados a una red, impidiendo las conexiones entrantes no solicitadas mediante TCP/IP

2.3.7.2. Firewall de Hardware

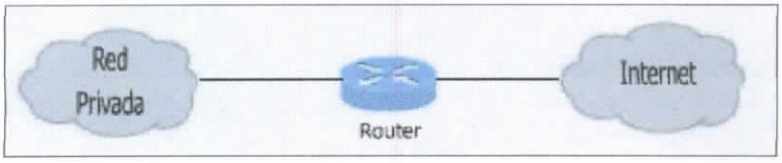
Figura 2.17 Esquema del Firewall de Hardware



Los firewall de hardware se utilizan más en empresas y grandes corporaciones. Normalmente son dispositivos que se colocan entre el router y la conexión telefónica. Como ventajas, podemos destacar, que al ser independientes del PC, no es necesario configurarlos cada vez que reinstalamos el sistema operativo, y no consumen recursos del sistema.

2.3.7.3. Firewall a Nivel de Red

Figura 2.18 Firewall a Nivel de Red utilizando un Ruteador



Este tipo de firewall utiliza dispositivos como ruteadores (filtradores de paquetes) o computadores cuyos sistemas operativos permiten crear conjuntos de reglas (listas de sentencias de código) para aplicar las políticas de seguridad de una determinada entidad al momento de controlar el tráfico haciendo básicamente uso de:

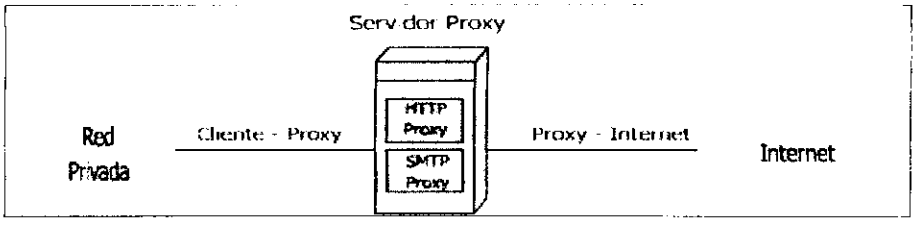
i. Direcciones IP de origen/destino de los datos.
ii. Protocolo de sesión de los datos. TCP, UDP o ICMP.
iii. Si el paquete es el inicio de una petición de conexión.
iv. El puerto de aplicación de origen/destino del servicio deseado.

Los firewall a nivel de red se caracterizan por ser transparentes al usuario y por lo tanto consumir menos recursos. Por otro lado entre las limitaciones que presenta este tipo de firewall están que las reglas son dificiles de probar una vez que ya están implementadas, además el administrador de la red necesita tener un conocimiento preciso de cómo manejar la estructura que poseen los paquetes que se transmiten.

2.3.7.4. Firewall a Nivel de Aplicación

Normalmente llamado servidor proxy[1], que es un programa pequeño y sencillo que se lo instala en el sistema operativo de un computador y que al igual que un filtrador de paquetes es capaz de controlar el tráfico existente en la red, generado por servicios como FTP, Telnet, HTTP, SMTP, etc. utilizando reglas de filtrado que son más fáciles de configurar.

Figura 2.19 Firewall a Nivel de Aplicación



Otra de las características de manejar servidores proxy es el hecho de que cada programa o servidor proxy como se puede apreciar en la fig. 2.19 es totalmente independiente.

Lo que implica que si un servicio como por ejemplo el de SMTP es atacado puede desinstalarse sin afectar la operación de los demás servicios a los que pueden estar accediendo otros usuarios.

Una de las desventajas que presenta este tipo de firewall es que no resulta transparente para el usuario ya que se deben realizar pasos adicionales para acceder a los servicios deseados.

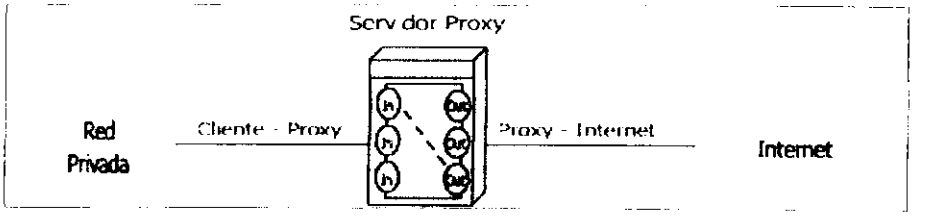
[1] Servidor proxy.- También actúa como una cache de páginas web ya que son capaces de almacenar las páginas web visitadas por los usuarios y de esta manera si otro usuario quiere acceder a alguna página que el servidor proxy tenga guardada, no tendrá que acceder a Internet sino que directamente se la enviará al usuario.

2.3.7.5. Firewall a Nivel de Circuito

También conocido como proxy transparente. Bastante similar a un firewall a nivel de aplicación, en los cuales se tiene que configurar en cada computador de la red interna la comunicación con el servidor proxy.

Con un firewall a nivel de circuito ya no se necesita realizar ningún tipo de configuración en cada computador por lo que se establece una comunicación a manera de circuito como se puede apreciar en la figura 2.20, lo cual implica que sea totalmente transparente para el usuario.

Figura 2.20 Firewall a Nivel de Circuito



Resumen de los tres tipos de firewall:

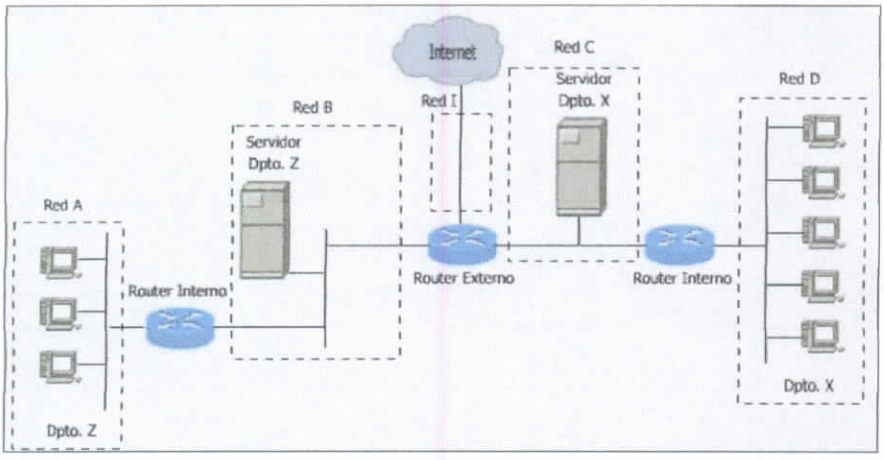
Tabla 2.3 Tipos de Firewall

Tipo de Firewall	Descripción
Firewall a Nivel de Red	• Crea reglas de control haciendo uso de herramientas incorporadas en los sistemas operativos de ciertos dispositivos de hardware creados justamente para realizar el control de paquetes, como por ejemplo routers. Así como también se puede hacer uso de sistemas operativos especializados en el manejo de cortafuegos como Linux.
Firewall a Nivel de Aplicacion	• Realiza un filtrado de paquetes de una manera mas especifica que un firewall a nivel de red. • Utiliza software que es el encargado de habilitar el servicio de proxy. En dicho software se implementan las reglas para controlar el tráfico de paquetes. • Además requiere de ciertas configuraciones, dentro de un navegador de Internet.

Firewall a Nivel de Circuito	• Funciona de igual manera que un firewall a nivel de aplicación, la gran diferencia radica en que el usuario no necesita realizar cambios en los parámetros de un navegador para poder acceder al Internet, razón por la cual se vuelve totalmente transparente.

Para facilitar la comprensión de un sistema de firewall (combinación de distintos tipos y arquitecturas de cortafuegos), se ha ilustrado un diagrama de red sencillo, ya que como se puede apreciar en la fig. 2.21 si la empresa creciera el sistema de firewall sería más complejo.

Figura 2.21 Sistema de Firewall de una Empresa



La empresa está empleando firewalls a nivel de red y a nivel de aplicación, así como también una arquitectura de filtrado de subred doble.

Las políticas de seguridad de la empresa incluyen los siguientes requerimientos:

a) Permitir que los usuarios de los departamentos X y Z se conecten solo a su servidor y a la Internet.

Esta necesidad es muy práctica ya que se está restringiendo que ambos grupos de usuarios no puedan acceder a datos que no sean propios de su departamento. Por lo tanto para poder realizar esto se deberían aplicar reglas de filtrado en los ruteadores como las siguientes:

i. Permitir que los usuarios de la red D se conecten a la red C
ii. Permitir que los usuarios de la red D se conecten a la red I
iii. Negar a los usuarios de la red D el acceso a la red B y A

iv. Permitir que los usuarios de la red A se conecten a la red B

v. Permitir que los usuarios de la red A se conecten a la red I

vi. Negar a los usuarios de la red A el acceso a la red C y D

b) Los distintos departamentos solo se podrán comunicar vía correo electrónico. Para cumplir con esta política se deberá instalar el servicio de servidor proxy SMTP en los servidores de ambos departamentos.

c) Los departamentos solamente podrán utilizar el Internet con fines de investigación y no podrán descargar archivos.
La última política implica instalar el servicio de servidor HTTP pero no el de FTP.

2.3.9. Beneficios de un firewall en Internet

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se expone al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (envudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles.

2.3.10. Configuración de Firewall.

La configuración del Firewall lo podemos observar en el anexo, en donde se encuentran los pasos en una forma detallada.

Capitulo III

Desarrollo del Proyecto

3.1. Análisis de la Implementación

Para la implementación del dispositivo de seguridad, es necesario tener conocimiento de la dirección IP pública, que es la información necesaria que nos provee el servicio de Internet para la configuración, para que el dispositivo actue correctamente, y así proteger al servidor de los hackers, virus, etc. Otra característica importante es que el dispositivo tenga la capacidad necesaria para proteger a la red que esta conformada por los laboratorios asignados para la labor academia, y la parte administrativa.

3.1.1.Análisis y estudio de la Red Actual de la PUCESA

Tabla 2.4 Análisis de la Red

Laboratorio	# Maquinas	Clase
Lab # 1	12	iMAC
Lab # 2	12	PC´s
Lab # 3	10	PC´s
Lab # 4	12	PC´s
Lab # 5	12	PC´s
Lab # 6	28	PC´s
Área Administrativa	30	PC´s

Diagrama de la Red de los Laboratorios en el Campus Universitario de la PUCESA

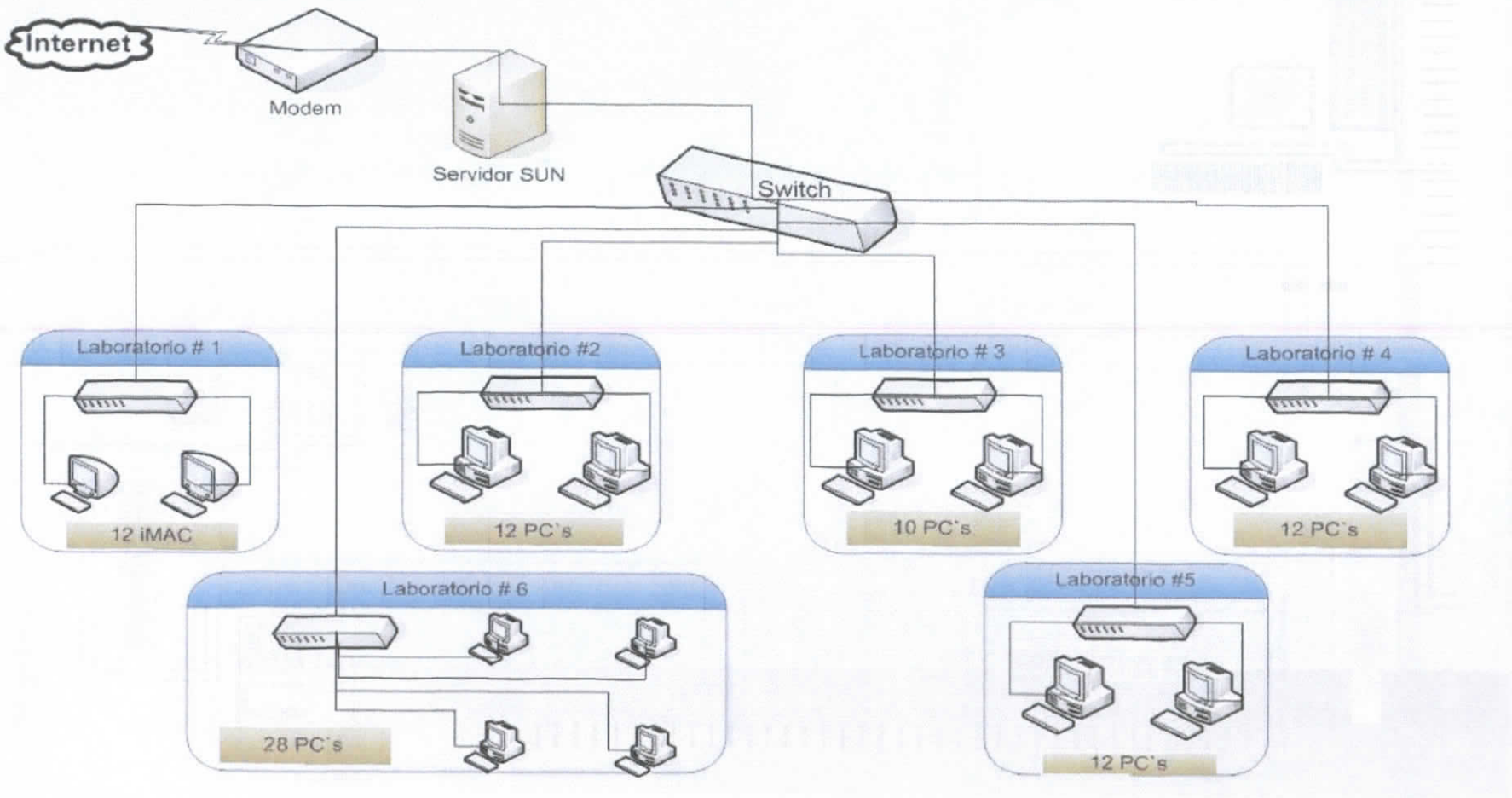
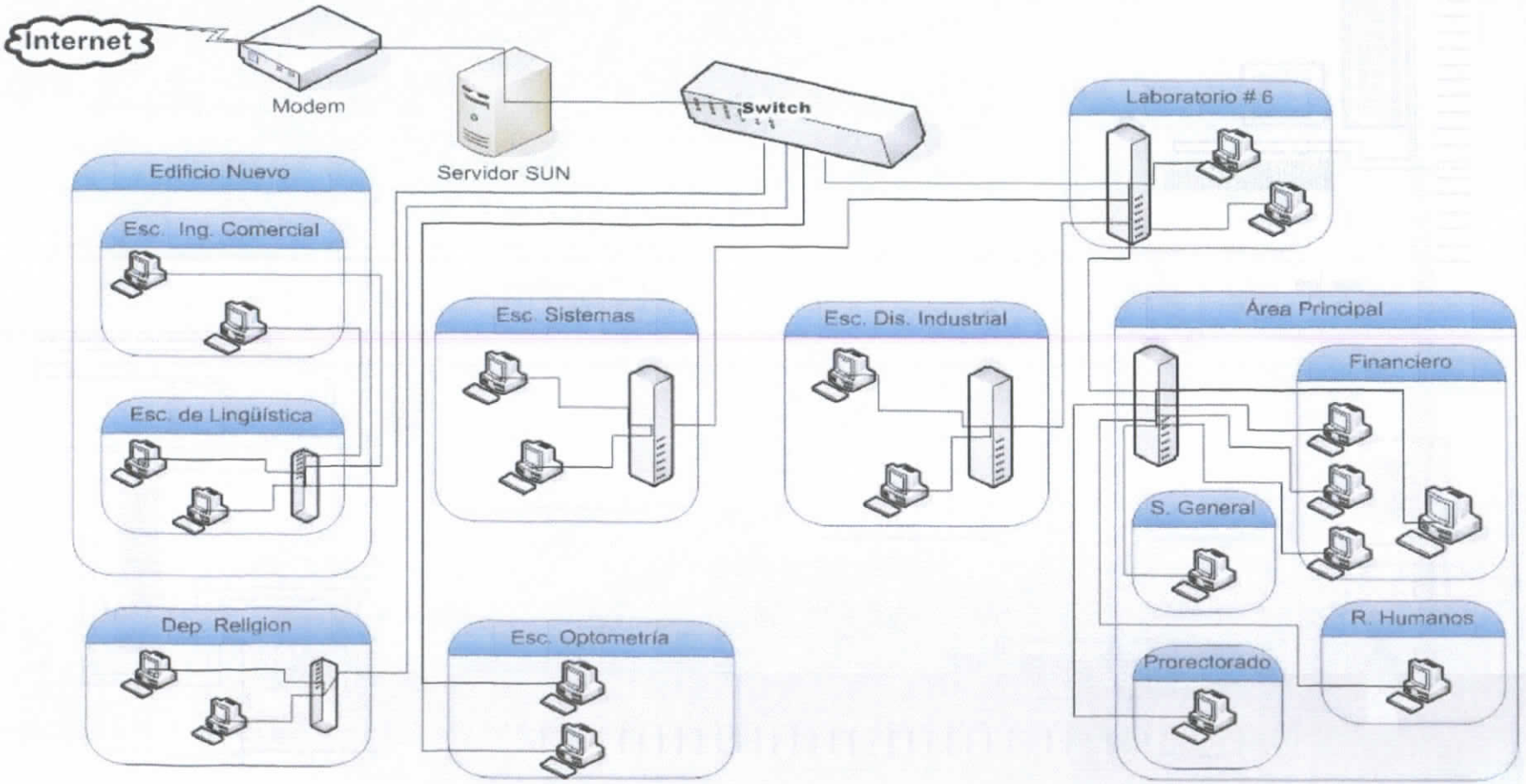


Diagrama de la Red de la parte Administrativa en el Campus Universitario de la PUCESA



3.1.2. Análisis de requisitos sobre la implementación

Para poner en marcha el proyecto de implementación de dispositivos de seguridad en la red del Campus Universitario de la PUCESA, fue necesario la adquisición de un dispositivo de seguridad, como lo es el Firewall con las características indispensables para proveer seguridad absoluta a la red al servidor, además es necesario la obtención de un nuevo Switch para obtener un mejor rendimiento del Firewall.

3.1.3. Análisis de Requerimientos del Hardware

El Firewall Hardware es una gran herramienta de protección para la red de la universidad, sin duda para todas las redes que necesiten estar protegidas, el mismo que requiere de una dirección IP pública, propia para el Firewall

3.1.4. Funcionalidad del Proyecto

La instalación del dispositivo de seguridad en la red de la PUCESA se realizó satisfactoriamente para la validación del proyecto, ya que al momento la Universidad solamente dispone de una dirección IP. En la instalación del Firewall se requiere una dirección IP propia necesario para que el Firewall sea reconocido en la red pública y así realizar su función. La dirección IP existente se está utilizando para el Servidor Web. El mismo que es un servidor en producción y es imposible deshabilitar ya que ocasionaría problemas.

Para su funcionamiento continuo es necesaria la adquisición de un bucle de direcciones IP, y cambiar la configuración actual del MODEM, que tiene un tipo de configuración llamado bridge, con la adquisición de nuevas direcciones IP la configuración cambia a tipo Router para así tener varias direcciones IP disponibles.

Basándonos en el problema actual de la red, de la Universidad Católica sede Ambato. La inexistencia de un dispositivo físico que contrarreste los ataques de hackers, virus al servidor de la PUCESA, la inseguridad en la navegación en Internet, y para estar protegidos sobre algún tipo de ataque al servidor que es el cerebro de la red hemos decidido implementar un dispositivo de seguridad que nos brinde la mayor protección.

Los pasos que se ejecutaron para la instalación fueron: investigar que tipo de hardware nos podría ayudar a solucionar los problemas antes descritos, además de obtener información, si el dispositivo nos podría ayudar a proteger a toda la red. Con la información recopilada se decidió por el firewall físico con las características necesarias para la solución a los problemas

Las políticas de seguridad que se emplean son:

- El filtrado de contenidos es la opción donde se configura, para habilitar y deshabilitar las paginas Web.
- Deshabilitar el ping es la opción que nos permite proteger el servidor de los hackers, ya que una vez deshabilitado el ping el hacker no puede ingresar al servidor.
- El control de las Pc's por medio del bloqueo con la dirección IP de cada unas de las Pc's
- Configurar el ancho de banda para los usuarios de la red para así poder controlar la información que se transfiere desde el Internet.
- Configurar los permisos para las actividades deacuerdo a los puertos como por ejemplo correo electrónico, Chat etc.

Las políticas antes descritas son las más adecuadas en lo que se refiere a seguridad de redes porque así nos permite proteger a la red de programas maliciosos.

El Firewall VPN de 3com se nos brinda una serie de ventajas como son: protegerse de ataques de los hacker, provee de un paquete de Inspección (SPI), para impedir que los intrusos ingresen a la red, bloqueo de ataques sobre (DoS), usando un modelo de detección, estas funciones que el firewall realiza son indispensables para dar seguridad en la red del campus universitario, además, que el costo para un proyecto estudiantil es asequible.

De acuerdo a la validación y verificación de resultados los problemas que afectan a la red, se solucionaron ya que el firewall es un dispositivo con las características necesarias para poder solucionar los problemas antes descritos, además de otras actividades que nos permite realizar como lo es VPN, DHCP, NAT. Y por ende la

hipótesis se cumplió en lo que se refiere a la seguridad de la red y la protección del Servidor SUN.

Una vez implementado el dispositivo de seguridad, la funcionalidad de este nos permitirá obtener resultados útiles como tener una red confiable y segura, libre de virus y ataques de hacker que son los principales causantes de daños dentro de la red de la universidad. Así también el Firewall nos ofrece una serie de indicadores que se ponen en alerta cuando una de las herramientas de ataque quiere hacer su función.

3.1.5. Restricciones

Para la manipulación y la configuración del Firewall de acuerdo a las necesidades de la red de la universidad, solo va poder acceder el Administrador del centro de cómputo, que es quien tendrá la clave y el permiso para la configuración. Como también será quien deshabilite las páginas que no tienen relación con la parte académica. El Firewall va hacer un filtrado de contenidos, además protegerá al servidor Sun dando de esta manera una navegación más segura cuando se este en Internet.

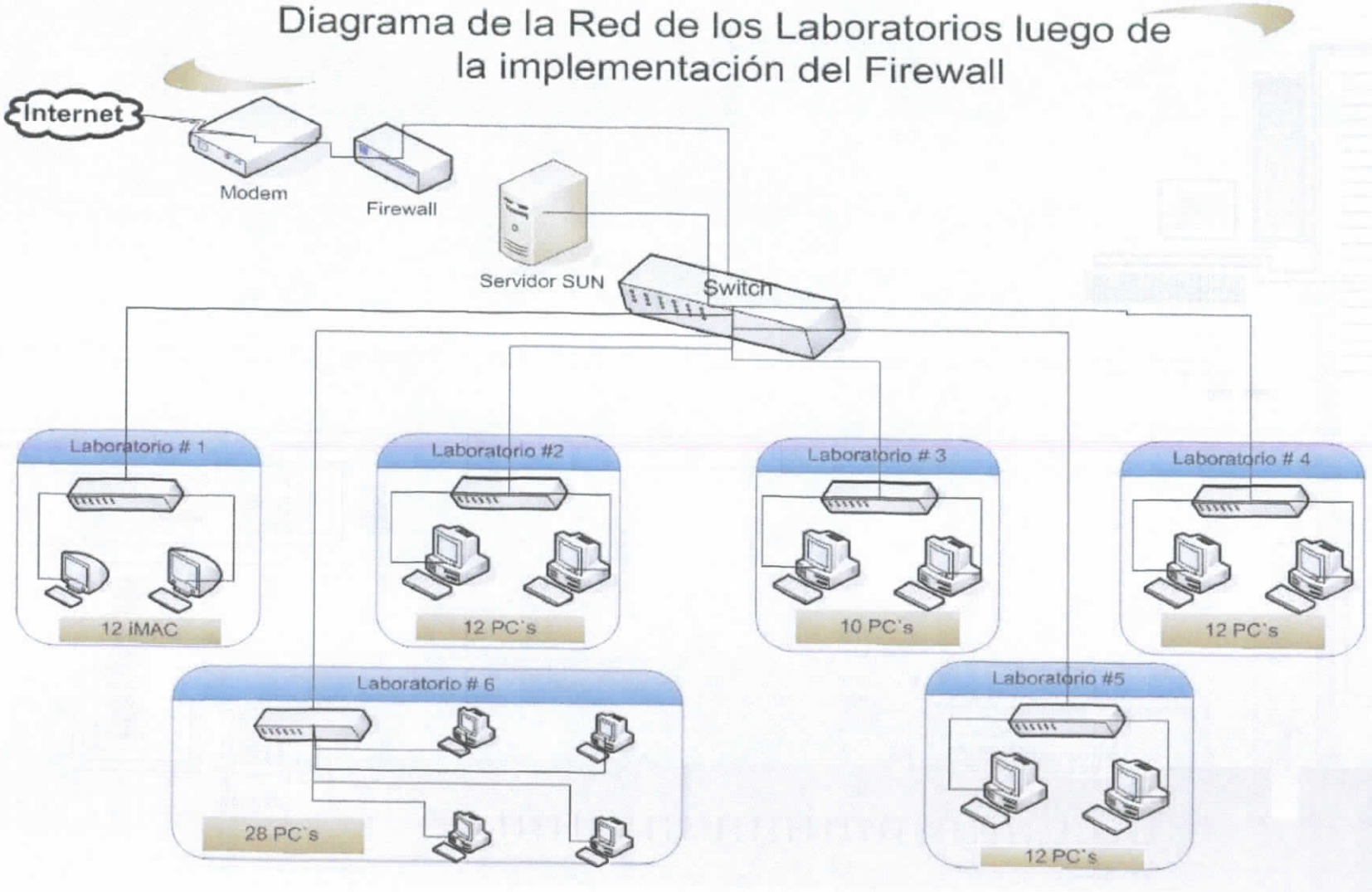
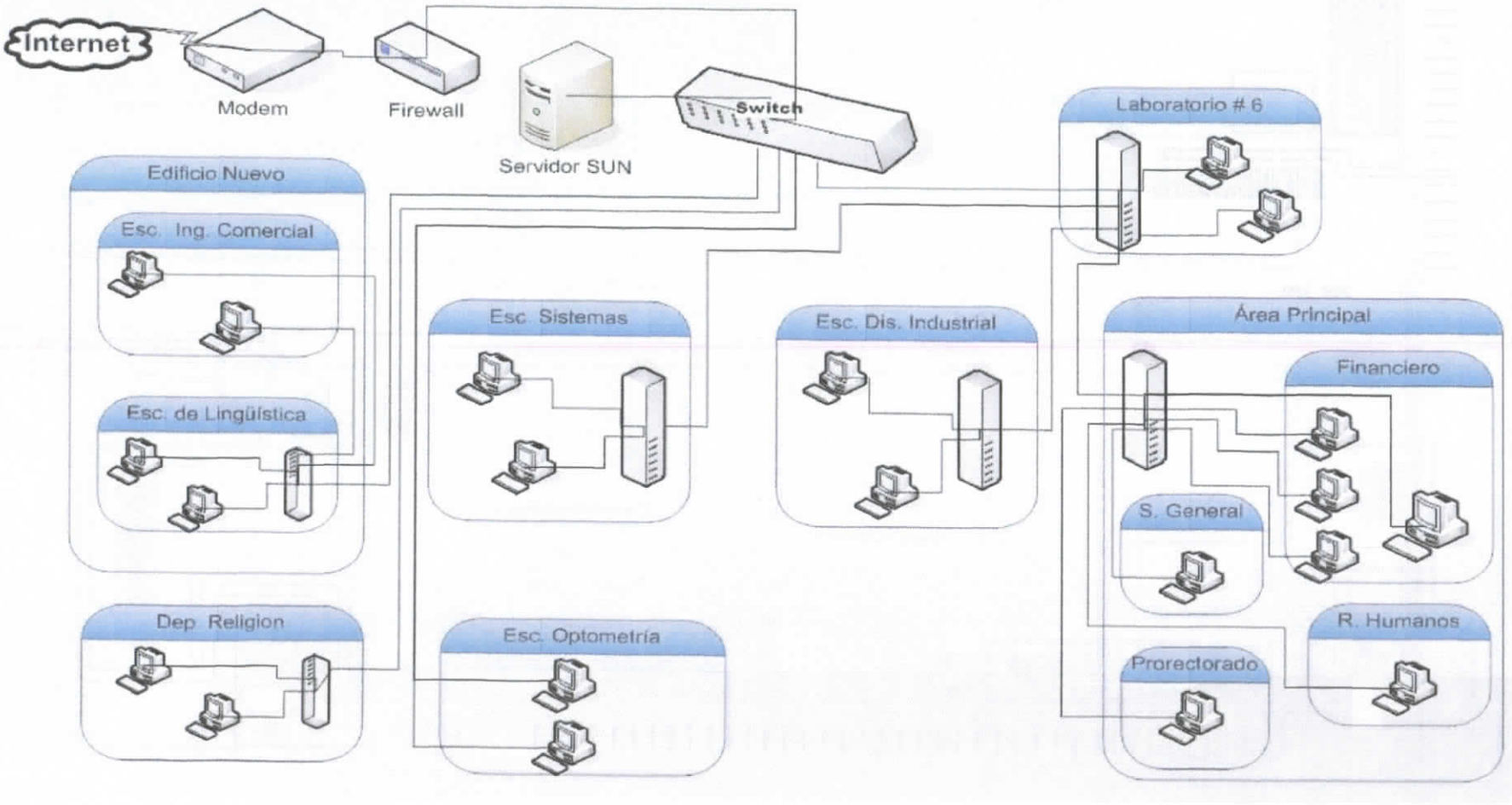

Diagrama de la Red de los Laboratorios luego de la implementación del Firewall
Internet
Modem
Firewall
Servidor SUN
Switch
Laboratorio # 1
12 iMAC
Laboratorio #2
12 PC`s
Laboratorio # 3
10 PC`s
Laboratorio # 4
12 PC`s
Laboratorio # 6
28 PC`s
Laboratorio #5
12 PC`s

Diagrama de la Red de la parte Administrativa luego de la implementación del Firewall



CAPITULO IV

VALIDACIÓN Y VERIFICACIÓN DE RESULTADOS

Ambato, Junio 22 de 2007

Yo, Ing. Diego Santacruz Abril, en mi calidad de Administrador del Centro de Cómputo de la Pontificia Universidad Católica del Ecuador Sede Ambato, tengo a bien

CERTIFICAR

Que el señor **ORTÍZ PAREDES WILLIAM FRANKLIN**, en el desarrollo de su tema de disertación de grado titulado "ESTUDIO E IMPLEMENTACION DE DISPOSITIVOS DE SEGURIDAD EN LA RED DEL CAMPUS UNIVERSITARIO DE LA PUCESA", ha configurado efectivamente el equipo de seguridad (firewall). Todos sus componentes han sido validados en su adecuado funcionamiento.

El interesado puede hacer uso de la presente como a bien tuviere.

Ing. Diego Santacruz Abril
Administrador Centro de Cómputo
Pucesa

PONTIFICIA
UNIVERSIDAD
CATOLICA
DEL ECUADOR
SEDE AMBATO
CENTRO DE COMP
BIBLIOTECA VIRT
Av. Manuelita Sáenz s/n
Sector El Tropezón
Apartado Postal No.18-01-662
Telef: 593 3 2416 220
Telefax: 593 3 2411 868 ext. 1
webmaster@pucesa.edu.ec
Ambato - Ecuador
www.pucesa.edu.ec

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
Sede Ambato

ESCUELA DE INGENIERIA DE SISTEMAS

Ambato, 28 de junio de 2007

Ingeniero
Telmo Viteri
DIRECTOR DE LA ESCUELA DE SISTEMAS DE LA PUCESA
Presente.

De mi consideración:

La presente es portadora de un saludo cordial y a la vez informarle que se ha procedido a la validación del trabajo de disertación del señor: William Franklin Ortiz Paredes, titulado: "Estudio e Implementación de dispositivos de seguridad en la Red del campus Universitario de la PUCESA", encontrando que el mencionado trabajo está concluido, cumpliendo los objetivos trazados.

Se destaca en el trabajo la investigación realizada y las ventajas que prestará en su futura implementación dentro de la PUCESA.

Atentamente,

Ing. Santiago Acurio M.
COORDINADOR ACADÉMICO
ESCUELA DE INGENIERIA DE SISTEMAS

Ambato, Junio 22 de 2007

Yo, Ing. Diego Santacruz Abril, en mi calidad de Administrador del Centro de Cómputo de la Pontificia Universidad Católica del Ecuador Sede Ambato, tengo a bien

CERTIFICAR

Que el señor **VILLALBA MORALES WILLIAM RAÚL**, en el desarrollo de su tema de disertación de grado titulado "ESTUDIO E IMPLEMENTACION DE DISPOSITIVOS DE SEGURIDAD EN LA RED DEL CAMPUS UNIVERSITARIO DE LA PUCESA", ha configurado efectivamente el equipo de seguridad (firewall). Todos sus componentes han sido validados en su adecuado funcionamiento.

El interesado puede hacer uso de la presente como a bien tuviere.

Ing. Diego Santacruz Abril
Administrador Centro de Cómputo
Pucesa

PONTIFICIA
UNIVERSIDAD
CATOLICA
DEL ECUADOR
SEDE AMBATO
CENTRO DE COM
BIBLIOTECA VIR
Av. Manuelita Sáenz s/n
Sector El Tropezón
Apartado Postal No.18-01-662
Telef: 593 3 2416 220
Telefax: 593 3 2411 868 ext. 1
webmaster@pucesa.edu.ec
Ambato - Ecuador
www.pucesa.edu.ec

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
Sede Ambato

ESCUELA DE INGENIERIA DE SISTEMAS

Ambato, 28 de junio de 2007

Ingeniero
Telmo Viteri
DIRECTOR DE LA ESCUELA DE SISTEMAS DE LA PUCESA
Presente.

De mi consideración:

La presente es portadora de un saludo cordial y a la vez informarle que se ha procedido a la validación del trabajo de disertación del señor: William Raúl Villalba Morales, titulado: "Estudio e Implementación de dispositivos de seguridad en la Red del campus Universitario de la PUCESA", encontrando que el mencionado trabajo está concluido, cumpliendo los objetivos trazados.

Se destaca en el trabajo la investigación realizada y las ventajas que prestará en su futura implementación dentro de la PUCESA.

Atentamente,

Ing. Santiago Acurio M.
COORDINADOR ACADÉMICO
ESCUELA DE INGENIERIA DE SISTEMAS

CONCLUSIONES

- En el ambiente amenazador de Internet en la actualidad, es importante que las redes dispongan de programas sobre seguridad, con las características necesarias para lograr una protección amplia.

- EL firewall VPN de 3COM, es un dispositivo que nos permitió solucionar los problemas que afectan a la red, como por ejemplo proteger de virus, y proveer al servidor de una seguridad absoluta ante los hackers.

- El firewall dificulta a los intrusos el acceso desde Internet, detectan el origen del intruso en algunos casos, y también dificulta que usuarios no deseados usen recursos tanto ajenos como suyos para atacar a otros, usando un paquete de Inspección.

- Los dispositivos de seguridad son parte fundamental en la redes. Nos ayudan al control de actividades dentro de la red como por ejemplo, el Firewall VPN de 3COM tiene la característica fundamental, controlar el ancho de banda para la transferencia de información en Internet.

- La red de la PUCESA, aumentó su nivel de seguridad con la implementación del firewall, lo que la convierte en un espacio libre de peligros seguro para el intercambio de datos a través de su infraestructura.

RECOMENDACIONES

- Adquirir la información necesaria de direcciones IP públicas que es proporcionado por el proveedor de Internet, para facilitar la instalación del Firewall

- Conocer las cuatro formas de las direcciones IP, para poder decidir cual es aplicable de acuerdo a los requerimientos de la implementación

- Configurar la zona de desmilitarización (DMZ), para tener la facilidad de comunicar a la computadora en formas de comunicación, como por ejemplo de una a muchas NAT, y de una a una NAT.

- Hacer uso óptimo del firewall, configurando las características que el Firewall proporciona para, tener un mejor rendimiento en la red.

- Adquirir un bucle de direcciones IP públicas para la instalación y configuración del Firewall, además de otros dispositivos que para su uso requieren direcciones IP publicas

BIBLIOGRAFÍA

http://www.terra.es/personal/tamarit1/redes/introduccion.htm

http://www.terra.es/personal/tamarit1/redes/index.html

http://www.terra.es/tecnologia/articulo/html/tec10569.htm

http://www.terra.es/tecnologia/articulo/html/tec16061.htm

http://www4.uji.es/~al019803/tcpip/paginas/capas.htm

http://www4.uji.es/~al019803/tcpip/index.htm

http://www.saulo.net/pub/tcpip/

http://www.saulo.net/pub/tcpip/b.htm#dr

http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

http://www.monografias.com/trabajos6/napro/napro.shtml

http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml

http://www.monografias.com/trabajos6/napro/napro.shtml

http://www.monografias.com/trabajos15/topologias-neural/topologias-neural.shtml#MECAN

http://ditec.um.es/laso/docs/tut-tcpip/3376c12.html#H16

http://www.adrformacion.com/cursos/wserver/leccion2/tutorial3.html

http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node243.html

http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-087-2-firewall.howto.html

http://www.infospyware.com/Firewall/Comparar%20cortafuegos.htm

http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo15.htm

http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo16.htm

http://www.csi.map.es/csi/silice/defglosario.html

http://www.zator.com/Hardware/H2_5_1.htm#El%20estándar%20RS-232

http://www.desarrolloweb.com/articulos/2176.php#manuales

http://www.nautopia.net/archives/es/varios_redes/nmap/escaneando_con_nmap.p

http://www.hackindex.com/articulo.php?cod=59

http://members.fortunecity.es/lanss/texto.htm

http://www.adslzone.net/puertos_lista.html

http://es.wikipedia.org/wiki/IPX/SPX

http://es.wikipedia.org/wiki/TCP/IP

http://usuarios.lycos.es/janjo/janjo1.html

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

http://www.telepolis.com/cgi-bin/web/DISTRITODOCVIEW?url=/1578/doc/Noti

http://www.viruslist.com/sp/viruses

http://www.segu-info.com.ar/amenazashumanas/amenazashumanas.htm

http://esp.sophos.com/pressoffice/news/articles/2006/02/phishstats.html

http://www.virusprot.com/Art40.htm

http://www.microsoft.com/technet/prodtechnol/exchange/ES/Guides/E2k3TransnRo
uting/b7c25326-3fd2-4049-bf3d-dc0e4976a373.mspx?mfr=true

http://www.yoreparo.com/articulos/seguridad/introduccion-al-uso-de-un-
firewall_2.html

LIBROS	AUTOR
Comunicaciones y redes de procesamiento de datos	Nestor Gonzalez Saionz
Redes Locales de Computadoras	Beltrao Moura Jose
Redes de Computadoras	Beltrao Moura Jose
Redes Globales de Información con Internet TCP/IP	Douglas E. Comer
Firewalls manual de referencia	Keith Strassberg, Richard Gondek y Gary
Manual de firewalls	Marcus goncalves
ADSL guia del usuario	José Antonio Carballar
Falcón	

GLOSARIO

Activo: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Administrador: Persona que se encarga de todas las tareas de mantenimiento de un sistema informático.

Amenaza: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema

Backdoor: Puerta de entrada trasera a una computadora, programa o sistema en general. Sirve para acceder sin usar un procedimiento normal

Crack: Desprotección de un juego o programa.

Cracking: Modificar un programa para obtener beneficios. Normalmente se basa en quitar pantallas introductorias, protecciones o, como en unas modificaciones de cierto programa de comunicaciones, conseguir nuevos passwords de acceso a sistemas...

Desastre o Contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Gusano: Programa que se reproduce, sin infectar a otros en el intento.

Hacking: Acto de hackear. Básicamente consiste en entrar de forma ilegal en un sistema, para obtener información. No conlleva la destrucción de datos ni la instalación de virus, pero pueden instalarse troyanos que proporcionen passwords nuevos. También consiste en llevar una vida acorde con el hackmode.

Impacto: consecuencia de la materialización de una amenaza

Ingeniería social: Arte de convencer a la gente de entregar información que no corresponde.

Log. Un log es un archivo normalmente de texto, donde quedan registradas con menor o mayor detalle, todas las acciones que se producen en un sistema. Actúan como diario del sistema y sirven para que el administrador lleve un control de todo lo que sucede y cuando sucede

Login: Procedimiento de identificarse frente a un sistema para luego usarlo. Este identificativo más el password o clave te permite acceder a información restringida.

Operador: Persona que usa una computadora. A menudo se llama 'operador' al administrador del sistema.

Packet switching: Conmutación de paquetes.

Password: Clave. Palabra que sirve para verificar que un usuario es realmente quien dice ser. Por eso mismo, el único que debe conocerla es ese mismo usuario.

Payload: Efecto visible de un software maligno.

Riesgo: posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.

Virii: Suele encontrarse en textos en inglés. Es la acción de crear virus.

Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

ANEXOS

Manual de usuario

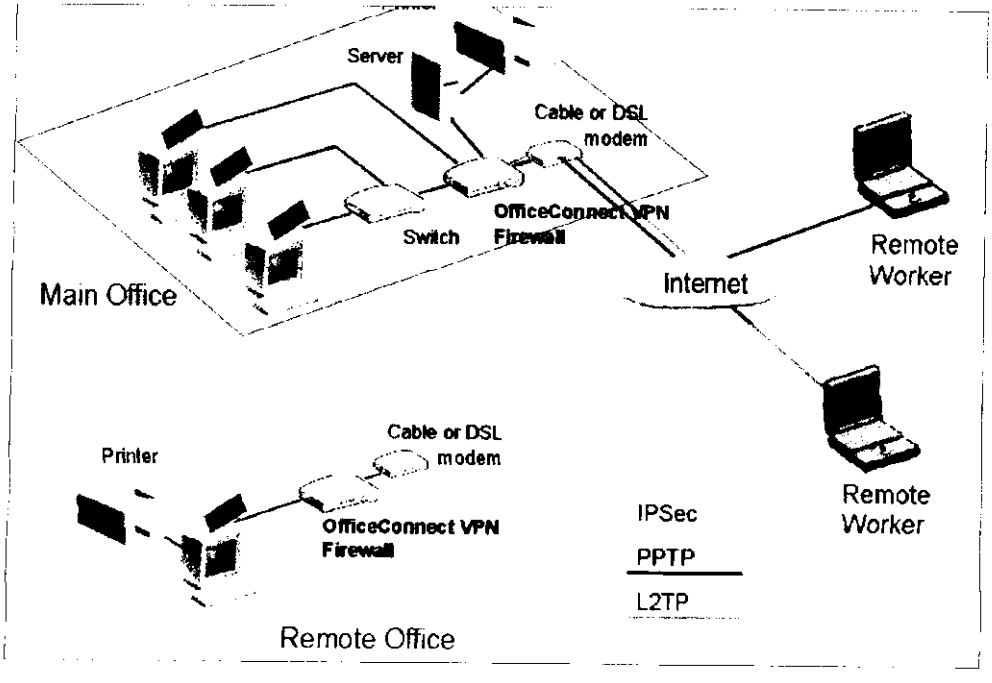
Office Connect VPN Firewall

Introducción

El Firewall Office Connect VPN es un dispositivo de seguridad para redes. Este dispositivo trabaja con banda ancha y VPN (Red Privada Virtual). La caracteristica principal del firewall es, prevenir el acceso de personas ajenas a la red creando (VPN's) encriptando vínculos hacia otras redes. El Firewall tambien provee protección y detección de intrusos, usando un paquete de inspección, que es el filtrado de contenidos.

Cuando el Firewall es colocado en la red, este empieza la conexión con el Internet. La conexión se puede hacer directamente como dispositivo, o a través de un Hub o Switch, dependiendo del número de computadoras que se encuentre en la red.

Diagrama de la conexión del firewall en la Red



On.- indica el link entre el puerto y la siguiente parte de la red.

Flashing.- significa que el link esta bien, y la transferencia de información es realizada.

OFF.- indica una de las siguientes condiciones:

i. No esta conectado.
ii. No esta conectado el dispositivo con el Switch.
iii. Hay un problema de conexión.

4.- Estado del Cable/DSL

Verde (100 Mbps Link) / Amarillo (100 Mbps link)

Indica una de las siguientes condiciones:

On.- el link entre el Firewall y el cable DSL se encuentra correctamente.

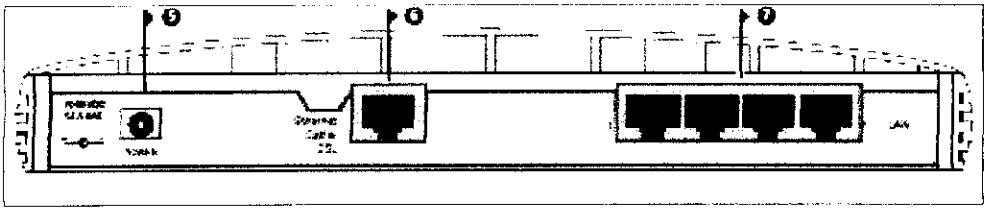
Flashing.- el link esta bien y la información que se transmite es recibida.

Off.- Indica las siguientes condiciones:

i. No esta conectado.
ii. El MODEM o el Switch se encuentran apagados.
iii. Hay un Problema con la conexión.

Panel Posterior

EL panel posterior de el firewall contiene cuatro puertos LAN, un Ethernet, un puerto de para cable DSL, y un socket para adaptador de poder.



5.- Enchufe de poder

Solamente se debe usar el adaptador que viene en el paquete del Firewall. No se debe usar ninguno otro adaptador

6.- Puerto para el Cable Ethernet DSL

Se usa la pequeña extensión de cable, para conectar el firewall a 10/100 Mbps. El puerto ajusta automáticamente la velocidad correcta.

7.- Cuatro 10/100 puertos LAN

Es conveniente usar el cable con conectores RJ-45. Se puede conectar el Firewall, a una computadora, o a otros dispositivos que tengan una conexión de Ethernet. Por ejemplo un Hub o Switch. Todos los puertos se ajustan automáticamente a las velocidades correctas

Instalación del Firewall

Posición del Firewall

La conexión se debe realizar con las siguientes condiciones:

i. Es conveniente localizar el cable DSL o MODEM, que puede ser usado para conectar al Internet
ii. Permitir una conexión a las computadoras, que pueden ser conectadas a los cuatro puertos LAN.
iii. Permitir una fácil visualización del los indicadores del panel frontal del firewall.

Antes de instalar el firewall

Antes de configurar el Firewall es necesario conocer la siguiente información: la IP Publica que es asignada por el ISP. Hay cuatro diferentes formas de información que asigna el proveedor de Internet como se describe a continuación:

a) Dirección IP dinámica (DLS o Cable)

La dirección IP dinámica (o DHCP), el Firewall asigna automáticamente la información de la IP. Este método es utilizado si existe un Servidor DHCP.

b) PPPoE (DSL solamente)

Cuando se instala en el firewall, un cliente PPPoE esta opción requiere conocer la siguiente información: nombre, clave, y el nombre del servicio (es asignado por ISP)

c) Dirección IP estática (DSL o Cable)

El proveedor de servicio de Internet asigna la información de la dirección IP. Para la configuración del Firewall es necesario conocer lo siguiente: la dirección IP pública, la máscara ISP, dirección Gateway, y la dirección del DNS.

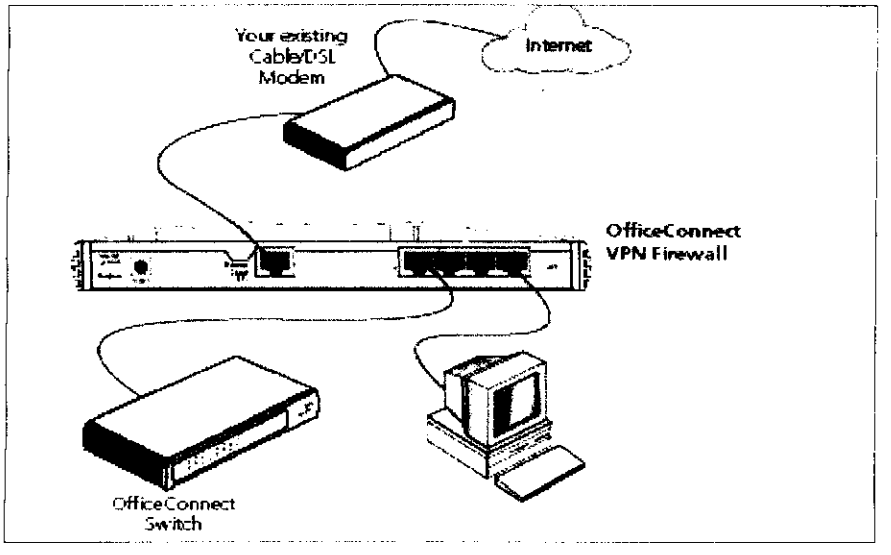
d) PPP (DSL o Cable)

PPTP es usado por muchos proveedores, la mayoría en Europa. En las instrucciones de instalación que son acompañados por la información del MODEM preguntan si se desea instalar con conexión usando PPTP VPN.

Nota cuando se instala el Firewall es probable que no se use VPN, en la computadora. Para configurar el Firewall es necesario conocer lo siguiente: la dirección IP asignada por el MODEM, para cuando empiece a ejecutar el Wizard.

Conexión del VPN Firewall

El primer paso para la instalación fisica del Firewall es conectar el cable DSL MODEM, para tener acceso a Internet.



a) Usar el cable suministrador, que conecta el Firewall, (Ethernet Cable DSL MODEM) y que el MODEM esté conectado al Internet.

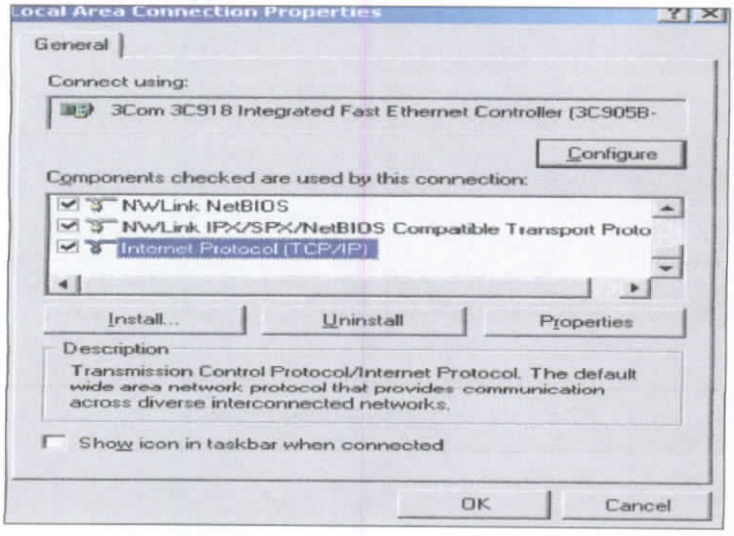
b) Conectar la computadora a cualquiera de los cuatro puertos LAN del Firewall

c) Conectar el adaptador del Firewall y esperar que el led de alerta deje de estar prendiéndose. Verificar que el led del Cable/DSL este iluminado.

d) Una vez que la computadora este en uso verificar los led`s de los cuatro puertos LAN que estén iluminados. Es necesario instalar en una computadora que pueda tener comunicación, con el firewall y también con Internet.

Instalación en la computadora

El VPN firewall tiene la aptitud de asignación de dirección dinámica de la computadora o de la red, usando DHCP. Sin embargo la computadora necesita ser configurada correctamente para que esté en red con el Firewall.



Ejecutar e Instalar el Wizard

Si el Firewall necesita ser configurado, por ejemplo si todavía no es configurado o es reseteado, se puede ejecutarse el Wizard automáticamente. Luego realizar los pasos de configuración para que el Firewall realice su función.

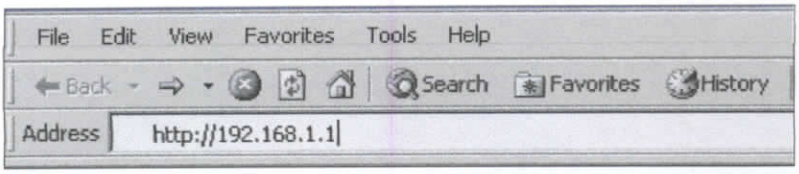
Acceso al Wizard

El Firewall VPN instala el Wizard basado en la Web, la cual significa que ingresa a través de la Web.

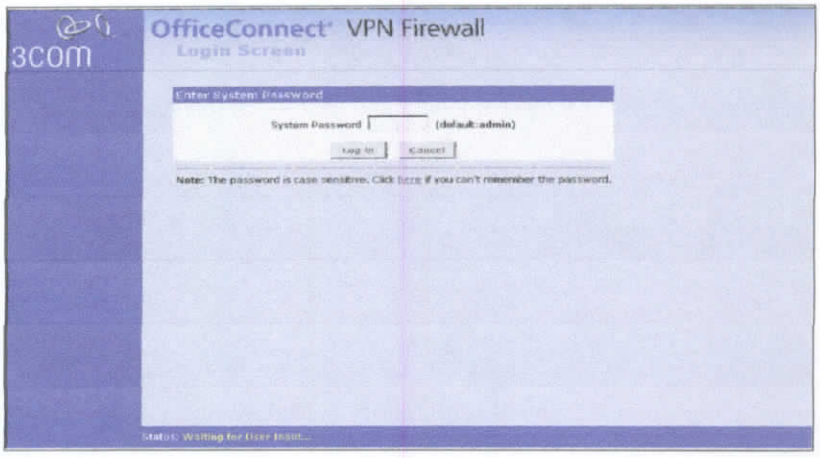
Pasos para acceder al Wizard

Entrar al URL del Firewall en la dirección que aparece en el recuadro.

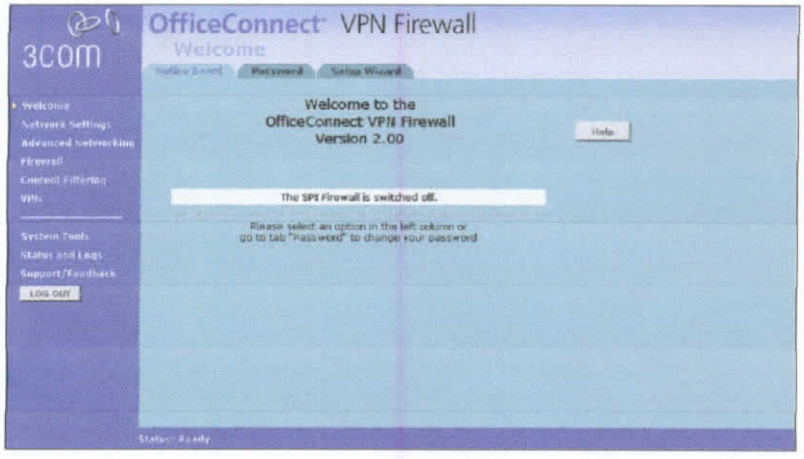
Por defecto el URL del Firewall es http://192.168.1.1, si es necesario cambiar la dirección IP en la unidad, es necesario sustituir la dirección que esta por defecto en el URL



La clave por defecto es ADMIN

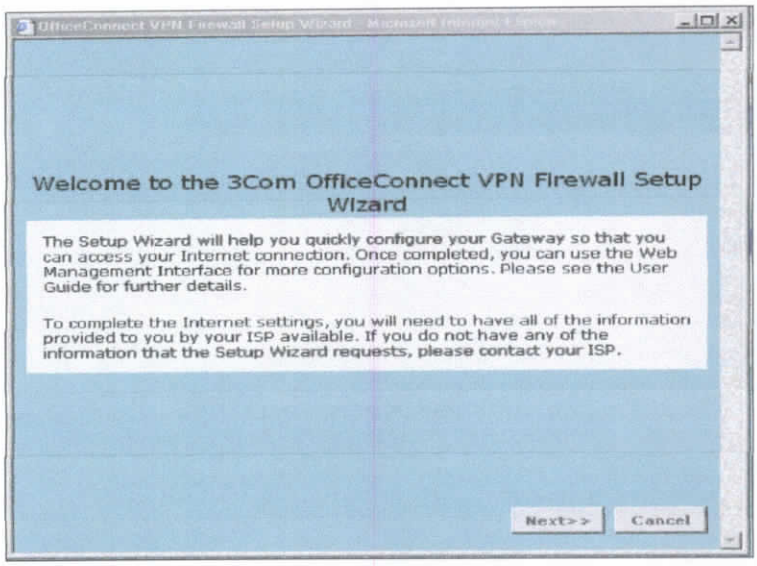


Si la clave es correcta, aparece la pantalla de bienvenida. Si el Firewall no ha sido configurado antes, el Wizard ejecuta automáticamente



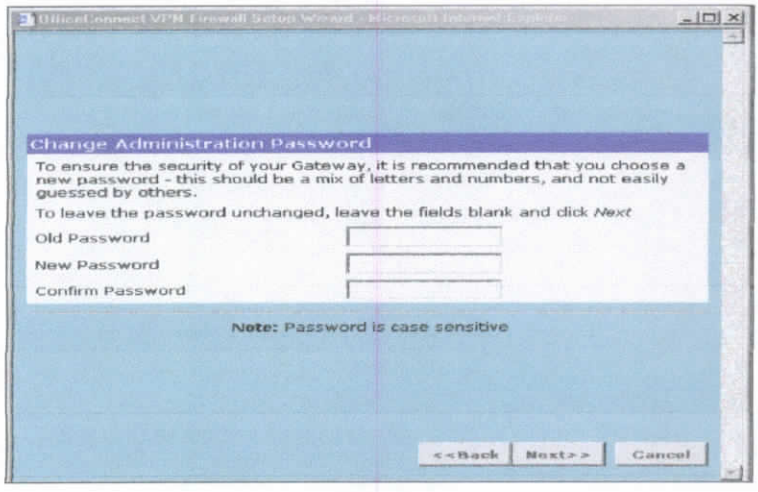
Si el Wizard no se ejecuta automáticamente es probable que el Firewall no este prendido o ha sido configurado anteriormente, es necesario instalar el Wizard manualmente.

Para ejecutar el Wizard manualmente debemos dar clic en la Setup Wizard en la pantalla de bienvenida.



Establecer la clave

Cuando se cambia la clave del administrador aparece en la pantalla, la anterior clave, luego la clave actual, y la confirmación de la clave actual. Por defecto la clave del Firewall es "admin." este es el caso de la clave anterior, o cuando el firewall es configurado por primera vez. 3COM recomienda cambiar de clave por preferencia numérico.



Establecer la Zona Horaria

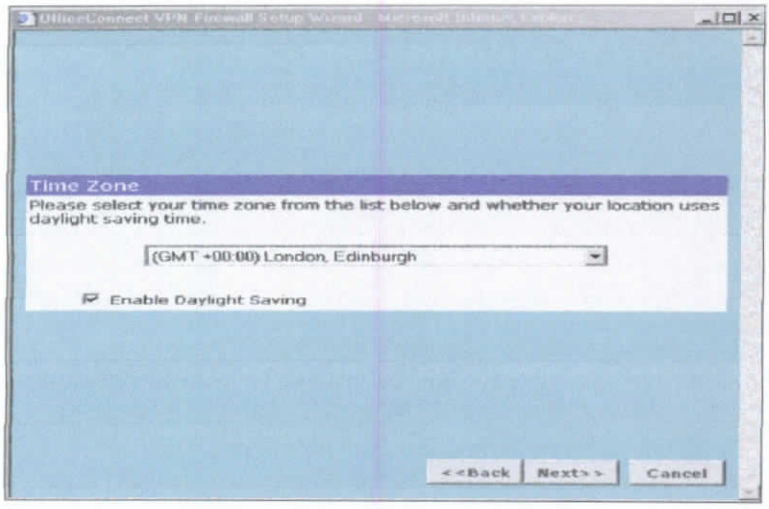
El Firewall establece la zona horaria cuando esta conectado al Internet. Esta zona es usada, cuando los registros requieren información.

Pasos para establecer la zona horaria en el Firewall:

i. Seleccionar nuestra zona horaria en el menú

ii. Verificar que este habilitado el cuadro de opciones para automáticamente ajustar el zona horaria.

iii. Clic en continuar



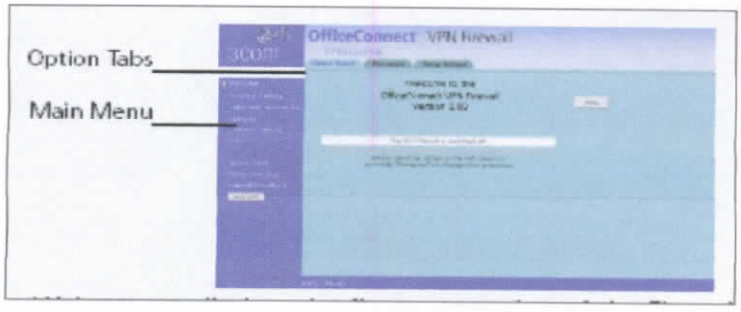
Configuración del Firewall

Navegar a través de la configuración del Firewall.

La configuración se toma por páginas, la localización es por medio de URL. Por defecto el URL es http://192.168.1.1, Si se cambia la dirección de la IP LAN durante la configuración, se usa la nueva IP. Cuando aparece el recuadro de la configuración del Firewall, el registro que se usa como clave en el sistema. Por defecto es "admin."

Menú Principal

En la parte izquierda de la pantalla se encuentra el menú principal, cuando se da clic en un tópico frente al menú principal, la página aparece en la parte central de la pantalla.



- **Welcome.** - aparece la versión del firewall, mensajes importantes, y permite cambiar la clave, y ejecutar el Wizard.

- **Network settings.-** permite instalar la dirección de Internet tales como la conexión PPPoE, IP dinámica, y la asignación de la dirección IP estática. Solamente permite configurar una dirección IP, la información de la mascara de subred, los parámetros del servidor DHCP, y el despliegue de la lista de los clientes DHCP
- **Advance Networking.-** permite la configuración de traslación de direcciones en la red. (NAT), rutina estática, rutina dinámica, dinámica DNS, y modelo de trafico.
- **Firewall.-** permite la configuración de las características del Firewall. Servidor Virtual, Aplicaciones Especiales, Privilegios del PC y otras opciones de seguridad general.
- **Content Filtering.-** permite el control de acceso a sitios Web en el Internet
- **VPN.-** permite al administrador instalar la conexión de red privada virtual (VPN)
- **System Tools. -** permite al administrador hacer cumplir las actividades del Firewall
- **Status and Logs.-** despliega el estado de actividades de los registros del Firewall
- **Support / Feedback.-** contiene un sistema de ayuda en linea con 3COM. contactos e información.

Espacio de opciones

En cada opción del menú, existe sub.-secciones las cuales se realizan a través del uso del espacio de opciones. El acceso a cada opción simplemente es dar un clic en el espacio que se requiere.

Getting Help (obtener ayuda)

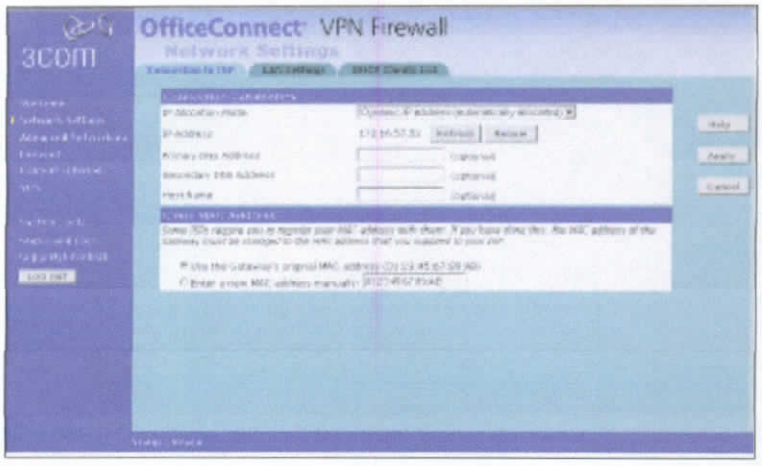
En cada ventana, hay un botón de ayuda que provee al acceso en línea del contexto del sistema. Dando Clic en el botón nos brinda una asistencia relacionado con la opción elegida.

Welcome Screen (Pantalla de bienvenida)

La sección de bienvenida permite ver la información y cambiar la clave. También se puede tener acceso a la configuración del Wizard.

El cuadro de información despliega importante información. Por ejemplo estar advertido, si las direcciones de LAN o Internet están en conflicto.

- Es necesario cambiar la clave de conexión de Internet (PPPoE)
- El informe ISP se puede cambiar con las características ISPs



a) Dirección IP Estática

El ISP provee la información de dirección IP, para la configuración del Firewall es necesario saber lo siguiente:

i. Dirección IP
ii. Sub.-Mascara
iii. Dirección DNS

b) Dirección dinámica IP (DSL o cable)

La dirección dinámica IP (o DHCP) automáticamente le asigna información al Firewall. Este método es popular con el proveedor de cable. Este método es solamente usado si el MODEM tiene construido un servidor DHCP

c) PPPoE (DSL solamente)

Las instrucciones de instalación que acompaña al MODEM es necesario para instalar el cliente PPPoE en el PC, luego de seleccionar esta opción. Para la configuración del Firewall es necesario saber lo siguiente:

i. Nombre del usuario
ii. Clave
iii. Nombre del servicio

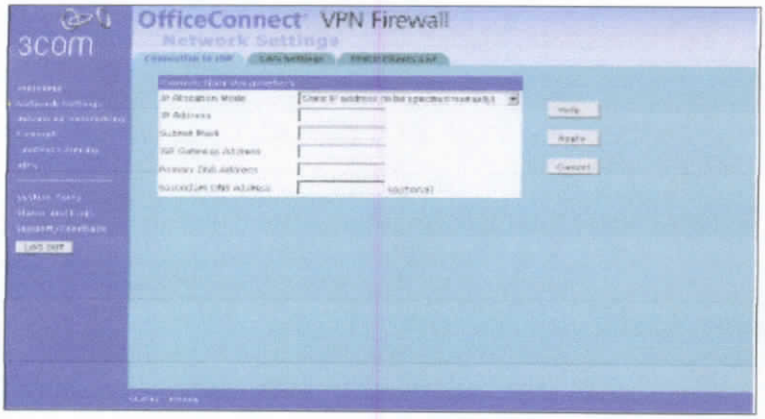
d) PPTP (DSL o Cable)

PPTP es usado por muchos proveedores, la mayoría en Europa. Si las instrucciones de instalación que acompañan en el MODEM preguntan, cómo instalar la conexión usando un túnel PPTP VPN, luego de seleccionar esta opción. Para la configuración del Firewall es necesario conocer lo siguiente:

i. Nombre del usuario
ii. La clave
iii. La dirección del servidor VPN

Configuración de la dirección IP estática

Si el proveedor de Internet tiene asignado una o mas direcciones IP estáticas, es necesario seleccionar la dirección IP estática como la IP asignada por el MODEM

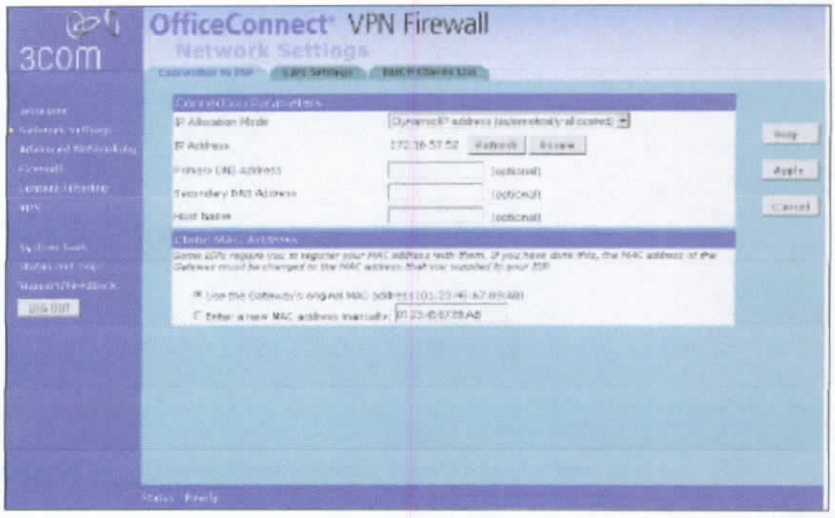


Las siguientes condiciones son requerimientos para instalar las direcciones IP. Colocar los valores que provee el ISP:

a) **LA dirección IP-** la dirección IP asignada por el ISP colocar, en el primer rango de dirección IP
b) **ISP dirección del Gateway** – la dirección del Gateway del proveedor de Internet
c) **La dirección primaria DNS** – la dirección del nombre del servidor de dominio ISP`s
d) **La dirección secundaria DNS** – el nombre del la dirección secundaria del Servidor de dominio ISP´s. El segundo Servidor es opcional, es asignado por el ISP en caso de fallar el primer servidor.

Configuración de dirección dinámica

Si el proveedor de Internet tiene asignado una dirección IP dinámica usando DHCP se puede seleccionar la opción Dynamic IP address como el ISP asignado en el MODEM



Para instalar el Firewall y usar la opción de dirección dinámica IP es necesario conocer lo siguiente:

a) **Dirección IP** –es la dirección de Internet asignada por el ISP, para esta conexión la configuración es automáticamente y no es editable.

b) **PPPoE Nombre de Usuario** – es el nombre de usuario es usado para acceder al *ISP*.

c) **Máscara del Sub red** -es la dirección de subred, es automáticamente configurado pero no es desplegado

d) **ISP dirección Gateway** – es la dirección del Gateway, el proveedor de Internet es automáticamente configurado pero no es desplegado

e) **Dirección primaria DNS** –el ISP requiere de direcciones de servidor primaria, luego de entrar a esta opción.

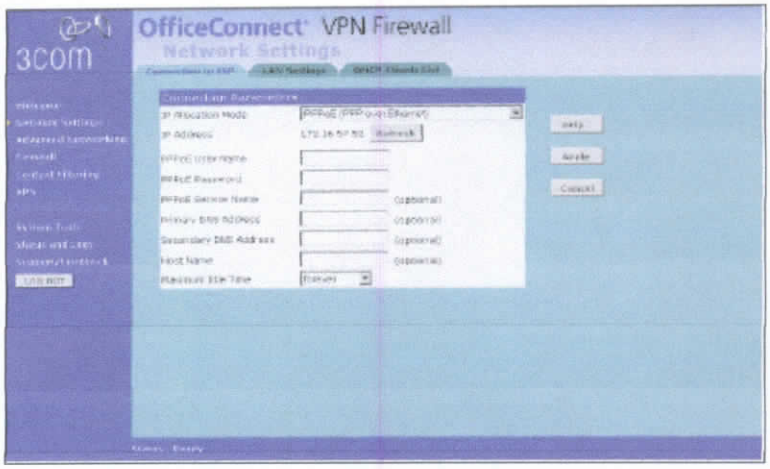
f) **Dirección secundaria de DNS** –el ISP requiere de la dirección del servidor *secundario de DNS luego de entrar a esta opción.*

g) **Nombre del Host** - el nombre del host en la computadora puede requerir por el ISP

h) **Dirección MAC** – El ISP puede requerir y tener una dirección MAC. Este puede ser la dirección MAC de la computadora con la cual se conecta con el ISP

Configuración de la conexión PPPoE

Si el ISP tiene asignado una dirección dinámica PPoE es necesario seleccionar PPPoE como la dirección IP del MODEM



El ISP puede necesitar para entrar, el nombre del host establecido. Para la instalación del Firewall con la conexión PPPoE es necesario las siguientes condiciones:

a) **Dirección IP** - la dirección de Internet asignada por el ISP, para esta conexión la configuración es automáticamente y no es editable

b) **PPPoE Nombre de Usuario** – el nombre de usuario es usado para acceder al ISP.

c) **PPPoE nombre de servicio** – el ISP probablemente requiera la especificación del nombre del servicio para la conexión

d) **Dirección primaria DNS** – el ISP requiere de direcciones de servidor primaria luego de entrar a esta opción.

e) **Dirección secundaria de DNS** – el ISP requiere de la dirección del servidor secundario de DNS luego de entrar a esta opción.

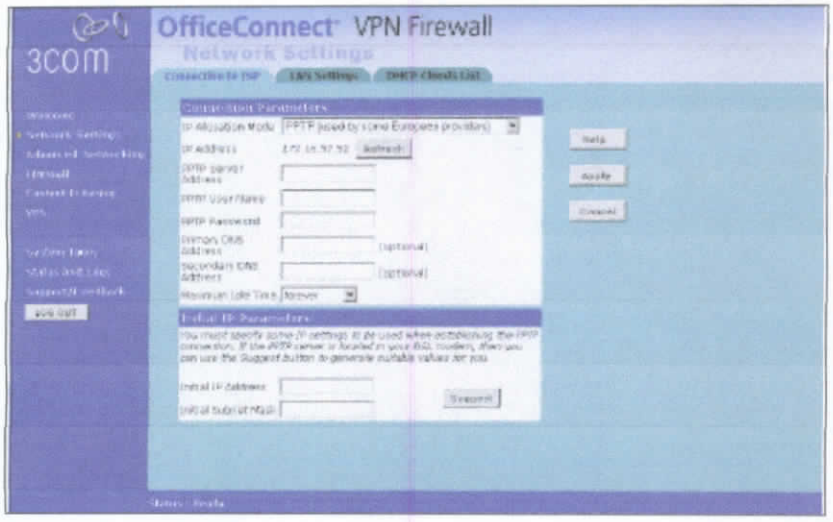
f) **Nombre del Host** - el nombre del host en la computadora puede requerir por el ISP

g) **Dirección MAC** – el ISP puede requerir y tener una dirección MAC. Este puede ser la dirección MAC de la computadora con la cual se conecta con el ISP

h) **Tiempo Máximo** – la cantidad de tiempo dentro de la actividad antes que el firewall termina la conexión con Internet.

Configuración conexión PPTP

Si el ISP tiene asignado una dirección dinámica usando PPTP es necesario seleccionar PPTP como la asignación de la IP en el MODEM



a) **Dirección IP** - la dirección de Internet asignada por el ISP, para esta conexión la configuración es automáticamente y no es editable

b) **PPTP dirección del servidor** – es típicamente la dirección del MODEM

c) **PPTP Nombre de Usuario** – es el nombre para acceder al ISP

d) **Clave PPTP** – la clave que se usa para acceder al ISP

e) ***Dirección primaria DNS*** – *si el ISP* requiere de direcciones de servidor primaria luego de entrar a este opción

f) **Dirección secundaria de DNS** – si el ISP requiere de la dirección del servidor secundario de DNS luego de entrar a esta opción.

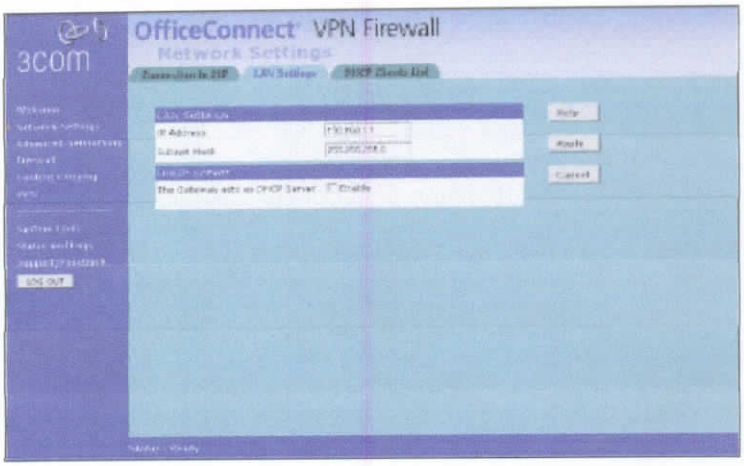
g) **Nombre del Host** - el nombre del host en la computadora puede requerir por el ISP

h) **Dirección MAC** – El ISP puede requerir y tener una dirección MAC. Este puede ser la dirección MAC de la computadora con la cual se conecta con el ISP

i) **Tiempo Máximo** – la cantidad de tiempo dentro de la actividad antes que el firewall termina la conexión con Internet.

Establecer LAN

La pantalla para establecer LAN permite cambiar el TCP/IP del firewall y el servidor DHCP



Cambiar LAN

Se puede cambiar en la instalación del Wizard cuando el dispositivo es usado por primera vez. Es necesario cambiar esto, si se reconfigura la red.

Cuando se cambia la dirección IP del firewall, se escoge una dirección que puede ser única en la red y en la redes de la sub.- red. La dirección IP del firewall por defecto es 192.168.1.1.

Si se usa la opción de dirección estática en la PC´s es necesario alternar la configuración del la red en cada PC, por lo tanto se debe tener una dirección IP igual a la sub-red, también se debe tener por defecto el Gateway como el firewall con la dirección IP LAN. Si se reconfigura la red es necesario cambiar la máscara de la sub-red. Ya que la máscara del sub-red determina que las direcciones IP sean validas dentro de la red. Por defecto la mascara de la sub-red es 255.255.255.0

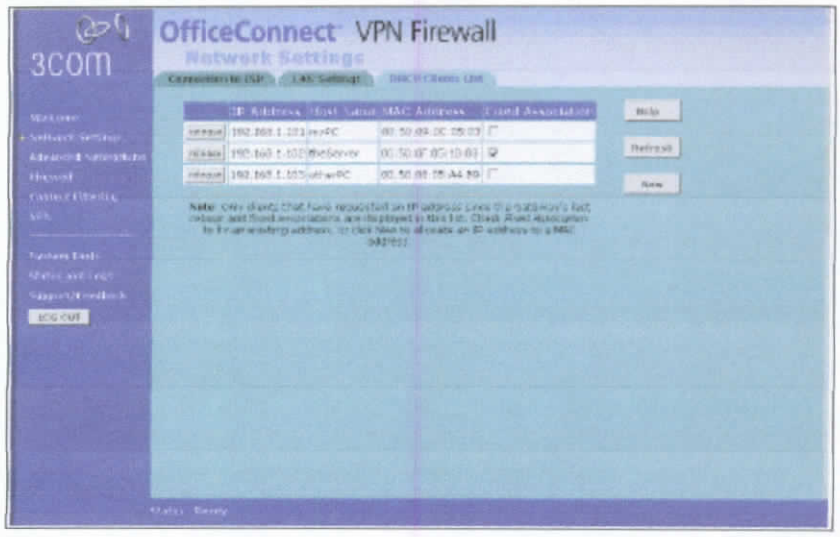
Por ejemplo si la dirección IP del Firewall es 192.168.1.1. Y la máscara de sub-red es 255.255.255.0. Luego la red puede tener un máximo de 254 direcciones desde 192.168.1.1 hasta 192.168.1.254 (192.168.1.0 y 192.168.1.255) son reservados por la subred y no son validos para usar. Cuando se cambia la dirección IP o la máscara de la Sub-red del Firewall es necesario revisar el Servidor DHCP como se describe a continuación.

Cambiar el Servidor DHCP

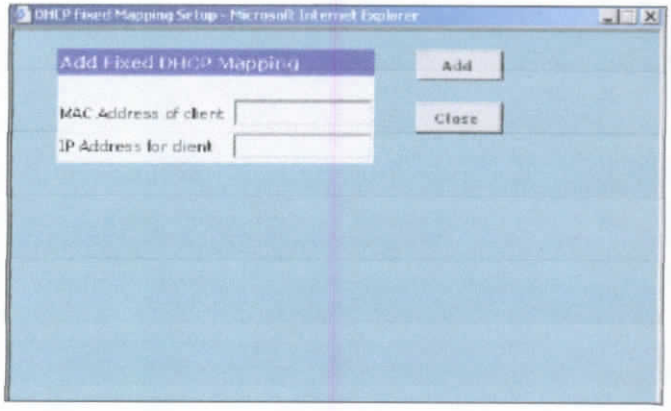
La sección permite habilitar y configurar en el Firewall el Servidor DHCP. Si el uso del Firewall controla los permisos de las máquinas en la red, es necesario usar la dirección del Servidor DHCP (o la dirección estática). Si se usa otro servidor DHCP puede tomar resultados inesperados.

Lista de Clientes DHCP

La pantalla de clientes DHCP provee detalles del dispositivo que tiene una dirección IP por el servidor DHCP. Por cada dispositivo existe una IP, nombre del host, y una dirección MAC para que cada dispositivo sea desplegado.



La dirección IP, nombre del Host, y a dirección MAC indica la dirección que está asignado. *Ellos identifican la maquina por el nombre y por el numero de MAC,* y las maquinas con tarjeta de red. Es necesario verificar el comportamiento:

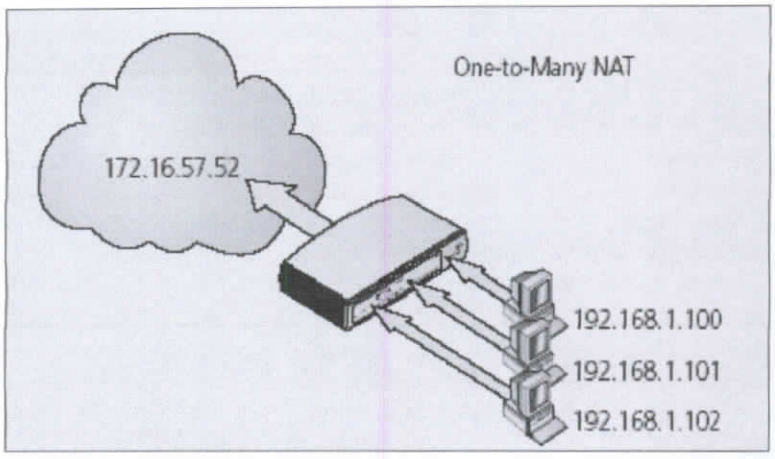


Estudio de la red

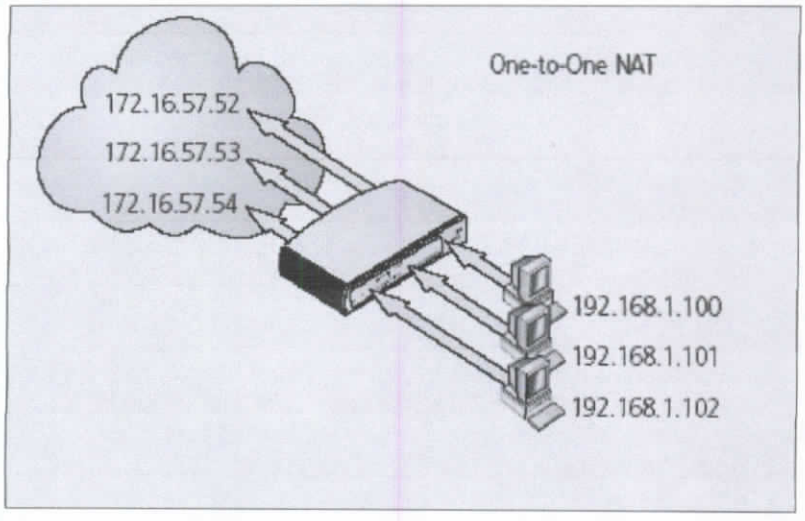
Establecer NAT

El Firewall esta habilitado para cumplir NAT (traslación de la dirección de red) en una o dos formas

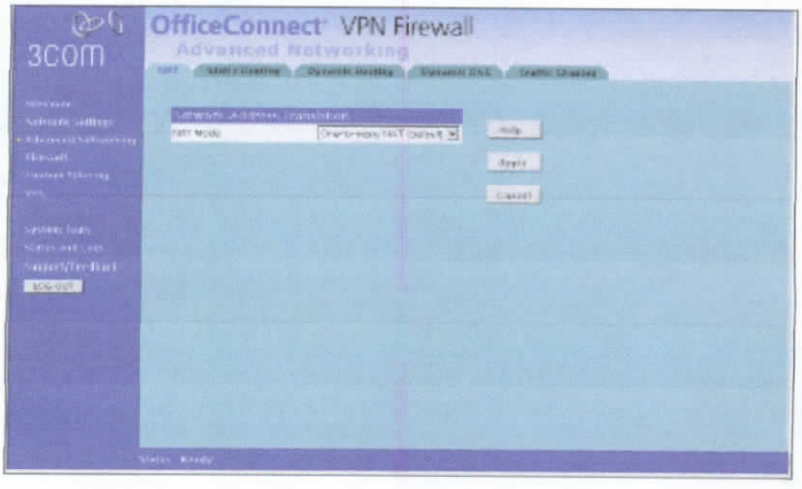
Una a muchas NAT – el firewall aparece solamente una dirección de Internet



Una a una NAT – cada dirección de Internet es vinculado con la dirección LAN, el firewall probablemente responde a todas las direcciones de Internet.



Instalar una-a-muchas NAT



Es fácil de instalar en el Firewall. Se trabaja con muchas direcciones IP asignadas por le MODEM y el mapa de todas las direcciones LAN del Internet

Instalar una a muchas NAT

i. Seleccionar una a muchas NAT en el cuadro de texto

ii. Clic en aplicar

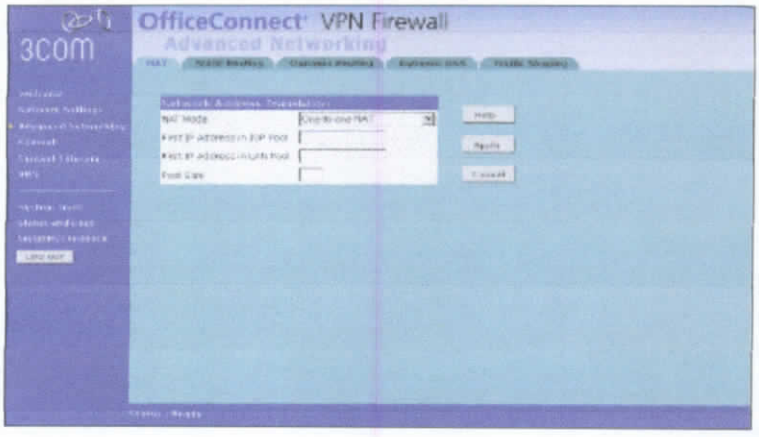
Instalación de una-a-una NAT

Los siguientes criterios son necesarios para usar una a una NAT:

a) Es necesario tener una dirección IP estática para cada computadora en la red además de una dirección para el firewall

b) La dirección puede ser un bloque continuo igual en la Sub-Red

c) Se debe tener una dirección IP estática y una dirección IP asignada por el *MODEM* y dar al Firewall la primera dirección asignada por el ISP



Instalar una-a-una NAT

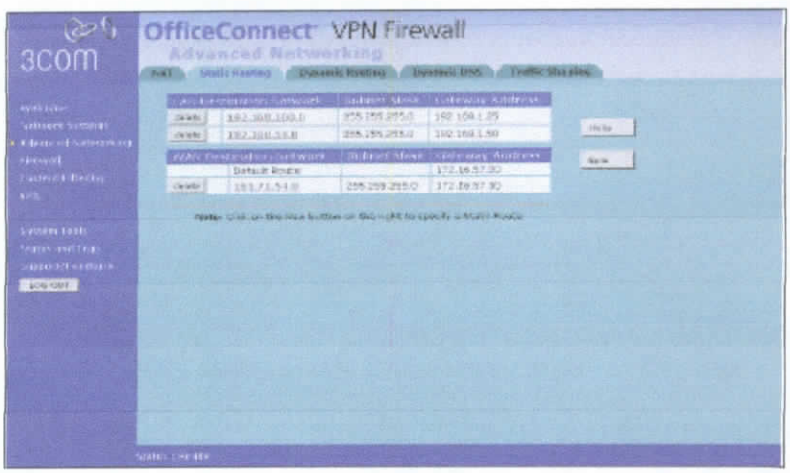
1. Seleccionar una-a-una NAT de la opción NAT
2. Poner la segunda dirección de Internet y el rango de direcciones en la primera dirección IP, en el espacio de LAN
3. Colocar la primera dirección en el rango de direcciones la cual se usa el mapa de direcciones en la primera dirección IP en el espacio de LAN
4. Colocar el número del rango de direcciones dentro del espacio
5. Clic en aplicar

Establecer la rutina estática

El Firewall soporta hasta 10 rutinas estáticas en total, entre las interfaces LAN y WAN. El tamaño de las rutinas estáticas de WAN son solo asignadas por la configuración del MODEM que realiza el ISP

Pasos para la instalación:

1. Seleccionar nuevo, en la derecha de la pantalla y abrir la configuración de Static Routing
2. Colocar la dirección IP de destino de la red (ejemplo 192.168.20.0)
3. Colocar la dirección IP de la mascara de de sub-red (ejemplo: 255.255.255.0)
4. Colocar la dirección IP de la dirección del Gateway (ejemplo: 192.168.1.25)
5. Seleccionar la localización de destino de la Red en relación con el firewall (si es LAN o WAN) y localizar en el espacio
6. Clic en aplicar



Rutina dinámica

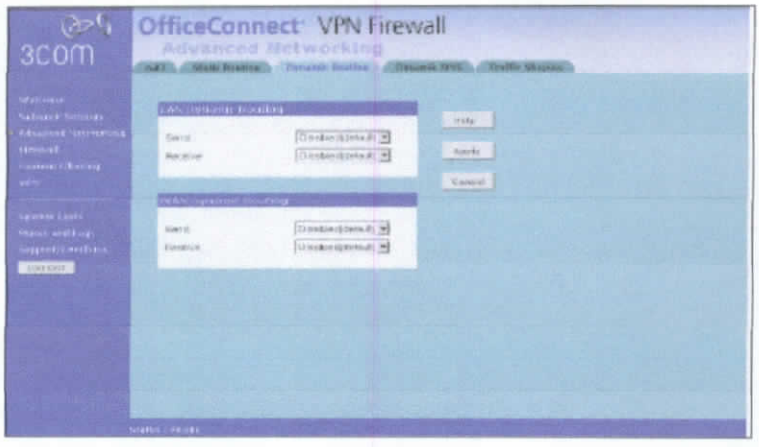
El Firewall soporta RIPv1, RIPv2 o las dos formas, para cada interfase, para enviar y recibir información, la rutina LAN son enviados a la mascara de sub-red LAN, y la rutina WAN son enviados a la mascara de sub-red WAN.

En la pantalla de rutina dinámica se puede habilitar el Firewall automáticamente y ajustar fisicamente los cambios en la red. Usando el protocolo RIP, el firewall determina el paquete de ruta basado en los pocos números de saltos entre las fuentes EL protocolo RIP regula la rutina de información de broadcasts y otros dispositivos de la red.

Establecer la Rutina Dinámica

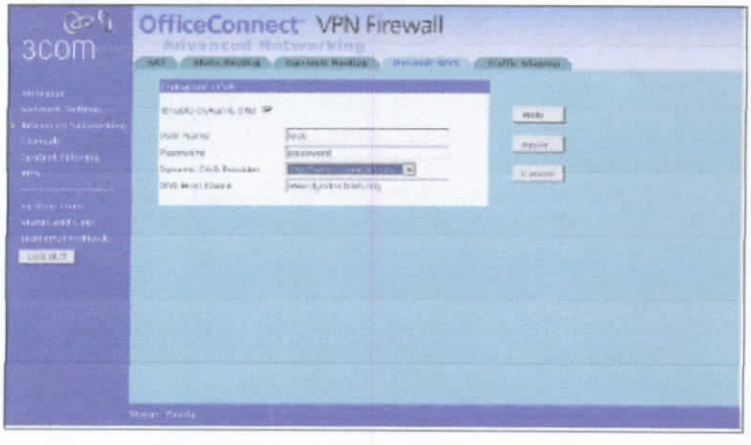
Pasos para instalar la rutina dinámica:

1. Seleccionar el servicio de la lista pull-down
2. Clic en Aplicar



DNS dinámico

El Firewall provee una lista DNS dinámicas para escoger. El DNS dinámico esta deshabilitado por defecto

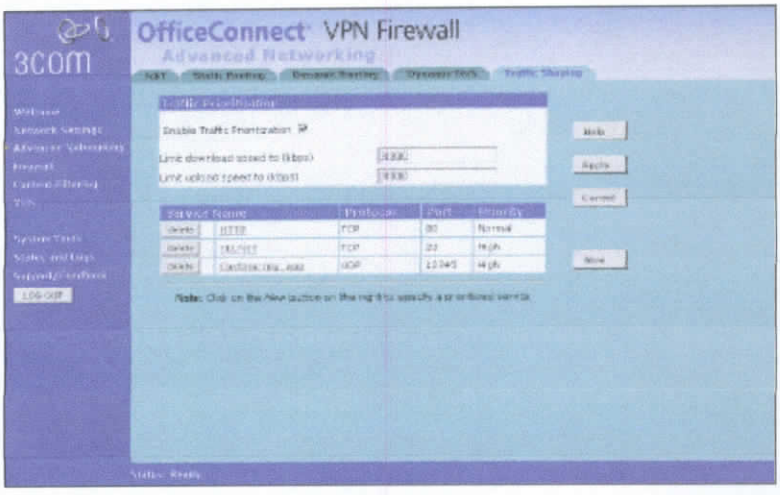


Establecer el DNS dinámico

Pasos para establecer el DNS dinámico:

1. *Verificar y habilitar el DNS dinámico en el cuadro y abrir DNS dinámico en la pantalla*
2. Colocar la clave y el usuario
3. Seleccionar DNS dinámico de la lista
4. Poner el nombre del Host DNS
5. Clic en aplicar y guardar los cambios

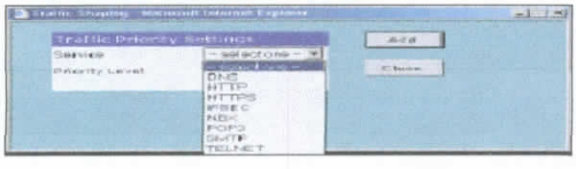
Configuración del Tráfico



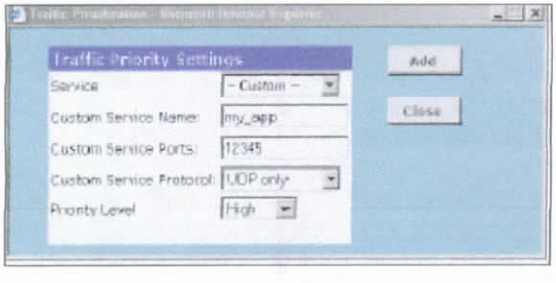
Establecer el tráfico

Pasos para establecer la configuración del tráfico:

1. Verificar la habilitación del tráfico en el cuadro de opciones de tráfico.
2. Verificar el límite de velocidad en (kbps) y el archivo, sea mas bajo que el ancho de banda. Esta información provee el ISP.
3. Seleccionar el nombre del Servicio o dar clic en nuevo y abrir la opción de tráfico en la pantalla
4. Seleccionar el servicio en la lista



5. Colocar el nombre del servicio que se requiere.
6. Seleccionar el número de puerto en el cuadro de servicio.
7. Seleccionar el nivel de prioridad en la lista.
8. Si se suma un nuevo servicio se debe dar clic en Add, o si se edita un servicio existente clic en aplicar y guardar los cambios.



Creación de una Virtual DMZ

El Firewall provee una virtual DMZ (zona de desmilitarización) en una computadora dentro de la red, Esta característica permite a la computadora configurar en dos formas de comunicación dentro de la red, en una a muchas NAT.

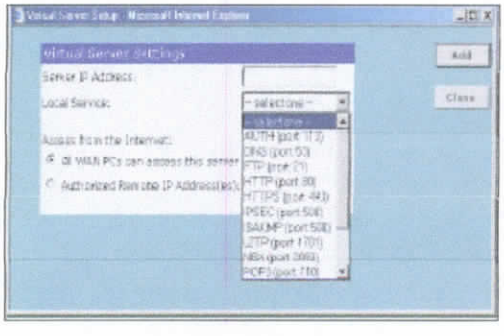
Para especificar a una computadora como host DMZ, se debe seleccionar el host de virtual DMZ y colocar la dirección IP de la computadora y la dirección del host de DMZ en el cuadro de texto, y luego dar clic en guardar.

Creación de un Servidor Virtual

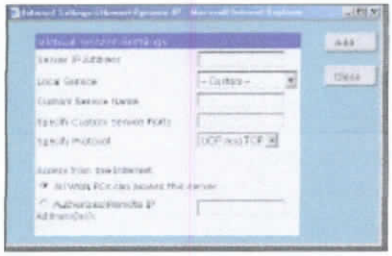
Activar y configurar un servidor Virtual permite a una o más computadoras de la red funcionar como host de servicio de Internet. Por Ejemplo una de las computadoras puede configurar como host FTP, permitiendo a otras como red de oficina, y bajar los archivos escogidos. Si se tiene creado un sitio WEB se puede configurar una o más computadoras como servidores WEB.

Pasos para configurar un servidor Virtual:

1. Clic en nuevo, que se encuentra a la derecha de la pantalla y abrir Servidor virtual
2. Colocar la dirección IP de la computadora en el cuadro del servidor de dirección IP
3. Seleccionar el servicio de la lista



Si se selecciona Custom, la pantalla que aparece, se debe especificar un nombre de servicio y luego se debe dar enter en el número de puerto requerido por el servicio. Si el servicio requiere más de un número colocar los números múltiplos, separado por coma en el rango por ejemplo 51, 52,54-59

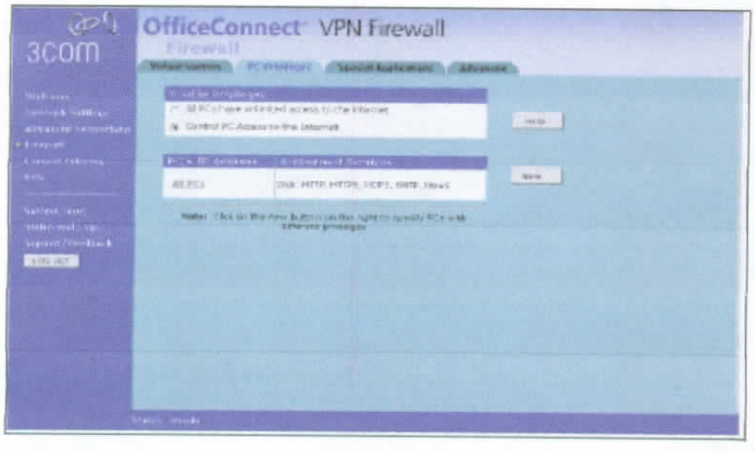


4. Seleccionar todas las computadoras de la red WAN que tengan acceso a este servidor, o este autorizado por la dirección IP. Si se selecciona Authorized IP address es necesario especificar una dirección IP en el rango de las direcciones. Por ejemplo 162.223.41.12 o162.223.41.15 que dan acceso a todas las direcciones IP
5. Clic en sumar y guardar.

Privilegios para PC,s

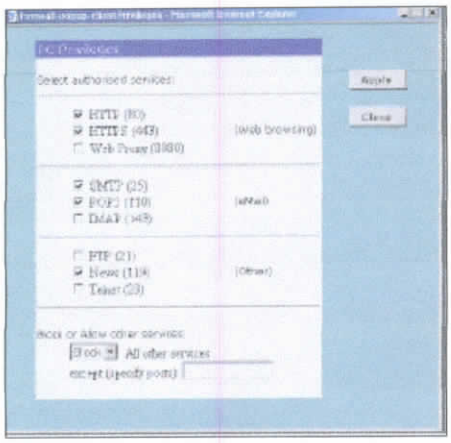
El acceso a la red de Internet puede ser controlado de PC a PC. Por defecto la configuración del Firewall puede permitir que todas estén conectadas ilimitadamente al Internet.

El privilegio de la PC permite asignar diferentes accesos para diferentes computadoras en la red como también restringir acceso y controlar a los usuarios, el acceso a las fuentes



Controlar el acceso para todas las computadoras

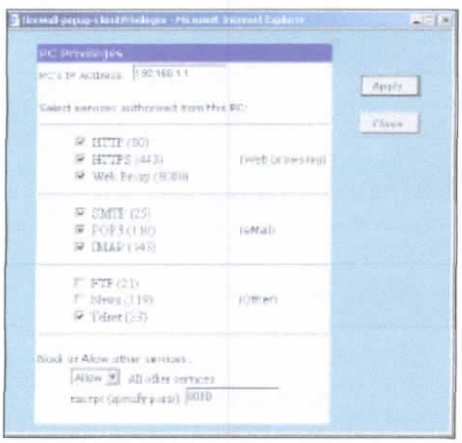
1. Clic en el control de acceso de PC al Internet.
2. Clic en todas las PC´s y instalar el acceso para todas las computadoras que estén conectadas.
3. Verificar en la opción de servicio autorizado.



4. Colocar el servicio adicional deseado.
5. Clic en aplicar.

Para asignar diferentes accesos para diferentes computadoras

1. Clic en el acceso de control de Pc´s para Internet.
2. Clic en nuevo y ejecutar los privilegios de Pc´s en la pantalla.
3. Colocar la dirección IP de la computadora en la opción de dirección IP.
4. Verificar el servicio autorizado.



5. Colocar el servicio adicional deseado.
6. Clic en aplicar.

Ejemplo

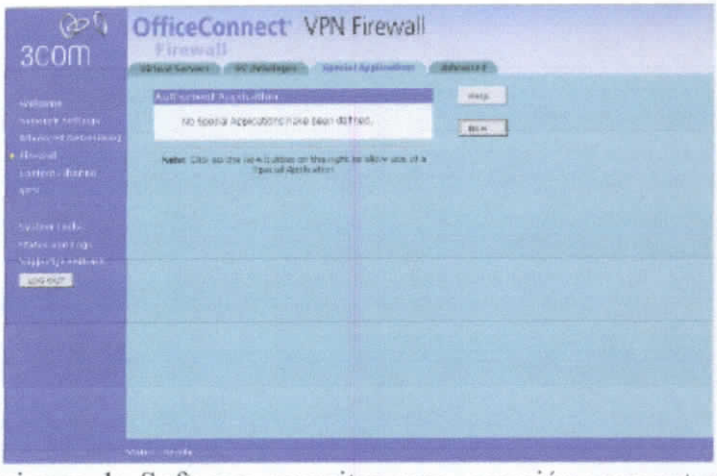
Permitir solamente Web y acceso al E-mail. Para permitir Web y acceso al E-mail en el bloque y otros servicios en el Firewall.

1. Asegurar que el acceso a Pc´s, el botón este seleccionado.

2. Clic en todas las Pc´s para dar privilegios, asegurar que el e-mail (110,25) y Web (80) sean verificados.
3. Establecer el bloque y permitir otros servicios.
4. Colocar el número 8000 en el lugar específico.
5. Clic en aplicar y guardar los cambios y cerrar la ventana de privilegios.

Aplicaciones Especiales

Seleccionar aplicaciones para desplegar en la pantalla la instalación de aplicaciones autorizadas.



Muchas aplicaciones de Software necesitan una conexión para estar conectadas al Internet y el acto es usualmente bloqueado por el Firewall. Por lo tanto estas aplicaciones especiales pueden trabajar y no ser bloqueadas.

En cada instancia hay disparadores que avisa al firewall, la aplicación que empieza y permite la conexión. Para cada aplicación especial la configuración del firewall es sumado en la tabla.

Cada fila contiene los siguientes ítems:

Delete button – *suprime la aplicación especial de la fila. Este puede prevenir al* Firewall salir de la conexión.

Nombre – Cada aplicación especial es nombrada. El nombre es usado por el Firewall y solamente es habilitado para identificar la conexión.

Trigger Port – Este es el puerto TCP/IP que el firewall usa y reconoce la aplicación que comienza.

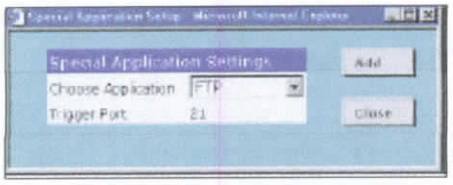
Adicionalmente hay dos botones dentro de la tabla:

Help – despliega la página de ayuda en línea

New – crea una nueva aplicación especial

Añadir y editar aplicaciones Especiales

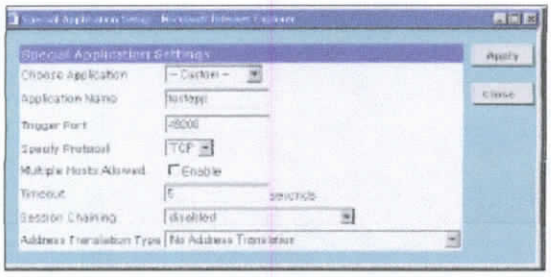
1. Clic en el botón nuevo para crear o editar una aplicación especial.
2. Seleccionar la aplicación en la cuadro de opciones. Si la aplicación que desea definir no esta en la lista "Crear aplicación Especial"



3. Clic en añadir aplicación especial en la lista de protocolos o cerrar la selección y regresar a la pantalla de aplicación especial.

Crear aplicación especial

Si la aplicación especial no esta en la lista, en la selección de aplicación se puede configurar manualmente. Seleccionar la lista de aplicaciones y en la pantalla de aplicaciones especiales existen campos extras para escribir la selección especial.



Nombre de la aplicación – cada aplicación especial es nombrada para que puedan detectar los puertos que necesitan abrir, por lo que no es necesario especificar. Este nombre no es usado por el Firewall y es solamente habilitado para identificar la conexión.

Trigger Port – este es el puerto TCP/IP que el firewall usa, y reconoce la aplicación que empieza. El Firewall permite valores singulares o en rango pero no en lista. Ejemplo '6599' y '6577-6587' son los dos validos '6577, 6579,6582' no son validos.

Special Protocol – selecciona el protocolo (TCP o UDP) que son usados para aplicaciones especiales.

Multiple Host allowed – si la aplicación provee usar mas de una IP durante la sesión, o responde a la dirección diferente se puede empezar la aplicación especial y se debe de estar seguro que el host este verificado. La aplicación provee la información.

Precaución: Seleccionar los anfitriones múltiples permitidos, debilita la seguridad que el cortafuego puede proporcionar y debe ser utilizada solamente si el uso especial lo requiere.

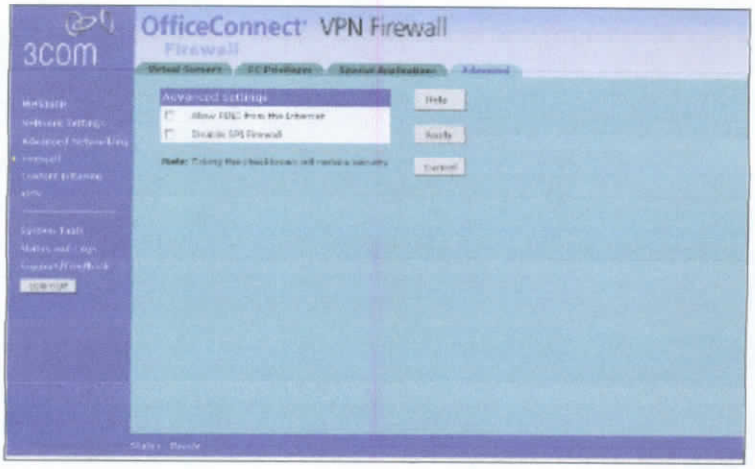
Descanso.- Es el número de segundos que el cortafuego debe esperar, antes de abandonar la conexión. El descanso por defecto es de tres segundos. Si se visualiza esto quiere decir que se están cayendo las conexiones y se debe incorpora un valor más alto.

Encadenamiento de la sesión.- Algunas aplicaciones especiales necesitan tomar control de una sesión. Si la aplicación especial que desea funcionar requiere esto, asegurarse de que el encadenamiento de la sesión esté permitido.

Precaución: Permitir el encadenamiento de la sesión debilita la seguridad del cortafuegos y debe ser utilizado solamente si el uso especial lo requiere.

Tipo de la conversión de dirección.- Si la aplicación especial del uso encaja las direcciones del IP en paquetes del TCP o del UDP que se tuvo permite la conversión de la dirección en el tipo apropiado del protocolo. Cuando se ha configurado la aplicación especial se debe hacer clic en agregar para guardar los cambios o cerrar sin realizar ningún cambio.

Avanzado.- Seleccionar avanzado para exhibir la pantalla avanzada de los ajustes.



Permitir hacer Ping desde Internet.- El ping es una opción, que se utiliza para determinarse si un dispositivo es activo en la dirección IP especificado. El ping se utiliza normalmente para probar la conexión entre dos dispositivos, asegurándose que todo esté trabajando correctamente.

Por defecto el cortafuego tiene el ping inhabilitado de modo que no responda a las peticiones de este. Esto hace que el dispositivo sea más difícil de encontrar en el Internet y el ataque menos propenso. Esta característica se lo permite haciendo clic en la caja de chequeo para poder considerar una señal y entonces seleccionar y aplicar. 3Com recomienda que la opción de ping en Internet obligue estar inhabilitada, para proporcionar mayor seguridad.

Inhabilitar el SPI del cortafuego.- La característica del cortafuego es detectar los ataques de los hackers en el Internet y una vez detectado bloqueará el acceso a la red.

Filtrado de Contenidos

El menú de filtrado de contenidos permita el control de acceso a los sitios Web en Internet.

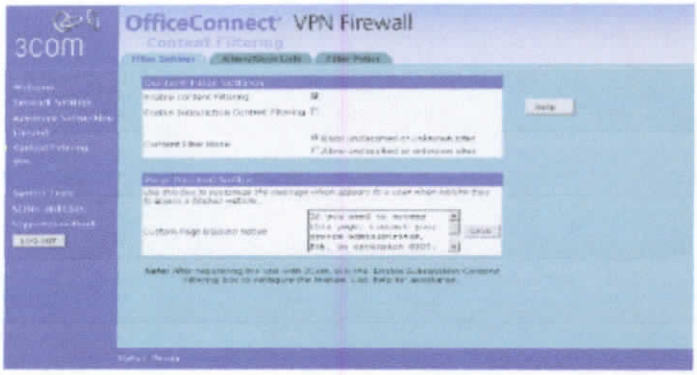
Filtrado de contenido Local.- se puede entrar a las URLs, direcciones IP o palabras claves de los sitios que permiten ser vistos o ser bloqueados.

Suscripción de filtrado de Contenidos.- se puede elegir, qué sitios son permitidos, ser vistos o ser bloqueados dependiendo de su contenido. Este es un servicio de suscripción basado en el registro de la unidad en el sitio Web 3Com.

Política de filtrado.- Se puede excluir ciertas PC de la red LAN con el filtrado de contenido especificando sus direcciones del IP.

Ajustes del filtrado

Verificar la pantalla que permite el filtrado de contenidos. Ver el cuadro de Filtrado.

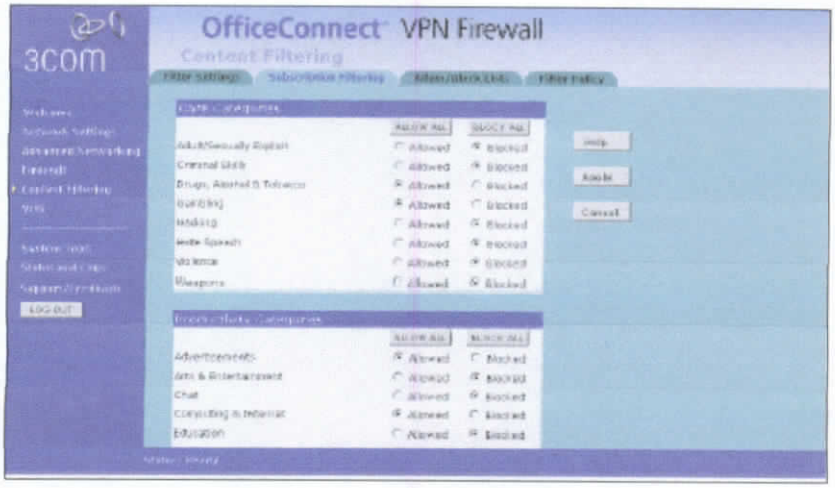


Usando los ajustes de filtrado en la pantalla, se puede:

- Chequear el contenido de suscripción que se filtra, para esto se exhibe el menú de filtración.
- Selección de Filtro de contenidos.- Este filtro permite comprobar sitios sin clasificar o desconocidos. Cuando el modo contenido del filtro se fija para bloquear sitios sin clasificar o desconocidos solamente los sitios permitidos pueden ser vistos.
- Modificar el mensaje para requisitos particulares, que aparece a un usuario cuando intenta tener acceso a un sitio Web bloqueado.

Suscripción de Filtrado

La suscripción permite elegir los sitios permitidos o bloqueados dependiendo de su contenido.



Para permitir o bloquear categorías:

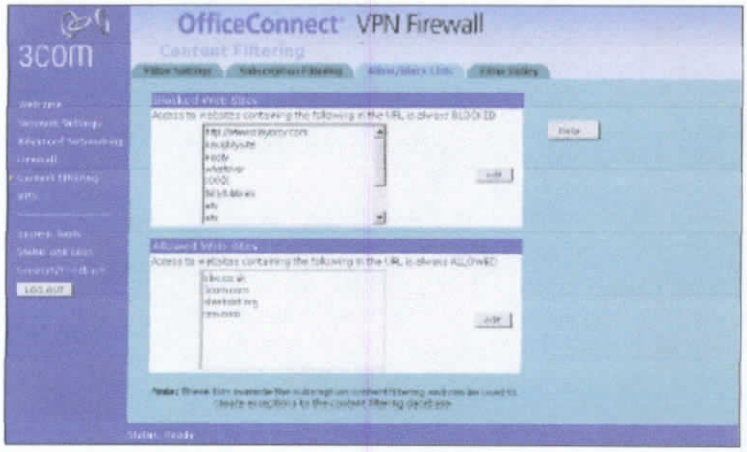
- Chequear la caja permitida o bloqueada contra cada base y categoría de la productividad como sea necesario.

- Clic para permitir que se fijen todas las categorías a permitir, o bloquear todos para fijar las categorías a bloquear.

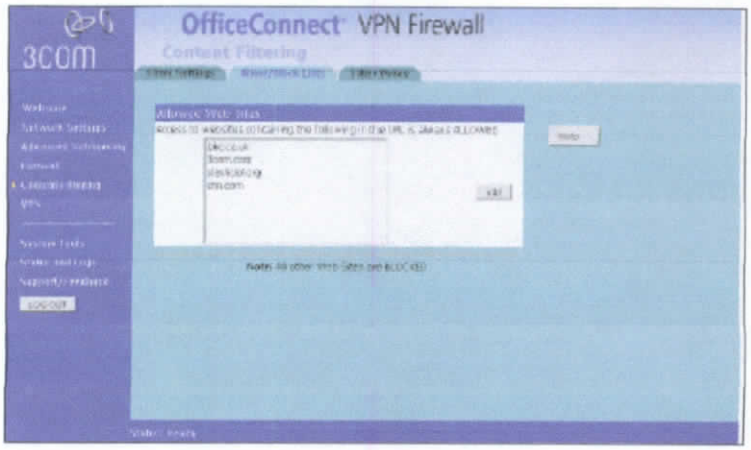
Permitir/las listas del bloque

Para fijar las listas permitir/del bloque, chequear el permiso de la filtración de contenidos en la pantalla de los ajustes del filtro y comprobar el modo de contenidos requerido del filtro. Seleccionar la lengüeta de las listas de permitir/bloquear para exhibir en la pantalla las listas del permitir/del bloque.

Si la filtración del contenido de la suscripción se comprueba en la pantalla los ajustes del filtro, se despliega una pantalla como en el cuadro siguiente.

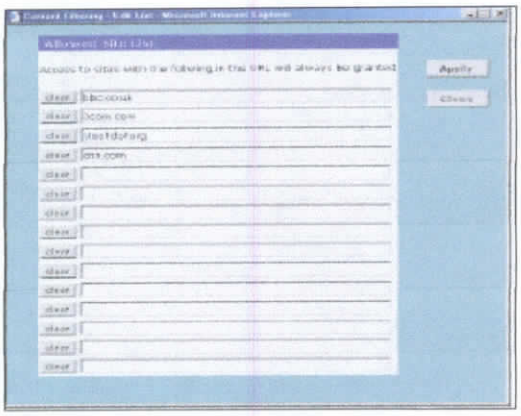


Si el permiso de filtración del contenido de suscripción no se comprueba en la pantalla de ajustes del filtro, se despliega una pantalla como el cuadro



Para instalar una lista de sitios:

1. *Hacer Clic en editar el display* para exhibir la filtración de contenidos.
2. Incorporar las URLs, las direcciones del IP o las palabras claves de los sitios que permiten ser vistos o ser bloqueados, dependiendo del contenido elegido modo de filtración.
3. Clic para guardar los cambio



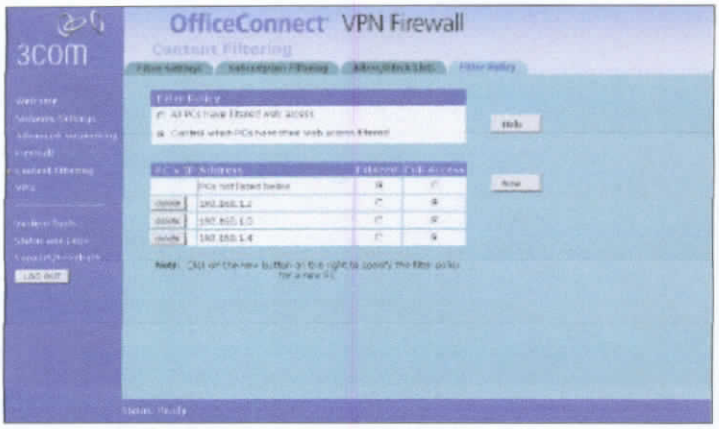
Políticas del filtrado

Para instalar la política del filtro, verificar la filtración de contenidos en la pantalla de los ajustes del filtro. Seleccionar la lengüeta de la política del filtro para exhibir en la pantalla la política del filtro.

Para instalar la misma política de filtración del contenido para todas las PC en la red, verificar todas las PC en el filtrado la caja del acceso.

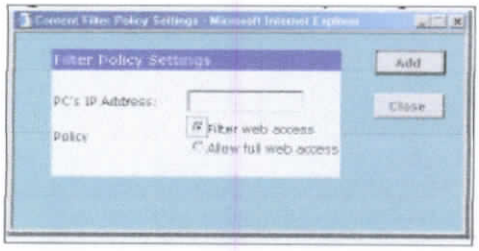
Instalación de las PC el contenido de filtrado:

1. *Chequear el control de las PC que tienen el filtrado de acceso Web a través de la* tabla.
2. Chequear el filtrado necesario del total acceso para cada PC.



Para instalar una nueva política del filtro:

1. Hacer Clic en nuevo, abrir la pantalla de los ajustes de la política de filtrado de contenidos.
2. Entrar a las direcciones IP de las PC's.
3. Chequear una política para la PC.
4. Hacer clic en agrega y configurar el nuevo filtrado.



Configurando el VPNs

Las redes privadas virtuales (VPN) proporcionan una conexión cifrada (o túnel) entre las redes o entre una red y un usuario sobre una red pública (tal como el Internet). En vez de usar una conexión dedicada, un VPN utiliza conexiones virtuales a través de la red pública. El cortafuego de VPN apoya a las conexiones de red y la red a conexiones alejadas del cliente.

Hay dos modos de operación, paso de VPN y servidor. El cortafuego apoya los túneles de IPSec, L2TP IPSec excesivo, y PPTP. Las conexiones que permiten el paso de VPN asegurando los dispositivos en la red y conexiones seguras.

Para permitir paso de VPN, se debe configurar un Virtual Server. Ver "el menú virtual de los servidores"

Fijar el modo de VPN

El cortafuego apoya tres modos de la operación de VPN:

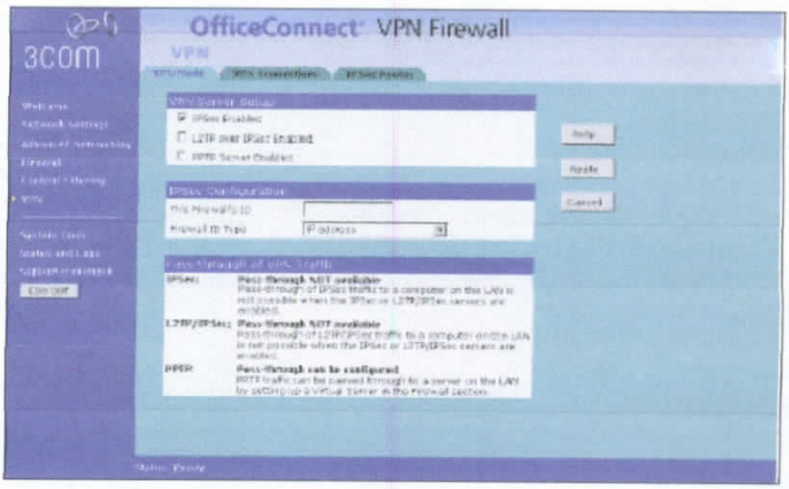
IPSec permitido - IPSec (seguridad del Internet Protocol) es un protocolo seguro complejo con una variedad de métodos de cifrado. El setting-up es una conexión de IPSec entre dos dispositivos deben apoyar el mismo método del cifrado.

L2TP IPSec excesivo permitido - L2TP sobre IPSec es una combinación de dos protocolos. Authentican (con L2TP) y el cifrado de un usuario, los datos (que usan IPSec).

PPTP de los usuarios permitido - PPTP (protocolo realiza un túnel Point-to-Point) es un protocolo cifrado de VPN como IPSec. No es tan seguro como IPSec sino es fácil administrar. PPTP no apoya la entrada a las conexiones y es solamente conveniente para conectar a usuarios remotos.

Configuración de IPSec

En el campo de la configuración de IPSec, se debe incorporar la identificación de este cortafuego como una dirección IP del Internet o nombre del cortafuego. Este valor es común a través de todas las conexiones de IPSec pero no se aplica a las conexiones de PPTP. Si se permite solamente PPTP, el campo de la identificación del cortafuego no aparece.



Configuración de L2TP

Si has permitido L2TP sobre IPSec debes incorporar los puntos siguientes:

1. En el campo de la configuración de IPSec, se incorpora la identificación del cortafuego como una dirección IP del Internet, la dirección del DNS de la unidad o el nombre del cortafuego que estás configurando. El valor es común a través de todas las conexiones de IPSec pero no se aplica a las conexiones PPTP. Si se permite PPTP solamente, el campo de la identificación de este cortafuego desaparece.
2. En el campo de la identificación del cortafuego, seleccionar una de las siguientes:
   - *Dirección IP por (defecto). Debe ser la dirección pública WAN del* cortafuego.
   - La dirección del DNS de la unidad.
   - Un nombre para la unidad.-Es Utilizado cuando no es posible utilizar uno de los otros nodos, por ejemplo, si la dirección IP guarda los cambios.
   - El campo de la configuración de L2TP,
   - El dominio cómo una dirección IP. Un Domain Name localiza un sitio Web en el Internet.
   - *La llave compartida IPSec. Ésta es la llave para la conexión y es una* combinación de letras, de números y de la puntuación y puede ser hasta 64 caracteres en longitud. 3Com recomienda que la llave y la contraseña no sean iguales.
   - El nivel del campo cifrado, elige el tipo del cifrado del DES, de 3DES o de AES. 3DES es más seguro que el DES pero puede durar mucho en descifrar. AES proporciona la seguridad más alta pero tardara más que 3DES cifre y descifre.
4. Configurar el cortafuegos para L2TP IPSec excesivo debes asignar direcciones del IP del LAN del cortafuegos para el uso con L2TP sobre IPSec.

Las direcciones deben estar en una continua gama.

En la piscina de la dirección para los clientes de PPTP y de L2TP, se debe entrar en el campo:

- La primera dirección del LAN debes reservar para L2TP sobre IPSec en el primer campo remoto de la dirección IP.

- La siguiente dirección del LAN debe reservarse para L2TP sobre IPSec en el anterior campo remoto del la dirección IP.

Si se seleccionan PPTP y los modos excesivos de L2TP IPSec, después la piscina de las direcciones es igual para ambos clientes. Estas direcciones deben estar dentro de la sub. red LAN del cortafuego y no deben formar parte de la piscina de DHCP.

1. Hacer Clic para grabar sus cambios.

Configuración de PPTP

Para instalar el cortafuego para PPTP Se debe asignar las direcciones IP del LAN del cortafuego para el uso con PPTP. Las conexiones hechas por PPTP aparecerán estas direcciones. Las direcciones deben estar en una gama continua.

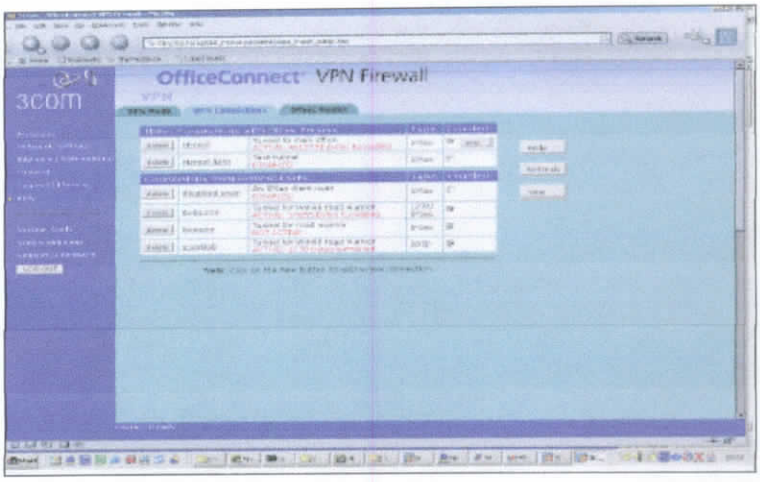
En la piscina de la dirección para los clientes de PPTP y de L2TP en el campo de entrada:

- La primera dirección del LAN que se desee reservar para los clientes de PPTP en el primer campo remoto de la dirección IP.
- La siguiente dirección de LAN que desea reservar para los clientes de PPTP en el siguiente campo remoto de la dirección IP.

Si se seleccionan PPTP y los modos excesivos de L2TP IPSec, después la piscina de dirección es igual para ambos clientes. Estas direcciones deben estar dentro de la sub. Red del LAN del cortafuego y no deben formar la parte de la piscina de DHCP.

Conexiones de la visión VPN

La pantalla de las conexiones de VPN demuestra la información sobre el IPSec, el L2TP IPSec, y las conexiones de PPTP hechas por el cortafuego. También permite que se agregue, suprima, corrija e inhabilita temporalmente estas conexiones.



Para cada conexión configurada para el cortafuego, una fila se agrega a la tabla. Cada fila contiene los puntos siguientes:

Botón de cancelación.- Cancelaciones de la conexión de VPN en esa fila. Esto evitará que el dispositivo o el usuario establezcan una conexión segura con el cortafuego en futuro.

Nombre.- Identifica el túnel. Haciendo clic el nombre de una conexión se exhibe en la pantalla la conexión de corrección del VPN.

Descripción.- Una descripción del texto que permite identificar una conexión. Este campo en la tabla exhibe además si la conexión es actualmente activa.

Tipo.- Indica el tipo de conexión.

Permitido.- Esta permite que se habilite o que se inhabilite una conexión sin suprimirla y así perder los detalles de la conexión.

Prueba.- *tentativas de establecer una conexión (en entrada al modo de la entrada solamente).*

Hay además tres botones fuera de la tabla:

Ayuda.- exhibe la página en línea de ayuda.

El restaurar.- Actualiza el contenido de la ventana permitiendo que se considere el estado actual de las conexiones.

Nuevo.- crea una nueva conexión de VPN.

Agregando y corrigiendo conexiones de VPN

Esta pantalla también permite que se agregue un nuevo IPSec, Al agregar valores en esta pantalla es necesario ingresar ambos lados de un IPSec, un L2TP IPSec excesivo

o una conexión de PPTP no pueden ser activados hasta que ambos extremos del túnel sean configurado.

Tipo de conexión.- Elegir la entrada (solamente disponible con IPSec) para conectar con otra entrada, o acceso de usuario remoto, para crear una conexión para una computadora remota.

Tipo del túnel.- Elegir IPSec (acceso o entrada de usuario remoto), L2TP IPSec sobre PPTP.

Descripción.- Una descripción de la conexión. Esto puede ser diferente en cada cortafuego pues no se utiliza en la conexión.

Si el sitio remoto tiene otra entrada, cortafuego o router con un IPSec establecido, L2TP la conexión será sobre la IPSec o de PPTP entonces allí no es ninguna necesidad de crear una conexión para un usuario remoto en este sitio.
Si se configura una conexión de IPSec para una computadora remota entonces la computadora requerirá el software que apoye a IPSec. Si se configura un L2TP sobre IPSec o la conexión de PPTP para una computadora remota entonces se debe entrar en contacto con Microsoft para la información requerida.
Dependiendo de qué tipo del túnel seleccionado, se debes elegir corregir o agregar los campos restantes:

- "conexiones de IPSec usando el acceso de usuario remoto"
- "conexiones de IPSec usando la entrada a la entrada"
- "conexiones sobre L2TP IPSec"
- "conexiones de PPTP"

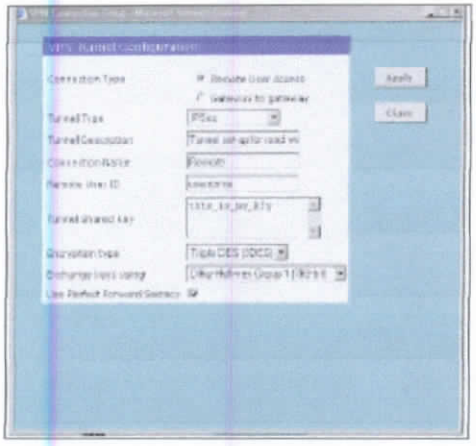
Conexiones de IPSec usando el acceso de usuario remoto

Si se selecciona IPSec como un tipo de túnel y acceso de usuario remoto, cómo tipo de conexión, se debe incorporar los valores siguientes:

Nombre de la conexión.- Incorporar un nombre descriptivo para la conexión.

Usuario remoto.- Incorporar el usuario remoto. Esto se debe entrar idénticamente en el software de IPSec instalado en la máquina del cliente.

Llave compartida del túnel.- es la contraseña para la conexión y es una combinación de letras, de números y de puntuación que puede ser hasta 64 caracteres en longitud.



Tipo del cifrado.- Elegir el tipo del cifrado DES, 3DES o AES. 3DES es más seguro que el DES pero puede tomar para cifrar y descifrar más de tiempo.

3DES y AES no se envían con el cortafuego como estándar debido a las restricciones internacionales en el cifrado.

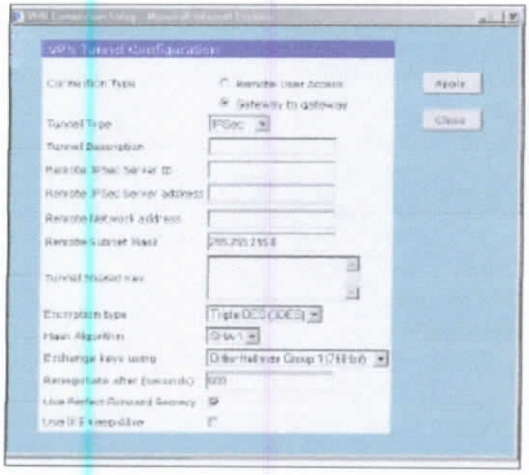
El intercambio de la llave.- Elegir el método del cifrado usado para intercambiar llaves compartidas.

Use Perfect Forward Secrecy.- si se utiliza esta opción .Esto cambiará las llaves de cifrado durante el curso de una conexión que hace el túnel más seguro pero que retarda la transferencia de datos. Para esta función hay que asegurarse del uso. Para guardar la misma llave la dimensión de una conexión se debe dejar la caja desenfrenada. Se hace clic para grabar los cambios o regresar sin guardar los cambios.

Identificación del servidor remoto de IPSec.- En el caso de otro cortafuego de 3Com VPN éste es el campo de la identificación del cortafuego en la página del modo de VPN.

Dirección del servidor remoto de IPSec. - Incorporar la dirección de Internet o el nombre del *DNS* del dispositivo remoto. Un nombre del *DNS* puede ser ingresado solamente si es igual que el IPSec remoto.

Dirección de red remota.- Incorporar la dirección de LAN de la red remota. Éste es la primera dirección de una sub_ red,



Si el dispositivo remoto tiene una dirección IP LAN de 192.168.1.1 y una máscara de *sub red de 255.255.255.0* entonces *la dirección de LAN de la sub red remota es* 192.168.1.0.

Los dispositivos se deben configurar con las gamas la dirección de LAN.

Mascara de la sub red remota.- se fija como 255.255.255.0 por defecto.

Llave compartida del túnel.- es la contraseña para la conexión y es una combinación de letras, de números y de la puntuación y pueden ser hasta 64 caracteres en tamaño.

Si se crea una entrada de conexión, no hay necesidad de recordar el túnel compartido.

Tipo del cifrado.- Elegir el tipo del cifrado del DES, 3DES o AES.

3DES es más seguro que el DES pero puede tomar para cifrar y descifrar más tiempo. AES ofrece la seguridad más alta pero tardara más que 3DES para cifrar y para descifrar. 3DES y AES no se envían con el cortafuego como estándar debido a las restricciones internacionales en el cifrado.

Algoritmo de corte (Hash).-Al elegir SHA-1 o MD5 del lista drop-down. Ambos extremos de la conexión deben utilizar el mismo valor.

El intercambio de clave.- elegir el método de cifrado usado para intercambiar llaves compartidas.

El renegociar después de (los segundos).- controla cuantas veces la conexión será renegociada (y la llave de cifrado cambiado). Períodos más largos son menos seguros pero pueden ser útiles para las conexiones a un equipo más viejo que no tiene energía de proceso de negociar con frecuencia. El valor prefijado es 600 segundos (10 minutos).

Use Perfect Forward Secrecy.- Esto cambia las llaves del cifrado durante el curso de una conexión haciendo el túnel más seguro pero retardando transferencia de datos. Al permitir esta función se asegura de que se compruebe. Para guardar la misma llave de tamaño de una licencia de la conexión la caja desenfrenada.

Use IKE keep- alive.- Cuando está comprobada la entrada procurará asegurarse de que este túnel sigue siendo operacional, aunque allí no es existe tráfico en él. Esto es útil para los túneles donde solamente un extremo puede establecer la conexión (Ejemplo. un extremo del túnel está en una dirección IP dinámica, en este caso fijó a IKE guarda-vivo en el extremo "dinámico" del túnel).

Ejemplo: establecer una conexión de IPSec entre dos cortafuegos de VPN.
El cortafuego uno de VPN está situado en la oficina central y configurada con los ajustes siguientes:
La dirección IP del Internet es: dirección IP LAN 174.19.201.162:
Máscara Sub_net de LAN es: 192.168.1.1:
El cortafuego dos de 255.255.255.0

VPN está situado en la oficina de ventas y configurado con los ajustes siguientes:
Dirección IP de LAN es: 172.27.34.202:
Máscara Sub_net remoto es: 192.168.2.1:

Máscara Sub_net remota es: 255.255.255.0

El cortafuego remoto de VPN usando este ejemplo podría ser cualquier otro dispositivo permitido VPN IPSec-que termina, Ejemplo un cortafuego de SuperStack Para instalar una conexión de IPSec entre los dos cortafuegos de VPN, se debe hacer lo siguiente en cada dispositivo:

IPSec selecto permitido de la pantalla del modo de VPN.

Incorporar la dirección IP de Internet en el cortafuegos que está configurando, en este campo se debe hacer lo siguiente:

1. Insertar 174.19.201.162 en el cortafuego uno.
2. Entra en 172.27.34.202 en el cortafuego dos.
3. Interruptor a la pantalla y hacer clic en las conexiones del VPN.
4. Asegurarse que la entrada al botón de radio esté seleccionada.
5. Verificar que IPSec está seleccionado como el tipo del túnel.
6. En el campo de descripción del túnel entrar: Conexión de la oficina central a la oficina de ventas.
7. En el campo remoto de la identificación del servidor de IPSec incorporar la identificación del cortafuego remoto.
   a) Insertar 172.27.34.202. en el cortafuego uno
   b) Insertar en 174.19.201.162 en el cortafuego dos
8. Incorporar la dirección IP de Internet del otro cortafuego en el campo de dirección remoto del servidor de IPSec.
   a) Insertar 172.27.34.202 en el cortafuegos uno.
   b) Insertar 174.19.201.162 en el cortafuego dos.
9. Incorporar la dirección IP del otro sub_net de LAN en el campo de dirección de red remota
   a) Insertar 192.168.2.0 en los cortafuegos uno.
   b) Entra en 192.168.1.0 en el cortafuegos dos.
10. En este ejemplo, la mascara de sub_red remoto es un ajuste por defecto de 255.255.255.0.
11. Incorporar una contraseña en el campo dominante en túnel compartido en ambas entradas Ejemplo: TYP0249//23b.

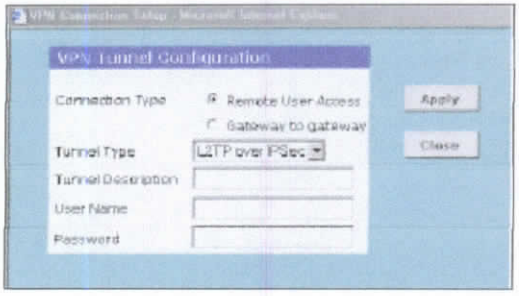
12. Elegir 3DES como el tipo del cifrado.
13. Elegir SHA-1 como el algoritmo del corte Hash.
14. Elegir el grupo 2 (1024 de Diffie-Hellman - mordido) en las llaves del intercambio usando la caja drop-down.
15. El sistema renegocia después de (los segundos) a 600.
16. Asegurarte que la caja delantera tenga la licencia comprobada
17. Agregar para ahorrar la nueva conexión

Conexiones excesivas de L2TP IPSec

Si se selecciona L2TP sobre IPSec como tu tipo de túnel, incorporar los valores siguientes:

Nombre de usuario.- Éste es el nombre de usuario que el cliente remoto de VPN utilizará al conectar.

Contraseña.- *La contraseña que necesitará ser proveída para conectar.*



Se graba los cambios o se regresa sin grabar estos cambios. Cuando se ha creado una cuenta del usuario, el usuario necesitará saber para permitir la conexión.

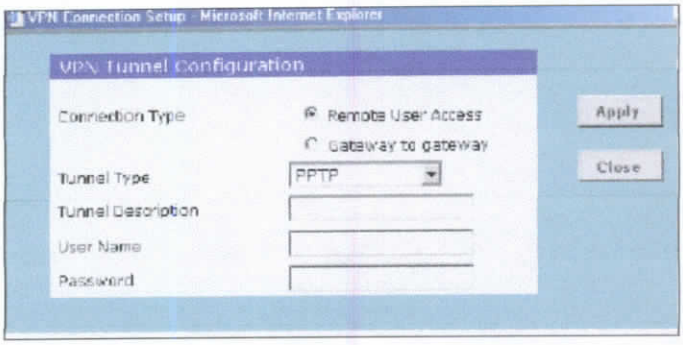
Conexiones de PPTP

Si se seleccionado PPTP como tipo del túnel, debes entrar en lo siguiente:

Nombre de Usuario- Éste es el nombre de usuario que el cliente remoto de VPN utilizará para conectarse.

Contraseña.- La contraseña que el usuario necesitará proveer para conectar.

Cuando se ha creado una cuenta de usuario, el usuario necesitará saber el nombre y la contraseña se ha asignado.



Las pantallas para corregir y para agregar un usuario de PPTP contienen los mismos campos. Se graba los cambios o se regresa sin grabar estos cambios.

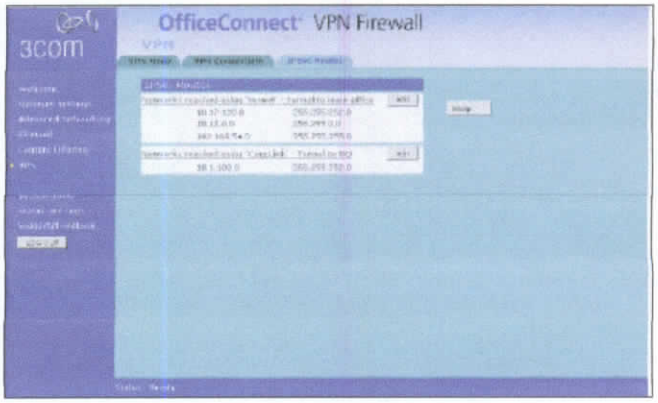
Corregir las rutas de IPSec

La lengüeta de las rutas de IPSec se exhibe solamente cuando IPSec es permitido se selecciona en la pantalla del modo de VPN. Esta pantalla permite agregar y sustituir redes en la ruta existente de IPSec.

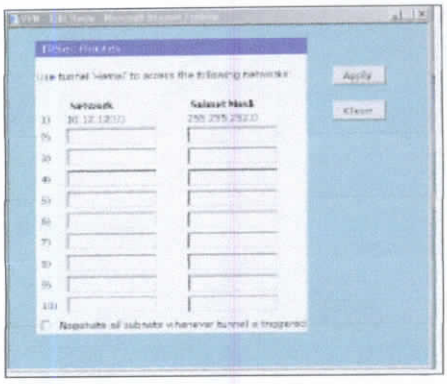
Para hacer esto:

1. *Seleccionar corregir para exhibir la pantalla de la ruta del corregir.*
2. Hacer clic en la tabla y agregar una nueva entrada de red y máscara de sub_red.
3. Has clic para aplicar y grabar los cambios o salir si grabar estos cambios.

En la entrada de una red remota se debe también fijar el túnel de VPN para tener acceso a tu red local. Por lo tanto, se debe incluir la máscara de sub_red para una red remota en la ruta de IPSec, entonces la red remota debe también incluir la máscara de sub_red en la ruta de IPSec.



Edit Route

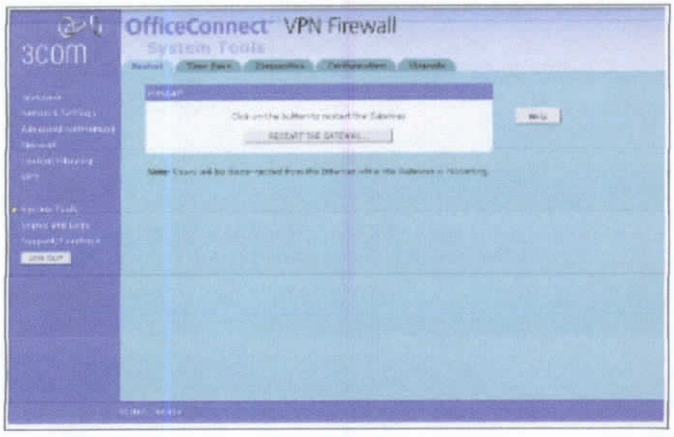


Tener acceso a las herramientas del sistema

El menú de las herramientas del sistema incluye cuatro artículos de la administración: recomenzar, diagnosticar, zona de tiempo, configuración, y mejorar.

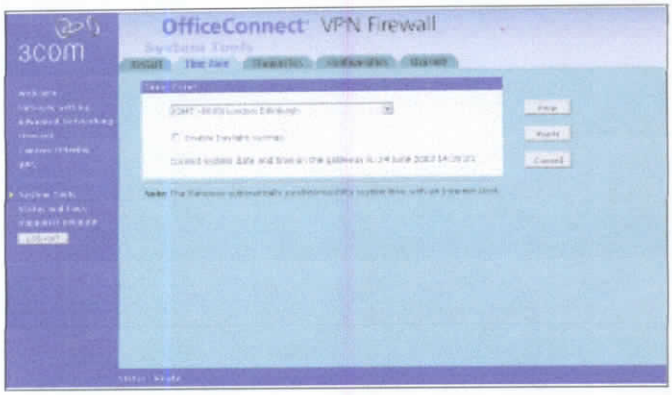
Recomenzar

Presionando el botón recomenzar de la entrada tiene el mismo efecto que la energía que completa un ciclo la unidad. No se perderá ninguna información de la configuración pero los ficheros de diario serán borrados. Esta función puede ser de uso si estás experimentando problemas y deseas reestablecer la conexión del Internet.



Zona de tiempo

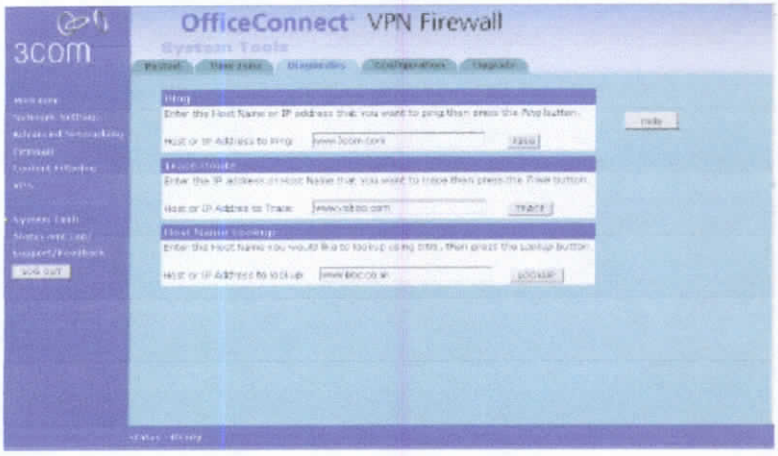
Elegir la zona de tiempo que está la más cercana a la localización real. El ajuste de la zona de tiempo es utilizado por el reloj del sistema al exhibir el tiempo correcto en los ficheros de diario.



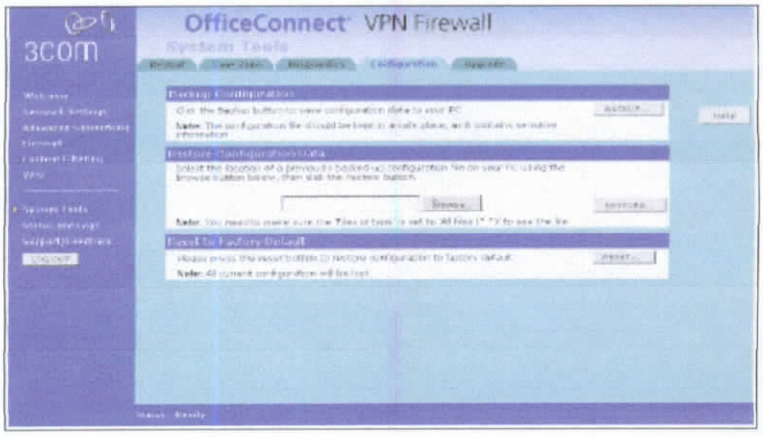
El cortafuego lee el tiempo correcto de los servidores del NTP en el Internet y fija su reloj del sistema por consiguiente. La opción de los ahorros de la luz del día ajusta automáticamente el reloj al tiempo de los ahorros de la luz del día como apropiado a la zona de tiempo.

Diagnóstico

Esta pantalla proporciona ping, la ruta del rastro e instalaciones de las operaciones de búsqueda del nombre de anfitrión.



Cargamento y ahorro la configuración del cortafuego



Reserva.- Para guardar las configuraciones actuales del cortafuego del Firewall VPN. Se incitarán a descargar y grabar un archivo al disco.

Si se desea reinstalar los ajustes de la configuración guardados previamente a un archivo, se debe dar clic y verificar para localizar el archivo de reserva en la computadora, y después restaurar para copiar la configuración detrás al cortafuego.

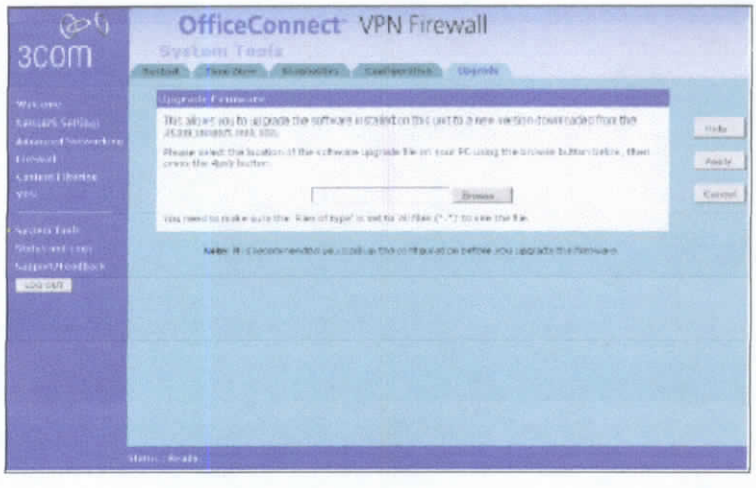
Para la seguridad los propósitos que restauran la configuración no cambian la contraseña.

Si deseas reajustar la configuración que es propia del Firewall, se debe dar clic en reajustar. Pero se pierde todos los cambios de configuración. La dirección del LAN del cortafuego invertirá a 192.168.1.1, y el servidor DHCP en el LAN será permitido.

Aumento de los soportes lógico inalterable del cortafuego

La facilidad de la mejora permite Instalar en el cortafuego cualquier nuevo lanzamiento del software del sistema que 3Com pueda hacer disponible.

3DES y el cifrado de AES no se envían con el cortafuego como estándar debido a las restricciones internacionales en el cifrado.



Una vez que se ha descargado el software, utilizar el botón de verificar para localizar el archivo en la computadora, y después dar clic para aplicar.

El archivo será copiado al cortafuego, y una vez que éste tenga terminado, el cortafuego recomenzará. Aunque el mejor proceso se ha diseñado para preservar la configuración los ajustes, 3Com recomiendan realizar una reserva por si se pierde la configuración, en caso de que el proceso de mejora falle por cualquier razón (por ejemplo, la conexión entre la computadora y el cortafuego mientras que el nuevo software se está copiando al cortafuego).

El procedimiento de la mejora puede tomar algunos minutos, y es completo cuando el *LED* alerta ha parado de destellar y está permanentemente apagado. Verificar que no interrumpas energía al cortafuego durante el procedimiento de la mejora; si lo haces, el software puede ser corrompido y el cortafuego puede no empezar para arriba correctamente luego. Si se adelanta el LED alerta continuamente o destellando lentamente después del fallado la mejora.

Estado y registro de visión

Seleccionar estado de registros del menú principal exhibe el estado y registra las pantallas en la Web. La pantalla de estado y de los registros exhibe una representación tabular de tu red y conexión del Internet.

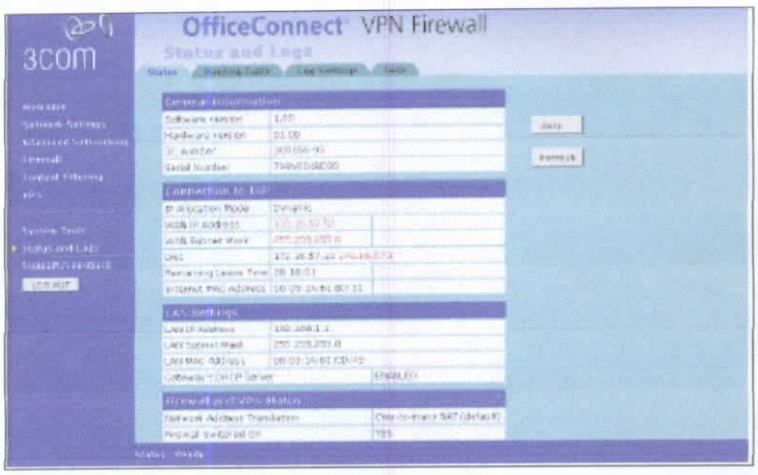
Estado.- exhibir el estado de la unidad actual, incluyendo un resumen de la configuración.

Tabla de encaminamiento para exhibir los encaminamientos estáticas y dinámicas configuradas.

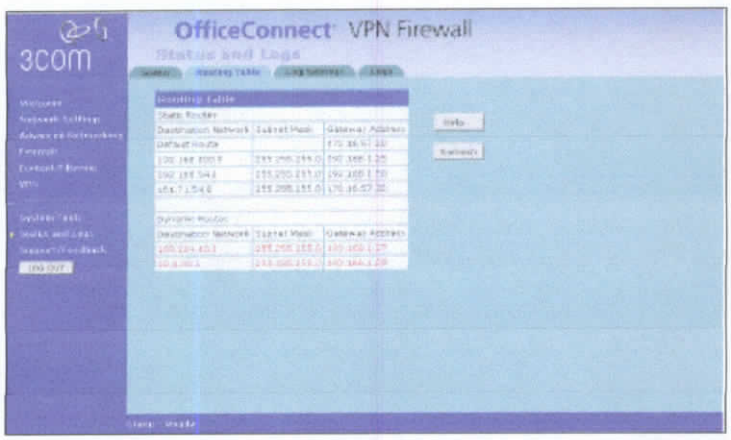
Ajustes del registro.- Elegir si almacenar la conexión el cortafuego o enviarla al usuario remoto o a ambos y elegir a permitir o inhabilitar algunas entradas del registro.

Si eliges la opción para almacenar la conexión el cortafuego, el fichero de diario será sobre escrito cuando esta lleno. Si eliges la opción para enviar registros a un servidor remoto entonces necesitarás especificar la dirección IP del servidor remoto. La dirección IP debe estar dentro de la sub_red LAN y un servidor del syslog se debe instalar en el servidor remoto.

Registros.- Ver ambos los acontecimientos normales, y amenazas de la seguridad registradas por el cortafuego



Puedes ser pedido referir a la información sobre la pantalla del estado si entras en contacto con tu proveedor para la ayuda técnica



Fotograma de Dificultades

Verificar Conexiones básicas

- Verificar el Firewall si esta conectado en la computadora y el cable/DSL MODEM, y que todos los equipos estén prendidos. Verificar que el LAN, el link del Cable/DSL y el estado de los led´s estén iluminados, y que los led´s correspondiente al Cable/DSL estén frecuentemente iluminados.
- Asegurar que las computadoras tengan completo el proceso de arranque y se encuentre bien para su uso. Muchas de las interfaces de las redes pueden no estar correctamente hasta que el proceso este completo.
- Asegurar que el Firewall este completo y este prendido.
- Si el link de estado de Led no esta iluminado por el puerto que esta conectado, verificar que el cable no este defectuoso. Comprobar con otro cable diferente

Pantallas de configuración en el Firewall

Si esta conectado el Firewall y las computadoras juntas, pero no aparece la configuración en la pantalla, verificar lo siguiente:

- Confirmar que la conexión física entre la computadora y el firewall este bien, y que el estado de unión de Led este iluminado en el Firewall los mismos que indican la velocidad (10 Mbps o 100 Mbps). Muchos no tienen el estado de los Led´s, en este caso el programa puede evaluar y puede dar la información.
- Asegurar que este configurado la computadora como se describe " Instalación de Computadora" resetear la computadora mientras este conectado el Firewall y asegurar que la computadora reciba la dirección IP
- Cuando se pone la dirección en el Firewall dentro de la Web, asegurar de incluir el URL incluido el htpp: // preferente. (Ej. http://192.168.1.1)

Conectar al Internet

Si se lee las pantallas de configuración pero no accede a los sitios de Internet, verificar los siguientes:

- Confirmar la conexión física entre el Firewall y el Cable/DSL MODEM este bien, y el estado de link entre el Firewall y el MODEM este iluminado.

- Confirmar que la conexión entre el MODEM y el Cable/DSL se encuentre bien.
- Asegurar que la información colocada en las pantallas de configuración del Firewall sea correcta, y dada por el ISP
- Para los usuarios DSL, verificar el nombre de PPPoE o PPTP, la clave, y el nombre de servicio correcto, si estos son requeridos. Solamente colocar el nombre del servicio si el ISP requiere uno.
- Para usuarios de cable, verificar el ISP requerido y la dirección MAC. Si se usa las características de la dirección MAC en el Firewall asegurar que sea correcta la dirección MAC.
- Asegurar que la computadora no este configurado como Web Proxy. En windows, este puede funcionar bajo, panel de **control>opciones de Internet>conexiones**
- Verificar los privilegios sean vistos, si se tiene permiso para conectar la PC al Internet.

Olvidar la clave

Si se puede leer las pantallas de configuración pero no entrar o porque no se conoce o se olvido la contraseña, seguir los siguientes pasos de abajo y resetear el Firewall. Nota: todas las configuraciones cambian y se puede perder, y es necesario ejecutar el Wizard nuevamente antes reestablecer la conexión con el Internet. Solamente otros usuarios pueden perder la conexión de red, este proceso toma lugar, cuando escoge un tiempo y esto es conveniente.

1. Prender le firewall.
2. Desconectar todas las computadoras y el Cable/DSL MODEM para el Firewall.
3. Usar el cable Ethernet, conectar el cable/DSL en el puerto y el otro extremo colocar en un puerto LAN del panel del firewall.
4. Resetear nuevamente el Firewall. El led de alerta puede estar prendiéndose, como cuando el firewall empieza a ejecutar, y después de 30 segundos aproximadamente, empieza el flash mas despacio (típicamente 2 segundos prendidos, y 2 segundos apagado)

5. Remover el cable que esta conectado en el puerto del Cable/DSL, en el puerto de LAN y reconectar una de las computadoras a un puerto LAN.
6. Resetear el Firewall, y cuando la secuencia de ejecución a completado. Y la dirección es http://192.168.1.1, y empezar la configuración. Es probable que necesite resetear la computadora antes de empezar la configuración.
7. Cuando la configuración del Wizard ha completado, se puede conectar la red como estaba antes.

Led de alerta

Cuando el Firewall se prende, el Led de alerta puede estar prendido de tres a cinco segundos, y luego empezar a titilar, mientras el sistema de software verifica las propiedades de operación.

El Led de alerta puede continuar titilando por cinco minutos o más, dependiendo de la configuración de la red. Una vez que el Firewall empieza la operación normal, la alerta desaparece.

Si la alerta no se desaparece, significa lo siguiente; iluminado continuamente, indica que el software detecta un posible desperfecto con el hardware. Si la alerta esta titilando lento esto indica que el Firmware falla. Apagar el Firewall por 10 segundos y luego volver a prender. Si el led de alerta empieza a prender continuamente, luego de la falla detectada, entonces se refiere "software corrompido"

Durante la operación normal, la luz de alerta se prende tiempo a tiempo. Esto indica que el Firewall detecta un ataque de hacker de Internet y previene, que haga daño en la red. Es necesario tomar especificaciones de este acto, al menos que se decida que este ataque sea de ayuda, en este caso es necesario comunicarse con el ISP.

Recobrarse de un Software corrompido

Si el led de alerta titila lento, prende y apaga, es posible que el sistema de software pueda estar corrompido. En esta condición el firewall puede entrar en proceso seguro; DHCP este deshabilitado, y la dirección de LAN es establecido 192.168.1.1. Seguir las siguientes instrucciones y realizar una copia del sistema de software del Firewall.

Asegurar que una de las computadoras tenga una copia del nuevo software en el archivo del disco Duro. Si no contactar con 3COM http://3com.com

1. Apagar el Firewall y desconectar el Cable/DSL MODEM y todas las computadoras con la imagen del software
2. Es necesario reconfigurar la computadora con las siguientes direcciones IP
   - Dirección IP 192.168.1.2.
   - Mascara de Sub-Red: 255.255.255.0
   - Dirección de Gateway por defecto: 192.168.1.1
3. Resetear la computadora, y prender el Firewall
4. Usar la Web en la computadora, colocar el siguiente URL: http://192.168.1.1,
5. Seguir las instrucciones de la pantalla. Colocar la trayectoria y el nombre del archivo del software
6. Cuando el proceso ha completado, resetear el Firewall, ejecutar, si está bien la operación la alerta desaparece.
7. Reconectar el Firewall el Cable/DSL MODEM y la computadora en la red. No olvidar la reconfiguración de la computadora y usar el software.

Preguntas Frecuentes

¿Cuantas computadoras soporta en LAN el Firewall VPN?

Soporta un máximo de 253 computadoras en LAN

¿Hay solamente cuatro puertos LAN en el Firewall? ¿Cómo son conectadas *otras computadoras?*

Se puede expandir el número de conexiones en LAN usando Hubs, Switches, conectados al Firewall.

¿EL firewall soporta la Red Privada Virtual?

El software tiene un completo soporte VPN:

- Inicia y termina en conexiones IPSec
- Termina en conexión L2TP encima IPSec y PPTP
- Provee encriptación acelerada con hardware para IPSec VPNs y SPSec VPNs con *L2TP encima IPSec*

- Provee VPN
- *Configuración 50 túneles VPN*

¿Dónde se puede bajar software para el Firewall?

Los VPN firewall son destino de 3COM Y el soporte esta en el sitio Web que se puede visitar: http://www.3com.com

¿Cuántas otra fuentes en línea hay?

El conocimiento de 3com: http://knowledgebase.3com.com es la base de datos técnicos que cubre todos los productos de 3COM.

Direccionamiento IP

EL protocolo de Internet consiste en definir correctamente el set de protocolos de comunicación y un estricto estándar de protocolos de aplicación. La transmisión de protocolos de Internet (TCP/IP). Es probable conocer la combinación de dos protocolos (IP y TCP) para que trabajen juntos. TCP/IP es adoptado internacionalmente y el soporte de red, es estándar y provee conectividad entre el equipo y muchos vendedores encima de una variedad de redes de tecnología.

Dirección IP y Masacra de Sub-red

Cada dispositivo en la red puede tener una única dirección IP para operar correctamente. Una dirección IP, identifica la dirección del dispositivo para que la información sea enviada a esa dirección de destino en la Red. La dirección IP tiene un formato n.n.n.x donde **n** es un numero decimal entre 0 y 255, y **x** es un numero entre 1 y 254 inclusive

Sin embargo, la dirección IP solamente, no es suficiente para que el dispositivo opere. Además de las direcciones IP, son necesarias las direcciones de la mascara de Sub_Red. Todas las redes son divididas en pequeñas Sub_Redes y en mascara de Sub_Red, es un numero que habilita al dispositivo y identifica la Sub_Red con la cual esta conectado.

Para que la red trabaje correctamente, se debe seguir los siguientes consejos:

- La misma dirección de Sub_Red
- *La misma mascara*

Un ejemplo de dirección IP es '192.168.100.8' Sin embargo el tamaño de la red determina la estructura de la dirección IP. Cuando se usa el Firewall es probable, solamente contar con dos tipos de dirección IP y la estructura de mascara de Sub_Red

Primer tipo

En una red pequeña, la dirección IP es '193.168.100.8' se divide en dos partes:

- Parte uno ('192.168.100') identifica la red en cual el dispositivo reside
- Parte dos ('8') identifica el dispositivo entre la red

Este tipo de dirección IP opera con una mascara de sub_red '255.255.255.0'

En la siguiente tabla hay un ejemplo acerca de una red con tres PC´s y un VPN Firewall

Dispositivo	Dirección IP	Mascara de Sub_Red
PC1	192,168,100,8	255,255,255,0
PC2	192,168,100,33	255,255,255,0
PC3	192,168,100,188	255,255,255,0
VPN Firewall	192,168,100,72	255,255,255,0

Segundo Tipo:

En una red grande, donde hay más dispositivos, la dirección IP de '192.168.100.8' es nuevamente dividida en dos partes pero la estructura es diferente:

- Primera parte ('192.168') identifica la red en la cual reside el dispositivo
- Segunda parte ('.100.8') identifica el dispositivo dentro de la red

Este tipo de dirección IP, opera la mascara de sub_red '255.255.0.0'

En la siguiente tabla se muestra un ejemplo (solo de cuatro PC´s) y el Firewall VPN que puede ser configurado:

Dispositivo	Dirección IP	Mascara de Sub_Red
PC 1	192,168,100,8	255,255,0,0
PC 2	192,168,201,30	255,255,0,0
PC 3	192,168,113,155	255,255,0,0
PC 4	192,168,2,230	255,255,0,0
VPN Firewall	192,168,2,72	255,255,0,0

¿Cómo el dispositivo obtiene la dirección IP y la mascar de Sub_Red?
Hay tres diferentes formas de obtener la dirección IP y la Mascara de Sub_Red:

- Configuración de la dirección dinámica del Host (DHCP)
- Dirección estática
- Dirección automática (Auto_IP dirección)

Dirección DHCP

El Firewall contiene un servidor DHCP, con permisos para que las computadoras obtengan la dirección IP y la Mascara de sub_red en la red, automáticamente. DHCP asigna temporalmente la dirección IP y la mascara de Sub_Red con la cual se asigna el Firewall. DHCP es particularmente usado para grandes redes.

Dirección estática

Se puede colocar una dirección IP y la mascara de sub_red manualmente en cada dispositivo. Usar la dirección estática y la mascara de sub_red, significa que la dirección es permanente.

Dirección IP Automática

Los dispositivos de Red usan automáticamente la dirección IP las redes están configuradas para adquirir una dirección usando DHCP, pero son imposibilitados para contactar con un servidor DHCP. Automáticamente la dirección IP es un esquema donde los dispositivos asignados con una IP, están en el rango de estándar *de la industria y la mascara de Sub_Red es 169.254.X.X* (con la mascara de Sub_Red 255.255.0.0). Si existen dos dispositivos con la misma dirección IP el conflicto es detectado y uno de los dispositivos asignados debe darse otra dirección.

Dirección IP Privada

Las siguientes direcciones tienen un rango, y tiene reservado para Internet

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

EL Firewall tiene detectado por defecto la Sub_Red 192.168.1.255. 3COM recomienda que el uso de la dirección de Sub_Red en LAN, en el primer dispositivo

y la sub. Secuencias de rangos (192.168.2.0- 192.168.2.255) para el rango de LAN o otros dispositivos que sean conectados al Firewall.

Glosario del manual de usuario

10BASE-T

La especificación de la IEEE para Ethernet rápido de 10 Mbps, sobre la categoría 3, 4,5 de cable

100BASE –TX

La especificación de la IEEE para Ethernet rápido de 100 Mbps, sobre la categoría 5 de cable.

3DES

Triple DES es una extrema seguridad, 168 bits de encriptación, sistema que trabaja aplicando encriptación DES, sistema de tres tiempos en el mismo mensaje usando diferentes llaves. Es típicamente usado en aplicaciones militares donde es espectado con el trafico VPN que puede ser interceptado.

AES

Estándar de Encriptación Avanzado. A 256 bits aprobado por el sistema de algoritmos de encriptación y es usado por el gobierno U.S. AES provee alta seguridad que 3DES

Ancho de Banda

Es la información de capacidad, la medida de bits por segundo, y cuanto puede transmitir el canal de transmisión. El ancho de banda de Ethernet es de 10 Mbps, el ancho de banda de Ethernet rápido es de 100 Mbps.

Categoría 3 Cables

Uno de los 5 grados de (TP) cableado definido por EIA/TIA-586 estándar. Categoría 3 es grado de cable y puede solamente ser usado en la red de Ethernet (10BASE-T) Para trasmitir información a una velocidad de 10 Mbps.

Categoría 5 Cable

Uno de los 5 Grados de (TP) cableado definido por EIA/TIA-586 estándar. Categoría 5 puede ser usado en Ethernet (10BASE-T) y Ethernet rápido en red de (100BASE-TX) y puede trasmitir información a una velocidad de 100Mbps. El cableado de Categoría 5 es mejor usar en la red que el cableado de categoría 3, porque el soporte entre Ethernet (10 Mbps) y el Ethernet rápido (100Mbps)de velocidad

Cliente

El termino es usado para describir el nombre de al computadora que es conectado a la red

DES

Estándar de encriptación de Información. DES es una de los protocolos de encriptación que pueden ser usados por una IP virtual privada. es un estándar de encriptación, solamente usado en seguridad por 3DES

DHCP

Protocolo de configuración dinámico del Host. Este protocolo automáticamente asigna la dirección IP para cada computadora dentro de la red. Windows 95, windows 98 y windows NT 4.0 contienen software que asignan la direcciones IP automáticamente a las estaciones de trabajo dentro de la red. Estas asignaciones son realizadas por el servidor DHCP que se ejecuta en el servidor de windows NT, y windows 95 y windows 98 las cuales pueden llamar al servidor APRA obtener la dirección. Windows 98 puede localizar la dirección aun sin no tiene el servidor DHCP.

DNS

Nombre de Servidor de Dominio. DNS permite que las computadoras del host de Internet tengan un nombre de dominio (tales como 3com.com.) y una o mas direcciones IP (tales como 192.34.45.8.) un servidor DNS mantiene la base de datos en el host de una computadora y sus respectivos nombres de dominio y las direcciones IP, por lo tanto cuando un nombre de dominio es preguntado, el usuario

envía con la dirección IP. El servidor DNS es usado por las computadoras en la red. es la dirección de localización del servidor DNS por el ISP asignado.

DSL modem

Línea de suscripción digital. Un DSL es usado para línea telefónica para enviar y recibir la información en alta velocidad.

Ethernet

Una especificación LAN descubierta por Xerox. La red Ethernet es usado para trasmitir paquetes a un rango de 10 Mbps.

Ethernet rápido.

Un sistema de Ethernet que es designado para operar a 100Mbps.

Firewall

Una protección electrónica que previene a la red que sus archivos sean dañados y las computadoras.

Full Duplex

Un sistema que permite a los paquetes sean trasmitidos y recibidos en el mismo tiempo y en efecto, duplicar el potencial a través del link.

Gateway

Es un dispositivo que actúa como un Hub central y esta conectado a cada computadora, la interfase de la red y la tarjeta de interfase esta controlando el tráfico de la información entre la red local y la de Internet.

Half duplex

Un sistema que permite trasmitir paquetes y recibir, pero no en el mismo tiempo. Lo contrario que Full duplex.

HUB

Es un dispositivo que regenera el trafico de LAN por lo que la distancia de transmisión se puede extender. Hubs son similares a los repetidores, que son los que conectan LAN en el mismo tipo sin embargo se puede conectar mas LAN que un repetidor y son generalmente mas sofisticados.

IEEE

Instituto de ingenieros de electricidad y electrónica. Esta organización Americana fue fundada en 1963 y establecida como estándar de computadoras y comunicaciones.

IETF

Fuerza de ingeniería e Internet. Una organización responsable de proveer soluciones para red TCP/IP.

IP

Protocolo de Internet. IP es una capa 3 el protocolo. Es un estándar para enviar información a través de la red. IP es parte de TCP/IP y describe la rutina de los paquetes y la dirección de los dispositivos. Una dirección IP consiste en 32 bits dividida en dos partes o tres archivos. El numero de red y el número de host o el número de red, y el numero de la mascara, y el nuecero de host.

Dirección IP

Protocolo de dirección de Internet. Un único identificador de un dispositivo dentro de la red usando TCP/IP. La dirección es escrita como cuatro octetos separados. Y esta realizado por secciones, la subred es opcional y la sección del host.

IPSec

Protocolo de Seguridad de Internet. Es un protocolo de encriptación basado en TCP/IP. Este protocolo es flexible con un gran rango de opciones de encriptación. IPSec es usado para dos conexiones entre red privada y conexiones entre PC's remotas y red privada.

ISP

Servicio de Proveedor de Internet. Un ISP es un negocio que provee conectividad con el Internet para individuales y tras negocios de organizaciones.

LAN

Red de área local. Una red de estaciones terminales (tales como Pc's, impresoras, y servidores) y red de dispositivos (hubs y switches) que cubren la relativa geografía pequeña. LAN's son característicos por la alta velocidad de transmisión sobre cortas distancias (hasta 1000 metros).

L2TP sobre IPSec

L2TP sobre IPSec es una combinación de protocolos comúnmente usados por autenticidad de un usuario (L2TP) e información de encriptación (usando IPSec)

MAC

Control de acceso. Un protocolo especificado por la IEEE para determinar cuáles dispositivos tiene acceso a la red.

Dirección MAC

Dirección de control de acceso llamado Hardware, fisicamente la dirección de Ethernet. Una dirección de Capa 2 asociada con un dispositivo de red particular. La mayoría de dispositivos que conectan LAN tienen dirección MAC asignado, para los dispositivos las cuales son usadas para identificar otros dispositivos en la red. La dirección MAC tiene un largo de 6 bytes.

NAT

Traslación de direcciones de red. NAT habilita a las computadoras dentro de la red a medida de una dirección IP. NAT tiene da capacidad al Firewall para permitir el acceso a Internet de una computadora a muchas computadoras en la red casera sin tener que comprar mas direcciones IP al proveedor de Internet

Red

Una red es una colección de computadoras y otros equipos que están conectados con el propósito de intercambiar información y otras fuentes. La red varía en tamaño y muchas están en un solo cuarto y otros sobre continentes.

Tarjeta de interaface en la Red (NIC)

Un circuito instalado en una parte de un equipo de computación, por ejemplo, una computadora, que habilita para conectar la red. Un NIC solamente reconoce como un adaptador o tarjeta de adaptación.

Ping

Paquete de Internet. Una utilidad de Internet usado para determinar dentro de una dirección IP particular en línea. Es usado para hacer prueba en la red y para enviar un paquete y esperar respuesta

Protocolo

Es establecer las reglas de comunicación entre dispositivos de una red. Las reglas dictan formatos, secuencias y un control de error.

PPPoE

Protocolo punto a punto sobre Ethernet es un método de seguridad de información originalmente creado por un radio de conexiones. PPPoE es para conexiones Ethernet

PPTP

Punto a punto canal de protocolo. PPTP es un simple encriptación de protocolo VPN basado en el protocolo punto a punto. Es usado mas frecuente para conexiones remotas en Pc´s de una red privada.

RIP

Protocolo de rutina de información. Una simple rutina de protocolo que es una parte de un grupo de protocolos TCP/IP. Esto determina la ruta basado en pequeños saltos de contadores entre las fuentes de destino. RIP es información para los compañeros de rutina.

Router

Dispositivo que conecta las sub-redes juntos. Los routers son usados en grandes redes como pequeños sub-redes, ellos introducen largos retrasos y típicamente tienen menos velocidad que los puentes.

RJ-45

Es un conector estándar usado para la conexión de red Ethernet. El "RJ" estándar fue registrado por Jack

Server

Una computadora en una red que es medida por múltiples estaciones. Un servidor provee estaciones con acceso a medida de la red, y servicios tales como archivos e impresoras

SPI

Estado de paquete de inspección. Esta característica requiere el firewall para recordar cual paquete puede ser enviado y cuáles solamente recibidos. Esta forma puede acceder a la red o denegar.

Dirección de Sub_Red

Es un esquema de una extensión de dirección IP que permite a un sitio usar una singular dirección IP por múltiple que sea la red fisica.

Mascara de Sub_Red

La mascara de Sub_Red, cual puede ser una parte de la información TCP/IP que provee el ISP. Es un grupo de números de configuración como una dirección IP. Es usado para crear direcciones IP. Números usados solamente entre una red particular. (Es valido como una dirección IP y reconocido por Internet, cual puede asignar por el *InterNIC)*

Sub_Red

Una red que es un componente de una red grande

BIBLIOTECA

Switch

Un dispositivo que conecta grandes LAN´s o una forma de lógica singular LAN´s. los Switches son similares a los puentes, y las conexiones son diferentes. Sin embargo hay mas conexiones LAN que los puentes y son generalmente mas sofisticados.

TCP/IP

Control de Transmisión de Protocolo/ Internet Protocolo este es un nombre de dos de los dos mas conocidos protocolos descubierto por la interconexión de la redes. Originalmente el estándar de UNIX TCP/IP es ahora el soporte de todas las plataformas, y es el protocolo de Internet.

TCP relata el contenido de la información que viaja a través de la red. Asegurando que la información enviada sea recibida. IP realiza la dirección de la estación de destino la cual la información es enviada, como también de la dirección de destino en la red.

Trafico

El movimiento de la información de la red.

VPN

Red Privada Virtual. Un VPN es una red privada virtual donde la información es cruzada por la red pública tales como Internet. La información se mantiene privada usando encriptación.

WAN

Red de Are Grande. Una red que conecta computadoras localizado en geografías separadas (por ejemplo, diferentes construcciones, ciudades, o países). El Internet es un ejemplo de una red de área extensa.

WIZARD

Una aplicación de windows que se ejecuta automáticamente tales como instalación y configuración.

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
BIBLIOTECA