FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

Trabajo de fin de carrera titulado:

DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE SERVICIOS DE RED Y RESGUARDO DE SERVIDORES LINUX A TRAVÉS DE OPEN SOURCE EN LA EMPRESA PROTECO COASIN S.A.

Realizado por:

LUIS GUILLERMO LEÓN BUSTAMANTE

Como requisito para la obtención del título de

INGENIERO DE SISTEMAS EN TELECOMUNICACIONES

QUITO, MAYO DE 2012

DECLARACIÓN JURAMENTADA

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

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

……

Guillermo León

DECLARATORIA

El presente trabajo de investigación de fin de carrera, titulado

DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE SERVICIOS DE RED Y RESGUARDO DE SERVIDORES LINUX A TRAVÉS DE OPEN SOURCE EN LA EMPRESA PROTECO COASIN S.A.

Realizado por el alumno

LUIS GUILLERMO LEÓN BUSTAMANTE

como requisito para la obtención del título de

INGENIERO DE SISTEMAS Y TELECOMUNICACIONES

ha sido dirigido por la profesor

ING. ADRIANA ABAD FREIRE

quien considera que constituye un trabajo original de su autor.

…….

Ing. Adriana Abad Freire

Director

Los profesores informantes

después de revisar el trabajo escrito presentado,

lo han calificado como apto para su defensa oral ante el tribunal examinador.

…… ……..

AGRADECIMIENTO

Agradezco a Dios, por darme la oportunidad de culminar esta etapa de mi vida.

A mis padres quienes con su ejemplo, dedicación y esfuerzo han logrado hacer de mí una persona con valores como la honestidad, el respeto, responsabilidad y tolerancia; a ellos que son mi pilar les dedico este trabajo y los frutos de mi carrera profesional.

A mis abuelos, por el apoyo que me han brindado durante todos estos años.

A mis hermanas a quienes también ofrezco este trabajo como ejemplo para que puedan cumplir con sus proyectos de vida en cualquiera de sus etapas.

A mi novia por todo el apoyo incondicional y la paciencia que me ha entregado estos años.

Finalmente agradezco a mi directora de tesis por el trabajo conjunto, enseñanzas y tiempo empleado.

A todos ustedes muchas gracias.

Guillermo

RESUMEN EJECUTIVO

El diseño e implementación de una infraestructura de servicios de red y resguardo de servidores Linux y clientes Windows junto con la integración de servicos con Active Directory de Microsoft es la base para comenzar con una infraestructura de red confiable y escalable, que permita en un futuro próximo continuar con los proyectos internos y mejorar la atención prestada a los usuarios internos y externos de la empresa.

La implementación de servicios basados en Open Source contribuirá notablemente en el aspecto económico de la empresa al permitir el ahorro en licenciamiento y adquisición de hardware, ya que se reutilizan equipos debido a la manejabilidad y bajo consumo de recursos de las aplicaciones instaladas en ellos.

La seguridad de información es primordial para el entorno empresarial, por este motivo se implementaron servicios con soporte de encriptación y transferencia segura de información que permitirán acceder de manera confiable a la información de la empresa en forma remota a través de la VPN.

El uso de información que deberá ser utilizada por clientes externos y usuarios internos de la empresa será accedida por un servidor FTP seguro, que permitirá resguardar la información durante la comunicación.

El firewall implementado junto con la aplicación de control del tráfico web y las herramientas de monitoreo implementadas, permitirá mantener un control de tráfico del canal de Internet evitando así la saturación del mismo.

Mantener un respaldo periódico de la información es de vital importancia y mediante la aplicación de políticas y la implementación de respaldos automáticos se aumentará la confiabilidad, disminuirá el peso de respaldar la información de los equipos y servidores de red manualmente, permitiendo dedicar más tiempo al monitoreo y administración de los servicios de red.

ABSTRACT

The design and implementation of network infrastructure services and protection of Linux servers and Windows clients with the integration of value added services with Microsoft's Active Directory is the basis to start with a network infrastructure reliable and scalable, allowing in the near future continue with internal projects and improve the care provided to internal and external users of the company.

The implementation of Open Source based services contribute in the economic aspect of the company, allowing savings in license and equipment purchases, because of the manageability and low resource consumption of applications installed on computers reused.

Information security is critical to the business environment, for this reason, services with support for encryption and secure transfer were implemented, that will allow access to reliable business information remotely through the VPN.

The use of information that should be used by external customers and internal users of the company will be accessed by a secure FTP server, which will protect the information during communication.

The firewall with the Web traffic control and monitoring tools implemented allow to keep the Internet traffic channel free of saturation.

Maintaining a regular backup of information is vital and through policies and implementation of automatic backups will increase reliability, decrease the weight of supporting computer information and network servers manually, allowing more time for monitoring and administration of network services, providing safety information and equipment in the enterprise.

ÍNDICE

Índice de Ilustraciones

INDICE DE ANEXOS

CAPÍTULO I

1.1. TEMA

Diseño e implementación de una infraestructura de servicios de red y resguardo de servidores Linux a través de Open Source en la empresa Proteco Coasin S.A.

1.2. INTRODUCCIÓN

Actualmente es muy difícil pensar en un mundo sin tecnología, los grandes avances tecnológicos que invaden y sofistican nuestras vidas dándonos facilidad, rapidez, seguridad y permitiéndonos un desempeño eficiente, son elementos casi indispensables para el actual ámbito laboral, por este motivo es muy importante para toda persona que este inmersa en el mundo tecnológico conocer sobre estas tendencias y nuevas tecnologías.

Gran cantidad de empresas públicas y privadas por motivo de costos, manejabilidad, estabilidad, soporte, han decidido migrar la base de sus sistemas para operar con Open Source, la fuerte inversión que varias empresas han realizado en licenciamiento en la actualidad y al comparar estas aplicaciones o desarrollos pagados con sus alternativas libres, aunque estas en ocasiones requieran una mayor dedicación y un mayor grado de investigación por los administradores de red ha logrado que el software libre tenga un agrado por varias instituciones.

Por tal motivo tener en claro la forma de implementar una infraestructura, poder dimensionar correctamente los equipos que van a formar parte de la red, conocer cómo proteger la red interna de ataques externos e internos no deseados, y proteger equipos expuestos al internet; es esencial para un administrador de red o persona encargada del manejo de redes y seguridad informática en la empresa.

Dado que el principal objetivo es satisfacer las necesidades de los usuarios y requerimientos de la empresa, se estudió la distribución de Linux correcta para utilizar como base de la infraestructura, de igual forma el correcto dimensionamiento de los equipos a utilizarse para un número de usuarios con opción a crecimiento, consiguiendo así el objetivo del estudio.

1.3. PLANTEAMIENTO DEL PROBLEMA

La falta de infraestructura y manejo adecuado de respaldos ocasionan pérdidas en tiempo y dinero a las empresas, el correcto dimensionamiento de los equipos junto con una planificación contra desastres adecuada brindará una mayor calidad y eficacia en las operaciones empresariales.

Varias empresas actualmente no disponen de una infraestructura de red segura y estable, o disponen de una pero sin un resguardo ni forma de actuación contra desastres adecuada.

Al disponer de una infraestructura lo más estable posible, la cual pueda brindar estabilidad en operaciones en una empresa se logrará una mayor productividad y desempeño de los procesos.

La falta de una base de infraestructura, mantenimiento y administración, son las causas principales por las que se desarrolla este estudio en el cual se emitirán propuestas de tipos de implementación y formas de recuperación contra desastres que ayude a lograr una infraestructura que cubra las necesidades operativas de la empresa.
Actualmente las redes se basan en la eficiencia y respuesta operativa que se puede brindar al usuario dejando a un lado el tema de seguridad, estas decisiones que a corto plazo parecen resultar efectivas para el negocio pueden sercostosas con el tiempo, por este motivo al realizar un diseño de red es necesario conocer las debilidades de los protocolos de comunicación que intervienen en el proceso de intercambio de información entre los equipos.

1.4. OBJETIVOS

1.4.1. Objetivo General

Diseñar e implementar una infraestructura de servicios de red y resguardo de servidores Linux a través de Open Source en la empresa Proteco Coasin S.A.

1.4.2. Objetivos específicos

- Realizar un análisis de situación inicial para determinar los problemas existentes en la red.

- Aprovechar los recursos existentes de acuerdo a los requerimientos en la infraestructura y cantidad de usuarios a ser administrados.

- Incrementar el ahorro de tráfico, disminuir el tiempo de respuesta y el filtrado de contenidos mediante una herramienta gratuita y de fácil implementación.

- Implementar un sistema de respaldos automáticos y restauración de equipos
- Implementar servicios básicos de red; DHCP, PROXY, DNS, WEB, FIREWALL, CORREO e integración con servicio de Directorio Activo Actual implementado en Windows server 2003.

1.5. JUSTIFICACIÓN E IMPORTANCIA

El principal motivo para realizar un modelo de diseño e implementación de una infraestructura de red es proporcionar una base de conocimientos que puedan ser aplicados en cualquier entorno laboral.

Es muy práctico mantener un modelo de infraestructura determinado el cual se puede daptar a la necesidad de la empresa con lo que se disminuye el tiempo de implementación y puesta en marcha del sistema.

El trabajo en especial servirá a profesionales que comienzan a incursionar en el mundo de la administración de redes, obtendrán una base teórica y práctica de cómo poner en marcha una infraestructura de red estable y con opción a crecimiento sin tener la necesidad de hacer cambios críticos para esto.

Mantener la confidencialidad de la información a más de la correcta capacitación a los usuarios e implementación de políticas internas de control de información, conlleva implementar servicios mediante protocolos seguros que brinden estabilidad confiabilidad y seguridad para el usuario y más aún para el administrador de la red; la seguridad de información mediante la utilización de protocolos seguros es un tema que se debe tratar como primordial en la infraestructura a implementar.

1.6. ALCANCE

El diseño e implementación se desarrollará en equipos físicos y virtuales, se elaborará un análisis de las características que estos equipos deben tener para sobrellevar la caga de usuarios requerida.

El diseño del cableado estructurado comprenderá el cambio total del cableado y un cronograma de instalaciones parciales para disminuir el impacto a los usuarios.

Se implementará servidores de Firewall, Correo, DNS, DHCP, WEB, PROXY, un equipo el cual cumplirá la función de sistema de respaldos e instalación para lo cual se desarrollarán scripts y se utilizará el método de instalación kickstart de Red Hat.

Este estudio servirá de base para cualquier infraestructura que maneje equipos con sistema operativo basado en Linux.

La implementación referirá a políticas y normativas físicas y lógicas recomendaciones y controles brindando un nivel de seguridad adecuado para las necesidades establecidas en la institución.

1.7. METODOLOGÍA

La metodología comprende 2 aspectos:

- Modalidad de campo determinando los problemas en sitio, mediante el análisis de indicencias encontrados en la red y las reportadas por los usuarios.

- Modalidad documental bibliográfica mediante la ayuda de textos y manuales referentes al tema de infraestructura, seguridad e implementación.

1.8. HERRAMIENTAS

Se utilizarán varias herramientas de Open Source las cuales ayudarán administrar de manera fácil y segura los diferentes servicios de que se implementaran en la red.

1.9. FACTIBILIDAD

La utilización de herramientas y software libre facilitó de gran manera reduciendo costos en la implementación de la infraestructura de red planteada.
La documentación es de acceso libre, los diferentes servidores pueden implementar de manera virtual dependiendo de las necesidades del negocio.

La operatividad y pruebas se pueden realizar en laboratorio simulando un entorno real, el presupuesto de implementación varía según las necesidades y usuarios en la red, en este caso se implementarán los servidores en máquinas virtuales y en equipos físicos propios de la empresa.

1.10. MARCO ADMINISTRATIVO

1.10.1. Recursos

Se utilizó equipos informáticos como servidores, laptops y equipos de escritorio, además, suministros de oficina, impresora, suministros y primordialmente acceso a internet,
La documentación e información presentada es basada en textos de libre acceso y de fuente fiable.

CAPÍTULO II

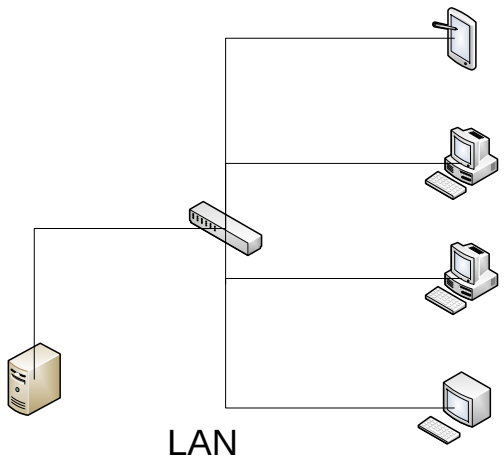
2.1. MARCO TEÓRICO

2.1.1. TIPOS DE REDES

Los diferentes tipos de redes varían por el tamaño que cubra, la cantidad de usuarios conectados, y los diferentes tipos de servicios que presten.

2.1.1.1. REDES LAN

Se denomina LAN (Local Area Network) a redes administradas por una organización única las cuales prestan servicios dentro de una organización como una empresa, un campus, un edificio; manejando velocidades relativamente altas y baja latencia dependiendo del tráfico que maneje.



Realizado por:
Guillermo León

Ilustración 2-1 - LAN (Local Area Network)

2.1.1.2. REDES MAN

Las redes MAN (Metropolitan Area Network) son redes de versión más grandes que las redes LAN, se extienden sobre áreas geográficas de tipo urbano como una ciudad. Están compuestas por conmutadores o Routers conectados entre sí con conexiones a alta velocidad. Este tipo de red permite que nodos remotos se comuniquen como si fueran parte de la misma red de área local.

En la actualidad su utilidad a caído en desuso las más comunes son las redes LAN y WAN.

2.1.1.3. REDES WAN

Una red WAN (Wide Area Network) o red de área ampliada, es utilizada para unir redes LAN separadas por extensas distancias geográficas, trabaja a velocidades menores que las redes LAN.
Están compuestas por routers o encaminadores que gestionan la comunicación y encaminan los mensajes hacia su destino. Pueden cubrir distancias desde unos 100 hasta unos 1000 km, por lo que pueden brindar servicio a un país o un continente.

La WAN más conocida es el INTERNET.

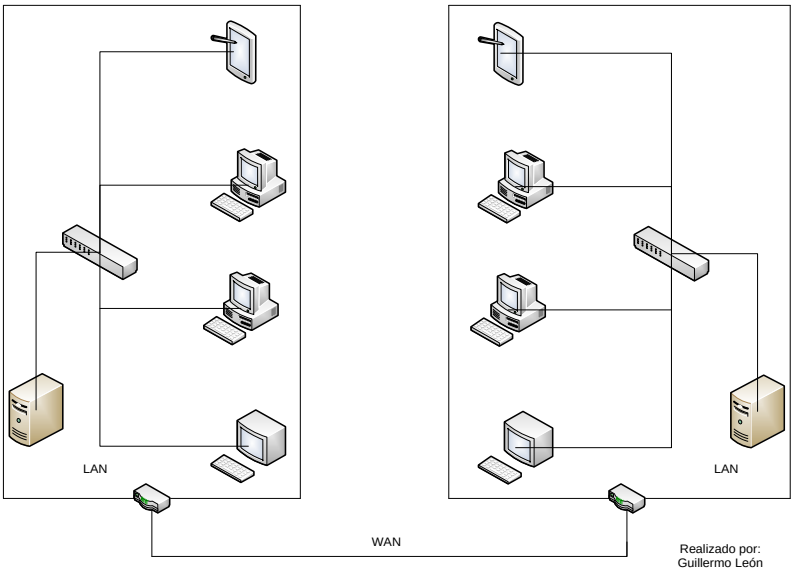


Ilustración 2-2 - WAN (Wide Area Network)

2.1.1.4. REDES WLAN

WLAN (Wireless Local Area Network), este tipo de red responden al desarrollo de los equipos portátiles, cubren lo equivalente a una LAN, con un alcance aproximado de 100 m.

Existen varios tipos de tecnologías: [1]

[1] Jeff. (16 de Octubre de 2008). *Kioskea*. Recuperado el 01 de Abril de 2012, de http://es.kioskea.net/contents/wireless/wlan.php3

WiFi (IEEE 802.11) con el respaldo de WECA (Wireless Ethernet Compatibility Alliance) ofrece una velocidad máxima de 54 Mbps en una distancia de varios cientos de metros.

HiperLAN2 (High Performance Radio LAN 2.0), estándar europeo desarrollado por ETSI (European Telecommunications Standards Institute). HiperLAN 2 permite a los usuarios alcanzar una velocidad máxima de 54 Mbps en un área aproximada de 100 metros, y transmite dentro del rango de frecuencias de 5150 y 5300 MHz.

2.1.1.5. REDES VLAN

VLAN (Virtual LAN), una red local que se crea con grupos de usuarios que tengan requerimientos similares o que compartan un conjunto de recursos, como impresoras y servidores, pero que no necesariamente están ubicados de manera física en un mismo lugar.

Los estándares más utilizados para este tipo de redes son ISL (Inter Switch Link) y 802.1Q, pero usan Internet para transportar datos de manera privada. [2]

2.1.2. SERVICIOS DE RED

2.1.2.1. CORREO ELECTRÓNICO

El correo electrónico también conocido como e-mail, es un recurso tecnológico que permite comunicarse desde cualquier parte del mundo a través de Internet.

El nombre correo electrónico proviene de la analogía con el correo postal: ambos sirven para enviar y recibir mensajes, y se utilizan "buzones" intermedios (servidores), en donde los mensajes se guardan temporalmente antes de dirigirse a su destino, y antes de que el destinatario los revise.
Fue creado en 1971 por Ray Tomlinson, un ingeniero de Bolt Beranek and Newman, la empresa encargada de poner en marcha Arpanet.

[2] Fortunecity. (s.f.). *Tipos de Redes*. Recuperado el 15 de Octubre de 2011, de http://members.fortunecity.es/elcastillodelainformatica/tiposderedes.htm

Tomlinson no consideró realizar un invento importante. A pesar de que no existía la manera de enviar mensajes de manera unipersonal y a otra computadora de una red. Su gran difusión promueve servicios para chequear una cuenta POP desde cualquier navegador.

El texto del primer mensaje contenía "QWERTYUIOP" (teclas pulsadas al azar en el teclado por razones de pruebas) según su inventor y fue enviado a través de un programa llamado SNDMSG que él escribió. El invento se estaba terminando en 1971 cuando Tomlinson, un ingeniero de la firma Bolt Beranek y Newman, contratada por el gobierno de los Estados Unidos para construir la red Arpanet (la precursora de Internet), tuvo la idea de crear un sistema para enviar y recibir mensajes por la red.

Tomlinson había escrito un programa para que los desarrolladores de la Arpanet se dejaran mensajes en las computadoras que compartían (15 en toda la red nacional).
Tomlinson eligió la arroba, que en inglés se lee "*at* (en tal lugar)", para especificar el destinatario del mensaje. Acto seguido, se envió un mensaje a sí mismo y dio inicio a la era del e-mail.

El uso de cuentas POP requiere de un software para conectarse a un servidor, subir y descargar mensajes. Los principales programas en el mercado son Eudora, Outlook o Thunderbird.

Principales programas para leer y organizar correo: [3]

- Windows Live Mail: Windows.
- Evolution: GNU/Linux.
- Mail: Mac OS X e iOS.
- Outlook Express: Windows.
- Thunderbird: Windows, GNU/Linux, Mac OS X.

Principales programas servidores de correo:[3]

- Mercury Mail Server: Windows, Unix, GNU/Linux.
- Microsoft Exchange Server: Windows.
- MailEnable: Windows.
- MDaemon: Windows.
- Exim: Unix.
- Sendmail: Unix.
- Qmail: Unix.
- Postfix: Unix.

[3] Wikipedia. (28 de Marzo de 2012). Recuperado el 15 de Octubre de 2011, de Wikipedia: http://es.wikipedia.org/wiki/Correo_electr%C3%B3nico

- Zimbra: Unix, Windows.
- Lotus Domino: GNU/Linux, OS400, Windows.

2.1.2.2. WEB

Software utilizado para intercambiar datos entre aplicaciones en redes mediante estándares y protocolos. La interoperabilidad depende de la adopción de estándares abiertos consiguiendo que desarrollos de software en diferentes lenguajes que corran en diferentes plataformas puedan intercambiar información.
Un Servidor web carga contenido estático y dinámico mediante la red al navegador de un usuario.

2.1.2.2.1. Ventajas de los servicios web

Los servidores web aumentan la interoperabilidad multiplataforma y geográfica, fomentando el uso de protocolos y estándares que se basan en texto, por lo cual es más fácil conocer su funcionamiento y comprender su contenido.

2.1.2.2.2. Servidor Web Apache

Servidor web de código abierto para sistemas operativos Unix, Linux, Windows y Macintosh, "presenta características altamente configurables, bases de datos de autenticación y negociado de contenido"

"La licencia de software bajo la cual el software de la Fundación Apache es distribuido es una parte distintiva de la historia de Apache HTTP Server y de la comunidad de código abierto. La Licencia Apache permite la distribución de derivados de código abierto y cerrado a partir de su código fuente original."[4]

2.1.2.3. PROXY

Un servidor proxy trabaja en la capa de aplicación de del Modelo OSI, permite o niega el acceso a una aplicación determinada entre dos redes. Los servidores proxy autorizan o niegan las peticiones que realizan los clientes proxy, para posterior enviarlas a los servidores reales y poder presentar la información al solicitante.

[4] Wikipedia. (21 de Marzo de 2012). *Servidor HTTP Apache*. Recuperado el 15 de Octubre de 2011, de http://es.wikipedia.org/wiki/Servidor_HTTP_Apache

Los servidores proxy-cache se han convertido en una herramienta indispensable en casi todo entorno donde es necesario distribuir una conexión de internet para navegación y acelerar al mismo tiempo la velocidad de navegación de los clientes, así como para implementar el filtrado de acceso por varios criterios como: tiempos (horarios), URLs, direcciones, dominios, entre otras.

2.1.2.3.1. Tipos de Servidores Proxy

- **Servidor proxy HTTP**

Este servidor utiliza el puerto 80 de HTTP pero también suele ser usado en los puertos 3128, 8080 o el 8085.

- **Servidor proxy HTTPS**

Funciona bajo tecnologías de cifrado como SSL/TLS[5] que proporcionan mayor seguridad y anonimato. El puerto utilizado varía, aunque suele ser 443/HTTP.

- **Servicio Proxy o Proxy Web**

Se basa en el del Proxy HTTP y HTTPs, la petición se realiza mediante una Aplicación Web embebida en un Servidor HTTP, es decir es una página web que permite estos servicios.

- **Proxy Caché**

Servidor proxy que almacena en su cache contenido web solicitado por el usuario para acelerar su presentación en futuras peticiones a este recurso.

2.1.2.3.2. Ventajas

- Control: el servidor proxy permite mantener un control de los sitios visitados y obtener estadísticas de navegación de los clientes.

[5] **SSL:** Secure Sockets Layer o protocolo de capa de conexión segura
TLS Transport Layer Security o seguridad de la capa de transporte

- Ahorro: el equipo destinado a cumplir las funciones de proxy será el intermediario y realizará el trabajo real al atender las solicitudes de los clientes.

- Velocidad: las peticiones de varios clientes que desean acceder al mismo sitio web pueden ser atendidas por el proxy de una manera más eficiente si el proxy trabaja como caché.

- Filtrado: mediante el control de navegación y estadísticas se puede determinar y controlar qué sitio web debe ser restringido para el uso de clientes.

- Anonimato: el proxy es el destinado a hacer todas las peticiones web con lo que se logra guardar la identificación de cada solicitante.

1.1.2.3.3 Desventajas

- Abuso: el servidor proxy está destinado a atender las solicitudes de los clientes, puede pasar que el servidor atienda solicitudes que no deba. Por este motivo, es importante determinar quién accede o no al servidor proxy.

- Carga: atender las solicitudes de gran cantidad de usuarios aumenta el trabajo a realizar por el servidor proxy.

- Intromisión: el servidor proxy es un intermediario entre el sitio de destino y el sitio de origen, por lo cual los datos solicitados pueden ser consultados.

- Incoherencia: en servidores proxy antiguos ocurría que la información presentada no era la correcta, actualmente esto no sucede, los servidores se comunican con los sitios y consultan la información actualizada.

- Irregularidad: en varios escenarios como en TCP/IP, donde se requiere comunicación directa entre emisor y receptor, se presenta como un inconveniente que el servidor proxy represente a varios usuarios.

2.1.2.4. DNS

Domain Name System o Sistema de Nombres de Dominio fue creado para traducir las direcciones numéricas en nombres sencillos y fáciles de recordar.
Por ejemplo es más sencillo recordar www.google.com que 74.125.229.112.
Si Google decide cambiar su dirección numérica sería transparente para el usuario ya que el nombre de dominio seguiría siendo www.google.com.

El Sistema de nombres de dominio (DNS) se creó para que el nombre del dominio busque soluciones para estas redes. DNS utiliza un conjunto distribuido de servidores para resolver los nombres asociados con estas direcciones numéricas.

2.1.2.4.1 Componentes

Para la operación práctica del sistema DNS se utilizan tres componentes principales:

- Los Clientes DNS: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor, como por ejemplo: ¿Qué dirección IP corresponde a www.google.com?

- Los Servidores DNS: Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.

- Zonas de autoridad, porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad

2.1.2.4.2. Tipos de registros DNS

- A = Address – (Dirección) Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.

- AAAA = Address – (Dirección) Este registro se usa en IPv6 para traducir nombres de hosts a direcciones IPv6.

- CNAME = Canonical Name – (Nombre Canónico) Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio. Es usado cuando se están corriendo múltiples servicios (como FTP y servidor web) en un servidor con una sola dirección IP. Cada servicio tiene su propia entrada de DNS (como ftp.ejemplo.com. y www.ejemplo.com.). Esto también es usado cuando se corre múltiples servidores HTTP, con diferentes nombres sobre el mismo host.

- NS = Name Server – (Servidor de Nombres) Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información

de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.

- MX (registro) = Mail Exchange – (Registro de Intercambio de Correo) Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio.

- PTR = Pointer – (Indicador) También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo direcciones IPs en nombres de dominio.

- SOA = Start of authority – (Autoridad de la zona) Proporciona información sobre el servidor DNS primario de la zona.

- HINFO = Host INFOrmation – (Información del sistema informático) Descripción del host, permite que la gente conozca el tipo de máquina y sistema operativo al que corresponde un dominio.

- TXT = TeXT - (Información textual) Permite a los dominios identificarse de modos arbitrarios.

- LOC = LOCalización - Permite indicar las coordenadas del dominio.

- SRV = SeRVicios - Permite indicar los servicios que ofrece el dominio.

- SPF = Sender Policy Framework - Ayuda a combatir el Spam. En este registro se especifica cual o cuales hosts están autorizados a enviar correo desde el dominio dado. El servidor que recibe, consulta el SPF para comparar la IP desde la cual le llega, con los datos de este registro.

2.1.2.5. DHCP

Dynamic Host configuration protocol o protocolo de configuración dinámica de host, permite a una máquina en la red obtener los diferentes parámetros de configuración de como son la dirección IP, Máscara de su red, Gateway, DNS, WINS, etc.

La dirección asignada al equipo que se conecta a la red proviene de un rango configurado de direcciones denominado pool, la dirección asignada es alquilada por un periodo establecido de tiempo.

Es recomendable el uso de DHCP en entornos de red grandes, lo cual facilitaría el manejo y administración eficiente del administrador de red, DHCP es muy útil en entornos abiertos como por ejemplo un centro comercial, lo cual permite a varias personas conectarse a la red sin la intervención de un administrador.
DHCP puede representar un riesgo a la seguridad porque cualquier dispositivo conectado a la red puede recibir una dirección. Este riesgo hace de la seguridad física un factor importante a la hora de determinar si se utiliza direccionamiento manual o dinámico.

2.1.2.5.1 Modos en DHCP

Existen 3 modos en DHCP para poder asignar direcciones IP a otros equipos:

Asignación manual: El administrador configura manualmente las direcciones IP del cliente en el servidor DCHP. Cuando la estación de trabajo del cliente pide una dirección IP, el servidor mira la dirección MAC y procede a asignar la que configuró el administrador.

Asignación automática: Al cliente DHCP se le asigna una dirección IP cuando contacta por primera vez con el DHCP Server. En este método la IP es asignada de forma aleatoria y no es configurada de antemano.

Asignación dinámica: El servidor DHCP asigna una dirección IP a un cliente de forma temporal. Digamos que es entregada al client Server que hace la petición por un espacio de tiempo. Cuando este tiempo acaba, la IP es revocada y la estación de trabajo ya no puede funcionar en la red hasta que no pida otra.

2.1.2.5.2 Proceso de obtención de parámetros de red mediante DHCP

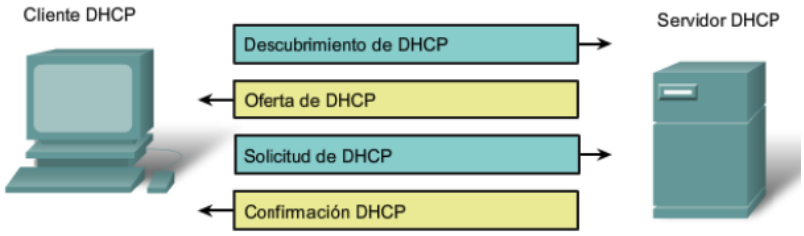


Ilustración 2-3 - DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)[6]

- **DHCPDISCOVER**.- ubica a los servidores de red disponibles en la red.

[6] Cisco. (s.f.). CCNA-EXPLORATION1. En Cisco, CCNA-EXPLORATION1

- **DHCPOFFER**.- respuesta del servidor a un paquete DHCPDISCOVER, contiene los parámetros iniciales.

- **DHCPREQUEST**.- solicitudes varias del cliente, por ejemplo, para extender su concesión.

- **DHCPACK**.- respuesta del servidor que contiene los parámetros de configuración y la dirección IP del cliente.

- **DHCPNAK**.- respuesta del servidor para indicarle al cliente que su concesión ha vencido o si el cliente anuncia una configuración de red errónea.

- **DHCPDECLINE**.- el cliente anuncia al servidor que la dirección ya está en uso.

- **DHCPRELEASE**.- el cliente libera su dirección IP.

2.1.2.6. FTP

File Transfer Protocol o protocolo de transferencia de archivos, está basado en una arquitectura cliente servidor utiliza el puerto 20 y 21 para la transferencia de archivos entre sistemas conectados a una red TCP.

Para una conexión exitosa se necesitan 2 conexiones una de control (comandos y respuestas) y otra para la transferencia de archivos.

El cliente establece la primera conexión con el servidor en TCP puerto 21. Esta conexión se utiliza para controlar el tráfico, que consiste en comandos del cliente y respuestas del servidor.
El cliente establece la segunda conexión con el servidor en TCP puerto 20. Esta conexión es para la transferencia real de archivos y se crea cada vez que se transfiere un archivo, la transferencia de archivos puede producirse en ambas direcciones. El cliente puede descargar un archivo desde el servidor o el cliente puede cargar un archivo en el servidor.

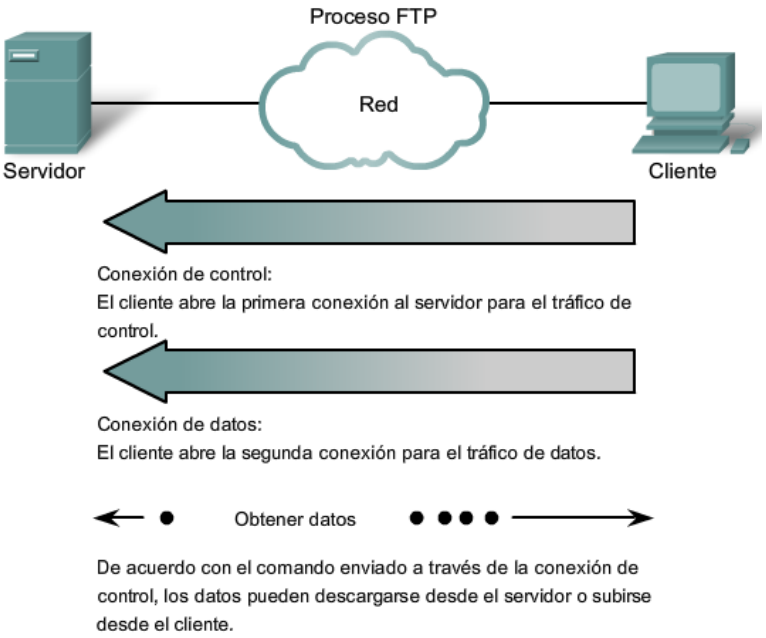


Ilustración 2-4 - FTP (File Transfer Protocol)

2.1.3. Seguridad de la información

Es la protección de la información de un rango amplio de amenazas para asegurar la continuidad del negocio, minimizar el riesgo comercial, y maximizar el retorno de las inversiones y oportunidades comerciales.

2.1.3.1 Propiedades de seguridad

2.1.3.1.1 Confidencialidad

Prevenir la divulgación de la información a personas o sistemas no autorizados.

2.1.3.1.2 Disponibilidad

La información debe estar a disposición de las personas o sistemas que la necesiten.

2.1.3.1.3 Integridad

Garantizar que la información no fue alterada.

2.1.3.1.4 No-retractación

No permitir que ni el emisor ni el receptor nieguen haber trasmitido un mensaje.

2.1.3.1.5 Responsabilidad ante terceros

Información emitida sea controlada y confiable.

2.1.3.2 Áreas de seguridad

2.1.3.2.1 Seguridad de perímetro

Protección frente ataques del exterior generalmente basada en Cortafuegos.

2.1.3.2.2 Seguridad en el canal

Proteger los datos frente a escuchas mediante Criptografía

2.1.3.2.3 Seguridad de acceso.

Se contemplan tres aspectos:

- Identificación del usuario
- Autorización del acceso y
- Auditoría de operaciones realizadas por el usuario.

2.1.3.2.4 Seguridad interna

Se debe tomar en cuenta:

- Provocado por empleados de la empresa, o porque las barreras externas son débiles (el enemigo está dentro)
- Segmentación de red mediante el uso de conmutadores (switches)
- Monitoreo de red

2.1.3.3 Tipos de ataques

2.1.3.3.1 Ataques pasivos

El objetivo de un ataque pasivo es obtener la información mediante la escucha o monitoreo de una trasmisión, estos ataques son difíciles de detectar, para evitar estos ataques es recomendable hacer énfasis en la prevención antes que en la detección.

2.1.3.3.2 Ataques activos

En este tipo de ataque se tiene la disposición activa del intruso ya sea para modificar un flujo de datos, crear datos, o interrumpir comunicaciones, este tipo de ataques son difíciles de evitar, debemos hacer énfasis en la detección la cual contribuirá de gran forma a la prevención.

Los ataques activos son:

Enmascaramiento.- Suplantación de un ente autorizado para acceder a información o recursos

Modificación.- Destrucción y creación no autorizada de datos o recursos

Interrupción.- Impedir a entes autorizados su acceso a la información o recursos a los que tienen derecho de acceso.

2.1.3.4 Servicios

2.1.3.4.1 Confidencialidad

Protección de los datos frente a intrusos

Variantes:

- Orientada a conexión
- No orientada a Conexión
- Selectiva
- Aplicada al análisis de tráfico

2.1.3.5 Medidas

Se pueden constituir como buenas prácticas:

- Acuerdos de confidencialidad
- Selección rigurosa
- Inclusión de la seguridad como responsabilidad contractual
- El personal debe conocer los riesgos y sus consecuencias.
- Los responsables del sistema deben saber que hacer y a quién informar, en todo momento, en caso de incidente.
- Seguimiento/control del personal

2.1.3.6 Defensa

2.1.3.6.1 Firewall

Un firewall puede ser un dispositivo o software dedicado al filtrado de tráfico, es decir, establece las reglas de filtrado para las conexiones. Para implementar un firewall entre redes es necesario tener por lo menos 2 interfaces de red.

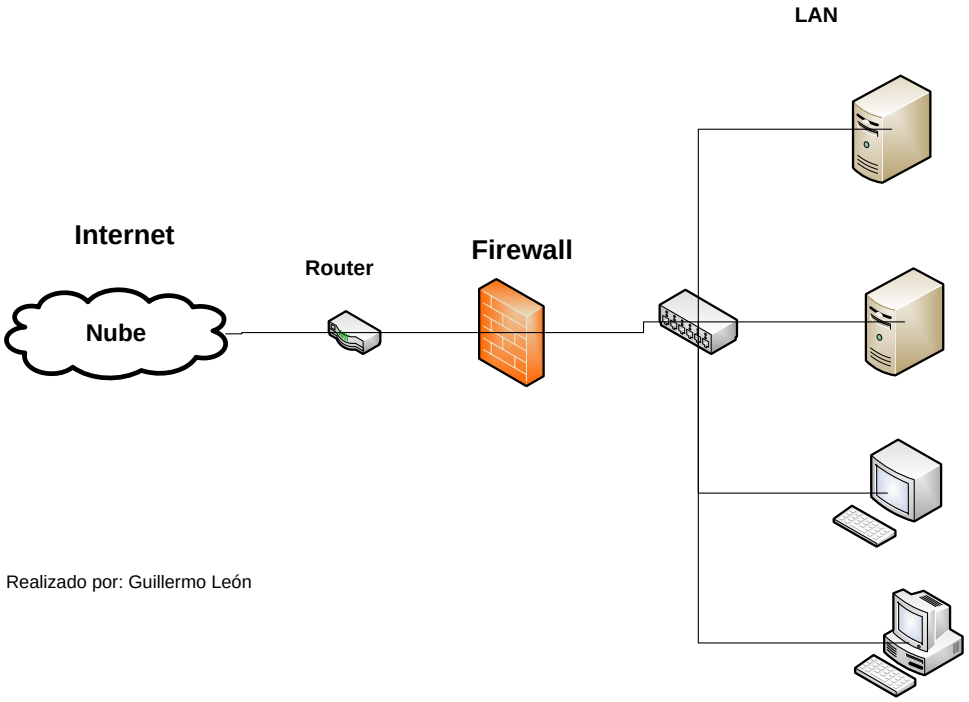


Ilustración 2-5 – Firewall

2.1.3.6.1.1 Tipos de Firewall

2.1.3.6.1.1.1 Nivel de aplicación de pasarela

Utilizados para aplicaciones específicas como pueden ser servidores FTP y Telnet. Tipo de firewall muy eficaz pero puede degradar el rendimiento de los servicios que se prestan.

2.1.3.6.1.1.2 Circuito a nivel de pasarela

Este tipo de circuito permite establecer sesión desde zonas de mayor a menor seguridad, cuando las conexiones TCP o UDP son establecidas se tiene un intercambio libre de paquetes entre las estaciones.

2.1.3.6.1.1.3 Cortafuegos de capa de red o de filtrado de paquetes

Trabaja en capa 3 de Modelo OSI, permiten realizar filtros según los distintos campos de los paquetes IP como el puerto de origen y el puerto de destino, también al nivel de enlace de datos como la dirección MAC

2.1.3.6.1.1.4 Cortafuegos de capa de aplicación

Trabaja en capa de aplicación, nivel 7 del modelo OSI, los filtros se adaptan a las características de este nivel. Al filtrar el tráfico HTTP, se pueden realizar filtrados según el URL al que se está intentando acceder.

Un cortafuego de nivel 7 de tráfico HTTP suele denominarse proxy, oculta de manera eficaz las direcciones de red verdaderas y permite que los computadores de una organización accedan a Internet de una forma controlada.

2.1.3.6.1.1.5 Cortafuegos personales

Cortafuegos a nivel personal, por lo general es software instalado en la PC del usuario, se encarga de bloquear conexiones salientes y entrantes no deseadas.

2.1.3.6.1.2 Políticas de firewall

Hay dos políticas básicas en la configuración de un firewall que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

Política restrictiva: Se deniega todo el tráfico excepto lo explícitamente requerido. El cortafuego obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Opción utilizada por empresas y organismos gubernamentales.

Política permisiva: Todo el tráfico es permitido excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Es usualmente utilizada por universidades, centros de investigación y servicios públicos de acceso a internet.

La política restrictiva es la más segura, ya que es más difícil permitir por error, tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

2.1.3.6.2 VPN

Virtual Private Network o Red Privada Virtual es una red privada que utiliza una infraestructura pública de transporte y lleva la información a los sitios remotos mediante un proceso de encapsulación y encriptación de los paquetes de datos.

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para la trasferencia de datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

CAPÍTULO III

3.1. IMPLEMENTACIÓN

3.1.1 Sistema Operativo

La distribución de Linux elegida para la instalación de los servidores de red es CENTOS[7], en su versión actual 5, compatible para infraestructuras i386 y x86_64

CentOS es una distribución Linux de clase empresarial derivada de fuentes libremente ofrecidos al público por un prominente proveedor de Linux de América del Norte, muy utilizada en el entorno de administración de redes, por diversos motivos como:

- Estabilidad
- Seguridad
- Actualizaciones durante 7 años
- Soporte para varios programas comerciales que soporta Enterprise Linux.
- Soporte de varios repositorios en los cuales encontramos más de 10 mil paquetes
- Manejo de paquetería mediante RPMs.[8]

3.1.1.1 Requerimientos

3.1.1.1.1 Requerimientos de instalación

Tipo de instalación	Memoria RAM mínima	Memoria RAM recomendada
Instalación modo texto	384 Mb	1 GB
Instalación modo Gráfico	652 Mb	1 GB

3.1.1.1.2 Memoria RAM

Procesador	Memoria RAM mínima	Memoria RAM máxima	Memoria RAM recomendad
x86	512 GB	16 GB	1 GB
itanium	1GB	N/A	1GB
x86_64	N/A	2TB/64TB	N/A

[7] Centos.- Community Enterprise Operative System
[8] RPM.- Originalmente denominado Red Hat Package Manager, actualmente es un acrónimo recursivo RPM Package Manager o manejador de paquetes RPM.

Procesador	Memoria RAM mínima	Memoria RAM máxima	Memoria RAM recomendad
Power	2GB	2TB	2 GB
System z	1GB	3TB	5 GB

3.1.1.1.3 Procesador

Procesador	Número de procesadores lógicos permitidos
x86	32
itanium	N/A
x86_64	160/4096
Power	128
System z	80

3.1.1.1.4 Disco duro

Capacidad de almacenamiento y sistema de archivos soportado	
Maximum filesize (Ext3)	2TB
Maximum filesystem size (Ext3)	16TB
Maximum filesize (Ext4)	16TB
Maximum filesystem size (Ext4)	16TB

3.1.2 Distribución de servicios en equipos de red

La implementación de los servicios de red se realizará en equipos físicos en la siguiente forma:

3.1.2.1 FIREWALL, SQUID, VPN y FTP

Los servicios mencionados se instalarán en un equipo independiente con 2 interfaces de red

Las características del equipo a utilizarse son:

SERVIDOR FIREWALL, DNS, VPN y FTP				
Equipo	**Placa**	**Procesador**	**Memoria**	**Disco**
Dell Power edge 1850	Intel	Intel(R) Xeon(TM) CPU 3.0 GHz	512 GB	40 GB

3.1.2.1.1 Direccionamiento

CONFIGURACIÓN IP FIREWALL, DNS, VPN					
Equipo	**Interface**	**IP**	**MÁSCARA**	**GW**	**DNS**
FIREWALL, SQUID, VPN, FTP	ETH0	192.168.3.1	255.255.255.0		
	ETH1	190.108.69.190	255.255.255.248	190.168.69.185	190.90.138.3 200.7.206.2

3.1.2.2 DNS, DHCP y WEB

Estos servicios se instalarán en un servidor DELL POWER EDGE 1750, cuyas características son:

3.1.2.2.1 Equipo a utilizar

SERVIDOR DNS, DHCP, WEB				
Equipo	**Placa**	**Procesador**	**Memoria**	**Disco**
Dell Power edge 1850	Intel	Intel(R) Pentium(R) 4 CPU 3.00GHz	1 GB	100 GB

3.1.2.2.2 Direccionamiento

CONFIGURACIÓN IP DNS, DHCP, WEB					
Equipo	**Interface**	**IP**	**MÁSCARA**	**GW**	**DNS**
DNS, DHCP	ETH0	192.168.3.218	255.255.255.0	192.168.3.1	192.168.3.1

3.1.2.3 Servidor de Correo Electrónico

Recomendablemente este servicio debe instalarse en un equipo independiente. Para la implementación se utilizará un equipo con las siguientes características:

SERVIDOR CORREO ELECTRÓNICO				
Equipo	**Placa**	**Procesador**	**Memoria**	**Disco**
HP	Intel	Intel(R) Xeon(TM) CPU 2.40 GHz	512 MB	40 GB

3.1.2.3.1 Direccionamiento

CONFIGURACIÓN IP CORREO ELECTRÓNICO					
Equipo	**Interface**	**IP**	**MÁSCARA**	**GW**	**DNS**
Correo Eelctronico	ETH0	192.168.3.219	255.255.255.0	192.168.3.1	192.168.3.1

3.1.2.4 Respaldos y SAMBA

Para la instalación de estos servicios se utilizará un equipo con las siguientes características:

SERVIDOR DE RESPALDOS Y SAMBA				
Equipo	**Placa**	**Procesador**	**Memoria**	**Disco**
CLON	Intel	Intel(R) Pentium(R) 4 CPU 2,4 GHZ	1 GB	500 GB

3.1.2.4.1 Direccionamiento

CONFIGURACIÓN IP SERVIDOR DE RESPALDOS Y SAMBA					
Equipo	**Interface**	**IP**	**MÁSCARA**	**GW**	**DNS**
DNS, DHCP	ETH0	192.168.3.217	255.255.255.0	192.168.3.1	192.168.3.1

3.2 Diagrama de red

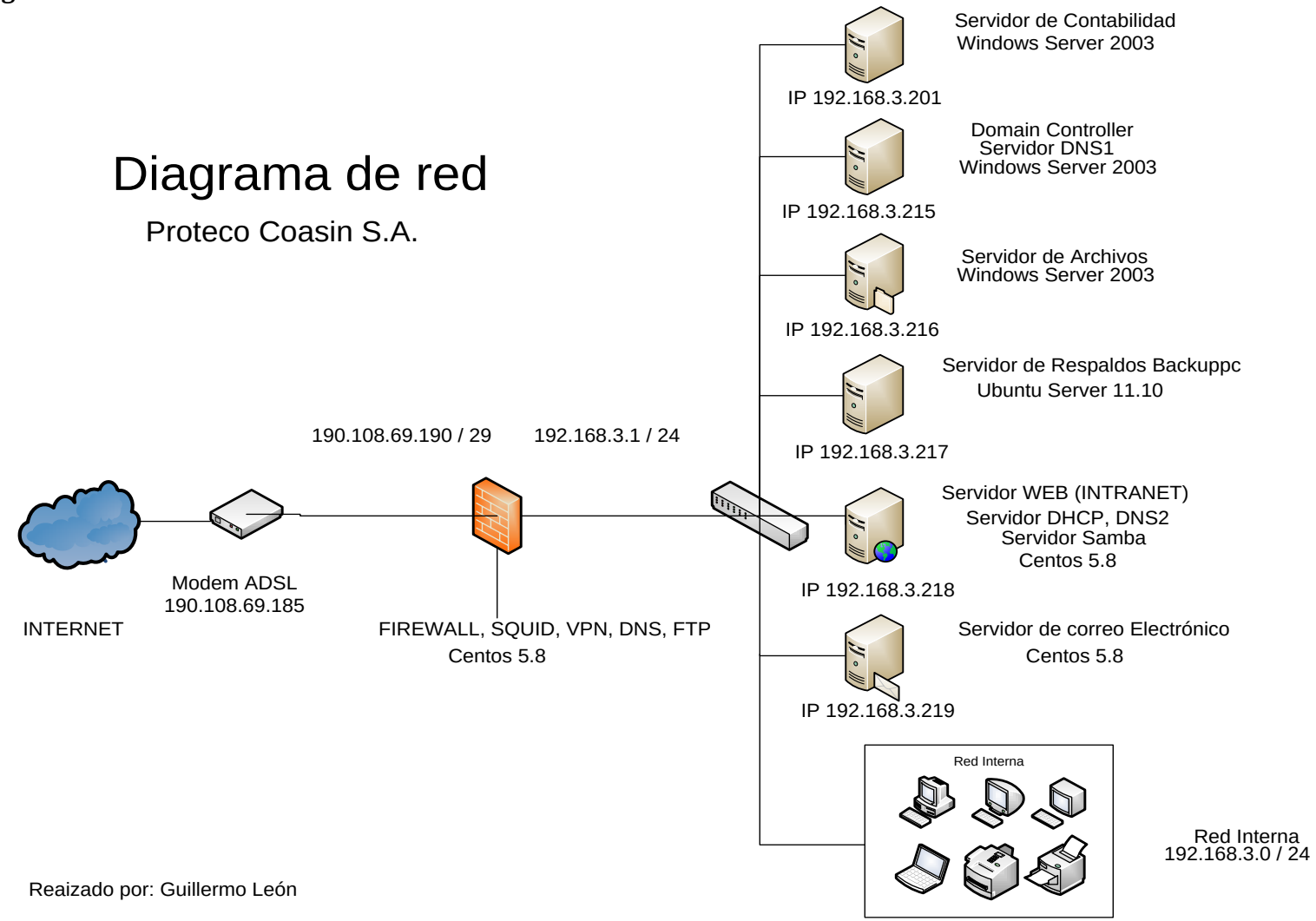


Ilustración 3-1- Diagrama de red Proteco Coasin S.A

3.3 Implementación de servicios de red

3.3.1 Firewall

3.3.1.1 Iptables

Es un software distribuido bajo licencia GNU GPLv2[9], viene incluido en el kernel de Linux desde su versión 2.4.

Sucesor del antiguo firewall/NAT de Linux Ipchains, que permite a los administradores inspeccionar y restringir conexiones a los servicios disponibles en una red interna utilizando un método llamado el seguimiento de conexiones.

3.3.1.1.1 Mejoras de Iptables con respecto a Ipchains

- Mejor integración del kernel de Linux con la capacidad de cargar módulos específicos de iptables diseñados para mejorar la velocidad y confiabilidad.

- Inspección completa de paquetes por su estado, el firewall mantiene el rastro de cada conexión que pasa y en ciertos casos podrá hasta ver el contenido de flujos de datos en un intento de anticipar la siguiente acción de ciertos protocolos. Esta es una característica importante en el soporte de DNS y FTP activos, así como de otros muchos servicios de red.

- Filtrado de paquetes basado en dirección MAC y los valores de las banderas en el encabezado TCP. Esto es de mucha ayuda al prevenir ataques usando paquetes malformados y en la restricción de acceso de servidores locales a otras redes sin importar la dirección IP.

- Autenticación y acceso al sistema que provee la opción de ajustar el nivel de detalle de reportes.

- Mejor traducción de direcciones de red (NAT).

- Soporte para integración transparente con programas de proxy Web como Squid.

[9]GNU GPLv2, publicada en junio de 1991, pretende garantizar la libertad de compartir y modificar software libre, para asegurar que el software es libre para todos sus usuarios

- Característica de límite por rango que ayuda al iptables a bloquear algunos tipos de ataque de denegación de servicio (DoS).

3.3.1.1.2 Procesamiento de Paquetes en iptables

Iptables inspecciona todos los paquetes a través de tablas, las cuales se dedican a un tipo particular de actividad de paquete y es controlada por una cadena asociada de transformación y filtrado de paquetes.

3.3.1.1.3 Tablas existentes

3.3.1.1.3.1 Mangle

Se encarga de la alteración de los bits de calidad de servicio (QoS[10]) en el encabezado TCP.

3.3.1.1.3.2 Filer queue

Se encarga del filtrado de paquetes. Las cadenas incluidas en las cuales se pueden poner las reglas de políticas del Hardware son:

- Forward chain: Filtra los paquetes hacia servidores protegidos por el firewall.
- Input chain: Filtra los paquetes destinados al firewall.
- Output chain: Filtra los paquetes originados en el firewall

3.3.1.1.3.3 Nat queue

Se encarga de la traducción de direcciones de red, sus cadenas incluidas son:

Pre-routing chain: Los paquetes NAT cuando la dirección de destino del paquete debe ser cambiada.

Post-routing chain: Los paquetes NAT cuando la dirección de origen del paquete debe ser cambiada.

[10] QOS.- Quality of service o calidad de servicio

3.3.1.1.4 Instalación y configuración de Iptables.

Iptables viene instalado por defecto en Centos 5, para conocer la versión instalada y comprobar su existencia se debe utilizar el siguiente comando:

rpm –qa iptables

De no encontrarse instalado se lo puede instalar mediante yum:

yum -y install iptables

Para la configuración del firewall se utilizará un script nombrado firewall-proteco, en el cual se determinarán todas las reglas y permitirá iniciar, detener y reiniciar el servicio de firewall muy fácilmente.

3.3.1.1.5 Creación y configuración del Script

- Para la creación del script se utilizó el editor de texto vi.

  vi /etc/init.d/firewall-proteco

- El script debe tener permisos de ejecución

  chmod +x /etc/init.d/firewall-proteco

- Se debe agregar el script como servicio

  chkconfig –add firewall-proteco

- Configurar el arranque por defecto del servicio al arranque del sistema

  chkconfig firewall-proteco on

- Iniciar el servicio

  service firewall-proteco start

- Posterior a realizar un cambio en el script se debe reiniciar el servicio

  service firewall-proteco restart

3.3.1.1.6 Contenido del Script

El script completo de configuración del Firewall se encuentra en el ANEXO 1

3.3.1.1.6.1 Información de redes

Interface Interna
INTERNALIF="eth1"

Red interna
INTERNALNET="192.168.2.0/24"

Broadcast de la red
INTERNALBCAST="192.168.2.255"

Interface Externa
EXTERNALIF="eth0"

IP Pública del servidor
MYADDR="190.108.69.190"

3.3.1.1.6.2 Llamar al script con los parámetros start/stop/restart

```
REDHAT="YES"
if [ X"$REDHAT" = X"YES" ]; then
        . /etc/rc.d/init.d/functions
        case "$1" in
                stop)
                        action "Shutting down firewall:" echo
                        $IPTABLES -F
                        $IPTABLES -P FORWARD DROP
                        exit 0
                        ;;
```

```
        status)
                echo "The status command is not supported for iptables"
                exit 0
                ;;
        restart|reload)
                $0 stop
                exec $0 start
                ;;
        start)
                action "Starting Firewall:" echo
                ;;
        *)
                echo "Usage: firewall (start|stop|restart)"
                exit 1
    esac
fi
```

- Vaciar reglas existentes

  Eliminación de reglas existentes para paquetes provenientes del exterior
  $IPTABLES -F INPUT
  Eliminación de reglas existentes para paquetes de la red interna hacia el exterior
  $IPTABLES -F OUTPUT
  Eliminación de reglas existentes para Forwarding/enmascaramiento
  $IPTABLES -F FORWARD
  Eliminación de reglas existentes para Tabla de NAT
  $IPTABLES -t nat -F

- No responder a pings

  echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all

- No responder a ping de Bradcast

  echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

- Habilitar el forwarding

  echo 1 >/proc/sys/net/ipv4/ip_forward

- Anular las marcas de tiempo (timestamps) para evitar que se averigüe el tiempo de actividad del sistema (uptime)

  echo 0 > /proc/sys/net/ipv4/tcp_timestamps

- Activar defensa del ataque inundación de SYN

  echo 1 > /proc/sys/net/ipv4/tcp_syncookies

- Habilitar protección contra mensajes inválidos que son guardados en log por el kernel.

  Con esta línea indicamos al kernel no guardar estos logs protegiéndolo contra un posible filesystem lleno o contra un posible ataque de negación de servicio.

  echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

- Definir rango de puertos locales que van a ser utilizados en las aplicaciones

  echo "32768 61000" >/proc/sys/net/ipv4/ip_local_port_range
- Reducir los timeouts para reducir la posibilidad de ataques de negación de servicio.

  echo 30 > /proc/sys/net/ipv4/tcp_fin_timeout

- Tiempo para finalizar una conexión no activa

  echo 1800 > /proc/sys/net/ipv4/tcp_keepalive_time
  echo 1 > /proc/sys/net/ipv4/tcp_window_scaling
  echo 0 > /proc/sys/net/ipv4/tcp_sack

- Máximo de conexiones SYN

  echo 1280 > /proc/sys/net/ipv4/tcp_max_syn_backlog

- Bloqueo de paquetes con combinaciones inválidas

```
$IPTABLES -A INPUT -m state --state INVALID -j DROP
$IPTABLES -A FORWARD -m state --state INVALID -j DROP
```

- Aceptar todas las conexiones en la interface local

```
$IPTABLES -A INPUT -i lo -j ACCEPT
```

- No permitir conexiones desde el exterior a la interface local

```
$IPTABLES -A INPUT -d 127.0.0.0/8 -j REJECT
```

- Bloquear conexiones a servidores SMTP remotos

```
$IPTABLES -A FORWARD -s $INTERNALNET -p tcp --dport 25 -j DROP
```

- No permitir navegación a una MAC específica.

```
$IPTABLES -A FORWARD -i $INTERNALIF -m mac --mac-source 00:14:51:27:c5:64 -j DROP
```

- Permitir el tráfico ilimitado de la red interna.

```
$IPTABLES -A INPUT -i $INTERNALIF -s $INTERNALNET -j ACCEPT
```

- Bloquear todo tráfico de la red externa que dice ser de la red interna

```
$IPTABLES -A INPUT -i $EXTERNALIF -s $INTERNALNET -j REJECT
```

- No reenviar el tráfico SMB

```
$IPTABLES -A FORWARD -o $EXTERNALIF -p tcp --dport 137 -j REJECT
$IPTABLES -A FORWARD -o $EXTERNALIF -p tcp --dport 138 -j REJECT
$IPTABLES -A FORWARD -o $EXTERNALIF -p tcp --dport 139 -j REJECT
$IPTABLES -A FORWARD -o $EXTERNALIF -p udp --dport 137 -j REJECT
```

```
$IPTABLES -A FORWARD -o $EXTERNALIF -p udp --dport 138 -j REJECT
$IPTABLES -A FORWARD -o $EXTERNALIF -p udp --dport 139 -j REJECT
$IPTABLES -A INPUT -i $EXTERNALIF -p udp --dport 137 -j REJECT
```

- Permitir salir al resto de tráfico

```
$IPTABLES -A FORWARD -o $EXTERNALIF -i $INTERNALIF -j ACCEPT
```

- Permitir respuestas entrar

```
$IPTABLES -A OUTPUT -m state --state NEW -o $EXTERNALIF -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A FORWARD -m state --state NEW -o $EXTERNALIF -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

- Activar OpenVpn y el puerto 1194

```
$IPTABLES -A INPUT -i tun+ -j ACCEPT
$IPTABLES -A FORWARD -i tun+ -j ACCEPT
$IPTABLES -A INPUT -i tap+ -j ACCEPT
$IPTABLES -A FORWARD -i tap+ -j ACCEPT
$IPTABLES -A INPUT -p udp --dport 1194 -j ACCEPT
```

- Activar shh en el puerto 1983

```
$IPTABLES -A INPUT -p tcp --dport 1983 -j ACCEPT
```

- Activar FTP puerto 20 y 21

```
$IPTABLES -A INPUT -p tcp  --dport 20 -j ACCEPT
$IPTABLES -A INPUT -p tcp  --dport 21 -j ACCEPT
```

- Activar HTTP puerto 80

```
$IPTABLES -A INPUT -p tcp --dport 80 -j ACCEPT
```

- Activar POP-3 puerto 110

```
$IPTABLES -A INPUT -p tcp --dport 110 -j ACCEPT
```

- Activar IMAP puerto 143

```
$IPTABLES -A INPUT -p tcp --dport 143 -j ACCEPT
```

- Limitar conexiones SMTP a 1 por segundo.

```
$IPTABLES -A INPUT -p tcp --dport 25 --syn -m limit --limit 2/s \
        -limit-burst 10 -j ACCEPT
$IPTABLES -A INPUT -p tcp --dport 25 --syn -j DROP
$IPTABLES -A INPUT -p tcp --dport 25 -j ACCEPT
```

- Enviar peticiones Web a un servidor interno

```
$IPTABLES -A PREROUTING -t nat -i $EXTERNALIF -p tcp -d $MYADDR --dport
80 \  -j DNAT --to 192.168.2.2:80
$IPTABLES -A FORWARD -i $EXTERNALIF -p tcp -d 192.168.2.2 --dport 80 -j
ACCEPT
```

- Enviar peticiones SMTP a un servidor interno

```
$IPTABLES -A PREROUTING -t nat -i $EXTERNALIF -p tcp -d
      $MYADDR --dport 25 \
          -j DNAT --to 192.168.3.10:25
$IPTABLES -A FORWARD -i $EXTERNALIF -p tcp -d 192.168.2.3 --dport 25 -j
ACCEPT
```

- Enviar peticiones FTP a un servidor interno

```
$IPTABLES -A PREROUTING -t nat -i $EXTERNALIF -p tcp -d $MYADDR --dport
20 \
            -j DNAT --to 192.168.2.5:20
$IPTABLES -A PREROUTING -t nat -i $EXTERNALIF -p tcp -d $MYADDR --dport
21 \
            -j DNAT --to 192.168.2.5:21
```

```
$IPTABLES -A FORWARD -i $EXTERNALIF -p tcp -d 192.168.0.10 --dport 20:21 -j
ACCEPT
```

- Puertos que deben ser denegados y guardados, son usados por troyanos conocidos

```
$IPTABLES -A INPUT -p tcp --dport 1433 -m limit -j LOG \
        --log-prefix "Firewalled packet: MSSQL "
$IPTABLES -A INPUT -p tcp --dport 1433 -j DROP
$IPTABLES -A INPUT -p tcp --dport 6670 -m limit -j LOG \
        --log-prefix "Firewalled packet: Deepthrt "
$IPTABLES -A INPUT -p tcp --dport 6670 -j DROP
$IPTABLES -A INPUT -p tcp --dport 6711 -m limit -j LOG \
        --log-prefix "Firewalled packet: Sub7 "
$IPTABLES -A INPUT -p tcp --dport 6711 -j DROP
$IPTABLES -A INPUT -p tcp --dport 6712 -m limit -j LOG \
        --log-prefix "Firewalled packet: Sub7 "
$IPTABLES -A INPUT -p tcp --dport 6712 -j DROP
$IPTABLES -A INPUT -p tcp --dport 6713 -m limit -j LOG \
        --log-prefix "Firewalled packet: Sub7 "
$IPTABLES -A INPUT -p tcp --dport 6713 -j DROP
$IPTABLES -A INPUT -p tcp --dport 12345 -m limit -j LOG \
        --log-prefix "Firewalled packet: Netbus "
$IPTABLES -A INPUT -p tcp --dport 12345 -j DROP
$IPTABLES -A INPUT -p tcp --dport 12346 -m limit -j LOG \
        --log-prefix "Firewalled packet: Netbus "
$IPTABLES -A INPUT -p tcp --dport 12346 -j DROP
$IPTABLES -A INPUT -p tcp --dport 20034 -m limit -j LOG \
        --log-prefix "Firewalled packet: Netbus "
$IPTABLES -A INPUT -p tcp --dport 20034 -j DROP
$IPTABLES -A INPUT -p tcp --dport 31337 -m limit -j LOG \
        --log-prefix "Firewalled packet: BO "
$IPTABLES -A INPUT -p tcp --dport 31337 -j DROP
$IPTABLES -A INPUT -p tcp --dport 6000  -m limit -j LOG \
      --log-prefix "Firewalled packet: XWin "
$IPTABLES -A INPUT -p tcp --dport 6000  -j DROP
$IPTABLES -A INPUT -p udp --dport 33434:33523 -j DROP
```

- Bloqueo de IGMP

```
$IPTABLES -A INPUT -p igmp -j REJECT
```

- Bloqueo todo el tráfico restante

```
$IPTABLES -A INPUT -p tcp -j REJECT --reject-with tcp-reset
```

```
$IPTABLES -A INPUT -p all -j DROP
$IPTABLES -A FORWARD -p tcp -j REJECT --reject-with tcp-reset
$IPTABLES -A FORWARD -p all -j DROP
```

- Aceptar demás conexiones de salida

```
$IPTABLES -A OUTPUT -j ACCEPT
```

- Redirección del tráfico HTTP puerto 80 al puerto 3128 para el uso de Squid

```
$IPTABLES -t nat -A PREROUTING -i $INTERNALIF -p tcp --dport 80 -j
REDIRECT --to-port 3128
```

- Registrar y descartar paquetes de la red local intentando salir

```
$IPTABLES -A FORWARD -p tcp --dport 25 -j LOG
$IPTABLES -A FORWARD -p tcp --dport 25 -j DROP
$IPTABLES -A OUTPUT -p tcp --dport 25 -j DROP
```

- Enmascaramiento de conexiones

```
$IPTABLES -A POSTROUTING -t nat -o $EXTERNALIF -j MASQUERADE
```

3.3.2 Proxy

El servicio de proxy lo brindará Squid, la versión a utilizarse es Squid-2.6.STABLE21-6.el5.

3.3.2.1 Squid

Es un servidor proxy-caché muy útil y efectivo en un entorno en el que se necesita compartir la conexión de internet para navegación y mantener un control de acceso mediante horarios, URLs, dominios, etc.

Se implementará un proxy transparente evitando la molestia de configuraciones en las máquinas clientes.

3.3.2.1.1 Instalación

yum install squid

3.3.2.1.2 Archivo de configuración

/etc/squid/squid.conf

3.3.2.1.3 Trabajo con ACL y accesos

3.3.2.1.3.1 Tipos de ACL.

- acl nombre src direccion_ip/mascara: Una dirección IP, red o subred de origen.

  Ejemplo: acl nombreACL src 192.168.3.1/255.255.255.0

- acl nombreACL src dir1-dir2/mascara: Un rango de direcciones IP de origen

  Ejemplo: acl nombreACL src 192.168.3.10-192.168.3.20/255.255.255.0

- acl nombreACL dst direccion_ip/mascara: Una dirección IP, red o subred de destino.

  Ejemplo: acl nombreACL dst 192.168.3.2/255.255.255.0

- acl nombreACL myip direccion_ip/mascara: La dirección IP de socket local.

- acl nombreACL arp direccion_mac (formato: xx:xx:xx:xx:xx:xx): Una dirección MAC del cliente (no está soportada en todos los sistemas).

  Ejemplo: acl macaddress arp 09:00:2b:23:45:67

- acl nombreACL srcdomain .midominio.com: Un nombre de dominio de origen (búsqueda reversa)

Ejemplo: acl my_other_proxy srcdomain .proxy.example.com

- acl nombreACL dstdomain .midominio.com: Nombre de dominio del servidor de destino en la URL

  Ejemplo: acl local-servers dstdomain my.domain.net

- acl nombreACL time [SMTWHFA] [h1:m1-h2:m2]: Día y/u horario de acceso. h1:m1, si se usa, deberá ser menor que h2:m2.

  Ejemplo: acl almuerzo time MTWHFA 13:00-14:30

- acl nombreACL url_regex [-i] expr: Coincidencia con expresión regular en la URL. Por defecto es sensible a mayúsculas y minúsculas, excepto si se usa el -i.

  Ejemplo: acl buenos url_regex -i "/etc/squid/reglas/permitidos"

- acl nombreACL port 80 70 21: Una lista de puertos.

  Ejemplo: acl msn port 6901

- acl nombreACL port 0-1024: Un rango de puertos.

  Ejemplo: acl msn port 6891-6900

- acl nombreACL proto HTTP FTP: Una lista de protocolos.

  Ejemplo: acl manager proto cache_object

- acl nombreACL method GET POST: Una lista de métodos HTTP.

  Ejemplo: acl msn_method method POST

- acl nombreACL browser [-i] expr: Coincidencia con expresión regular en el encabezado “User-Agent” enviado por el navegador.

  Ejemplo: acl MSN_Messenger browser ^Mozilla.compatible;.MSN Messenger.

Posterior a crear las ACL se debe indicar a cuales permitir y a cuales denegar mediante la directiva http_access.

Sintaxis

http_access <allow|deny> nombreACL [!][nombre_acl2]

allow permite el paso de las conexiones definidas por nombreACL
deny niega el paso de las conexiones definidas por nombreACL
“!” negación de la ACL que precede.

3.3.2.1.4 Manejo del servicio

Inicio del servicio: service squid start
Recargar el servicio: service squid reload
Reiniciar el servicio: service squid restart
Detener el servicio: service squid stop

Nota: después de realizar un cambio en el archivo de configuración /etc/squid/squid.conf se puede utilizar la opción service squid reload ya que al reiniciar el servicio los usuarios quedarán sin acceso a internet durante un periodo más largo de tiempo.

3.3.2.1.5 Configuración de Squid

El archivo de configuración completo se encuentra en el ANEXO 2.

3.3.2.1.5.1 Parámetro http_port

Se configura el puerto de escucha de squid por defecto el puerto es el 3128. Para la configuración de un proxy transparente se agregará la palabra “transparent”. Se puede también especificar la dirección IP del servidor

http_port 192.168.3.1:3128 transparent

3.3.2.1.5.2 Parámetro cache_mem

Parámetro que establece la cantidad de memoria RAM para objetos en tránsito, objetos frecuénteme utilizados y objetos negativamente almacenados en el caché, el valor predeterminado en Centos 5 es 8 MB, de pendiendo de la memoria se deberá cambiar este parámetro, con 256 MB es más que suficiente para el 99% de las necesidades.

cache_mem 256 MB

3.3.2.1.5.3 Parámetros cache_swap

Con estos parámetros que por defecto vienen desactivados se indica a Squid mantenga los niveles de espacio del área de intercambio en un 90% y 95%

cache_swap_low 90
cache_swap_high 95

3.3.2.1.5.4 Parámetro Maximum_object_size

Con este parámetro se especifica qué objetos mayores al especificado no se guardarán en el disco. Este parámetro se especifica en kilobytes, y si se requiere aumentar la velocidad más que resguardar el ancho de banda, se debería dejar este parámetro en valores bajos.

maximum_object_size 10240 KB

3.3.2.1.5.5 Parámetro hierarchy_stoplist

Este parámetro permite especificar un conjunto de palabras que al ser encontradas en un URL, van a ser manejadas directamente por este caché.

hierarchy_stoplist cgi-bin ?

3.3.2.1.5.6 Parámetro cache_dir

Con este parámetro se especifica el tamaño que se desea que Squid utilice para el almacenamiento en disco, mientras más objetos se almacenen en éste, menos ancho de banda se consumirá.

cache_dir ufs /var/spool/squid 2048 16 256

Se almacenarán 2048 MB en disco dividido en jerarquías de 16 directorios subordinados, hasta llegar a 256.

3.3.2.1.5.7 Parámetro cache_log

Este parámetro especifica donde se guardaran los mensajes de comportamiento de Squid.

cache_log /var/log/squid/cache.log

3.3.2.1.5.8 Parámetro access_log

Este parámetro especifica el directorio donde se guarda el registro de control de acceso, esta información es muy útil cuando se requiere estadísticas de navegación de los usuarios. Se utilizará el generador de reportes SARG para leer fácilmente los log de navegación.

access_log /var/log/squid/access.log squid

3.3.2.1.5.9 Configuración adecuada según los requerimientos de la empresa

3.3.2.1.5.9.1 Listas de control de acceso

Por administración y requerimiento se crearon 3 listas de control de acceso

1. En la primera lista de control de acceso “sin_restriccion” se listará a todas las direcciones IP de la red interna con permiso para salir a internet, el archivo completo se encuentra en el ANEXO 3.

   Por políticas internas a cada máquina se reserva una dirección IP en un rango determinado, esta reserva se realiza en el servidor DHCP mediante la dirección MAC del equipo. El rango de asignación es 192.168.3.2 a 192.168.3.70

acl sin_restriccion src "/etc/squid/reglas/sin_restriccion"

2. En la segunda lista de control de acceso “contabilidad” (ver ANEXO 4) se listarán las direcciones IP de usuarios que no pueden acceder a redes sociales como Facebook, Hi5, Tuenti, Twitter, Foursquare, Quora, Youtube, Linkedin

   acl contabilidad src "/etc/squid/reglas/contabilidad"

3. En la tercera lista de control de acceso (Ver ANEXO 5) se permite el acceso a internet a máquinas de visitas, el rango asignado para estas máquinas es : 192.168.3.100 a 192.168.3.130

   acl visitas src "/etc/squid/reglas/visitas"

4. Las listas de control de acceso 4 y 5 determinan una coincidencia con expresión regular en la URL determinada por el contenido de los archivos "/etc/squid/reglas/permitidos" y "/etc/squid/reglas/prohibidos".

   acl permitidos url_regex -i "/etc/squid/reglas/permitidos"
   acl prohibidos url_regex -i "/etc/squid/reglas/prohibidos"

3.3.2.1.5.9.2 Reglas de control de acceso

5. En la primera regla de control de acceso se da permiso total sin restricción alguna a las direcciones IP de las máquinas listadas en el archivo “etc/squid/reglas/sin_restriccion”

   http_access allow sin_restriccion

6. En la segunda regla de control de acceso se da permiso total sin restricción alguna, a las direcciones IP de las máquinas listadas en el archivo “etc/squid/reglas/visitas”

   http_access allow visitas

7. En la tercera regla de control de acceso se deniega la navegación a los clientes que se dirigen a las URL que contengan cualquiera de las palabras listadas en "/etc/squid/reglas/prohibidos" excepto si se encuentran en la lista "/etc/squid/reglas/permitidos".

http_access deny prohibidos !permitidos

8. En la cuarta regla de control de acceso se permite el tráfico a los clientes con las direcciones IP listadas en el archivo “etc/squid/reglas/contabilidad”

http_access allow contabilidad

3.3.3 VPN

Acrónimo de Virtual Private Network o red privada virtual, es una solución muy eficaz y segura que brindará un acceso remoto seguro a usuarios que se encuentren fuera de la empresa. Para la configuración e instalación del servidor se utilizará OPENVPN.

3.3.3.1 OPENVPN

OpenVpn es una solución de conectividad basada en SSL publicado bajo licencia de código abierto. Puede ofrecer conectividad punto a punto, host conectados remotamente y jerárquica de usuarios.

3.3.3.1.1 Instalación

yum install openvpn

3.3.3.1.2 Archivo de configuración

Es necesario crear el archivo de configuración, el cual puede tener cualquier nombre pero debe terminar en .conf

/etc/openvpn/server.conf

3.3.3.1.3 Manejo del servicio

Inicio del servicio: service openvpn start
Recargar el servicio: service openvpn reload
Reiniciar el servicio: service openvpn restart
Detener el servicio: service openvpn stop
Estado del servicio: service openvpn status

3.3.3.1.4 Implementación

Para facilitar la implementación se utilizarán scripts los cuales se encuentran en la documentación de OpenVpn:

/usr/share/doc/openvpn-2.2.0/easy-rsa/

Los archivos serán copiados en el directorio de trabajo de openvpn:

cp -r /usr/share/doc/openvpn-2.2.0/easy-rsa/2.0/ /etc/openvpn/easy-rsa

3.3.3.1.4.1 Cambio de variables de entorno

Las variables de entorno deberán ser cambiadas en el archivo /etc/openvpn/easy-rsa/vars

vi /etc/openvpn/easy-rsa/vars

Los siguientes parámetros deberán ser editados según información de la empresa

```
export KEY_COUNTRY="EC"
export KEY_PROVINCE="PICHINCHA"
export KEY_CITY="QUITO"
export KEY_ORG="PROTECO"
export KEY_EMAIL="gleon@proteco-coasin-com"
```

3.3.3.1.4.2 Cargar la configuración de las variables de entorno ejecutando

Se deberá cargar la configuración de las variables de entorno a través de la ejecución de los siguientes comandos:

```
cd /etc/openvpn/easy-rsa/
source ./vars
./clean-all
```

3.3.3.1.4.3 Crear archivo de configuración del servidor

Se crea el archivo de configuración del servidor a través de:

vi /etc/openvpn/server.conf

Contenido del archivo de configuración

```
# Puerto de trabajo de OpenVpn
port 1194

#Protocolo de trabajo
proto udp

#Tipo de interface virtual que utilizará el servidor OpenVpn
dev tun

#Ubicación del archivo de la Autoridad Certificadora
ca ca.crt

#Ubicción del certificado de servidor
cert SERVIDORNS.crt

#Ubicación de la llave creada por el servidor
key SERVIDORNS.key

#Ubicación del archivo que contiene el formato Diffie Helman
dh dh1024.pem

#Rango IP que se utilizará en la red privada virtual
server 10.8.0.0 255.255.255.0

#Archivo de registro de las direcciones ip de los clients conectados.
ifconfig-pool-persist ipp.txt

# Especificación de la ruta para que el cliente tenga acceso a la red local
push "route 192.168.2.0 255.255.255.0"

#Especificación de DNS de la red interna
push "dhcp-option DNS 192.168.3.1"
push "dhcp-option DNS 192.168.3.206"
# Envío de pings cada 10 segundos para comprobación de la actividad del cliente, si no recibe confirmación durante 120 segundos asume que el sitio remoto esta fuera.
```

keepalive 10 120

#Activación de compresión en la red privada virtual.
comp-lzo

#Preservar el estado después de un reinicio
persist-key
persist-tun

#enviar un reporte de clients conectado una vez por minuto al archive openvpn-status.log
status openvpn-status.log

#Nivel de verbosidad que se requiere, mientras más alto sea el nivel más información tendremos
verb 4

3.3.3.1.4.4 Creación de la autoridad certificadora

Para crear el la llave “ca.key” y el certificado “ca.crt” de la autoridad certificadora ejecutamos:

cd /etc/openvpn/easy-rsa/
./pkitool –initca

```
[root@ns easy-rsa]# ./pkitool --initca
Using CA Common Name: PROTECO CA
Generating a 1024 bit RSA private key
.........................................++++++
.....................................................................................
writing new private key to 'ca.key'
```

Ilustración 3-2 - Creación de la autoridad certificadora

./pkitool build-ca

```
[root@ns easy-rsa]# ./pkitool build-ca
Generating a 1024 bit RSA private key
.++++++
..++++++
writing new private key to 'build-ca.key'
-----
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'EC'
stateOrProvinceName   :PRINTABLE:'PICHINCHA'
localityName          :PRINTABLE:'QUITO'
organizationName      :PRINTABLE:'PROTECO'
commonName            :PRINTABLE:'build-ca'
emailAddress          :IA5STRING:'gleon@proteco-coasin-com'
Certificate is to be certified until Feb 13 00:31:01 2022 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

Ilustración 3-3 - Creación de la autoridad certificadora

3.3.3.1.4.5 Creación del certificado y llave de encriptación del servidor

Para crear el certificado y la llave de encriptación del servidor ejecutamos:

cd /etc/openvpn/easy-rsa/
./pkitool build-key-server SERVIDORNS

```
[root@ns easy-rsa]# ./pkitool --server SERVIDORNS
Generating a 1024 bit RSA private key
.......++++++
.....................++++++
writing new private key to 'SERVIDORNS.key'
-----
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'EC'
stateOrProvinceName   :PRINTABLE:'PICHINCHA'
localityName          :PRINTABLE:'QUITO'
organizationName      :PRINTABLE:'PROTECO'
commonName            :PRINTABLE:'SERVIDORNS'
emailAddress          :IA5STRING:'gleon@proteco-coasin-com'
Certificate is to be certified until Feb 13 00:49:38 2022 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

Ilustración 3-4 – Creación del certificado y llave de encriptación del servidor

3.3.3.1.4.6 Creación de parámetros Diffie Hellman.

Para crear los parámetros Diffie Hellman “dh1024.pem” realizamos:

cd /etc/openvpn/easy-rsa/
./build-dh

```
[root@ns easy-rsa]# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
..+.....................................................................
.....................................+.......+.........................
.....................+.............+...+.......+.............++*+
```

Ilustración 3-5 -Creación de parámetros Diffie Hellman

3.3.3.1.4.7 Creación de certificados para clientes

Para la creación de los certificados de cada cliente utilizamos la herramienta pktool:

cd /etc/openvpn/easy-rsa/
./pkitool gleon

```
[root@ns easy-rsa]# ./pkitool gleon
Generating a 1024 bit RSA private key
...........++++++
.............................++++++
writing new private key to 'gleon.key'
-----
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'EC'
stateOrProvinceName   :PRINTABLE:'PICHINCHA'
localityName          :PRINTABLE:'QUITO'
organizationName      :PRINTABLE:'PROTECO'
commonName            :PRINTABLE:'gleon'
emailAddress          :IA5STRING:'gleon@proteco-coasin-com'
Certificate is to be certified until Feb 13 00:58:01 2022 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

Ilustración 3-6 - Creación de certificados para clientes

Los certificados se guardan en el directorio /etc/openvpn/easy-rsa/keys. De este directorio se utilizarán los siguientes archivos:

- ca.crt
- ca.key
- SERVIDORNS.key
- SERVIDORNS.crt
- dh1024.pem

Estos serán movidos al directorio raíz de OpenVpn /etc/openvpn a través de las siguientes instrucciones:

cd /etc/openvpn/easy-rsa/keys/
mv ca.crt ca.key SERVIDORNS.key SERVIDORNS.crt dh1024.pem /etc/openvpn

Se reinicia el servicio de OpenVpn para cargar la nueva configuración mediante el siguiente comando:

service openvpn restart

3.3.3.1.4.8 Configuración de cliente

En su totalidad los clientes utilizan plataforma Windows por lo que se describe la configuración del cliente en este sistema operativo.

Serán utilizados los siguientes archivos creados anteriormente ubicados en /etc/openvpn/easy-rsa/keys/ los cuales deben ser copiados en la carpeta de configuración del cliente.

- ca.crt
- gleon.crt
- gleon.key

En Windows la ruta de configuración es:

C:\Program Files (x86)\OpenVPN\config

La aplicación de Windows para el cliente es gratuita y fue descargada de:

http://openvpn.net/index.php/open-source/downloads.html

3.3.3.1.4.8.1 Instalación de OPENVPN en Windows

Posterior a la descarga se procede con la instalación de la aplicación, se debe seguir los pasos guiados por el wizard de instalación:

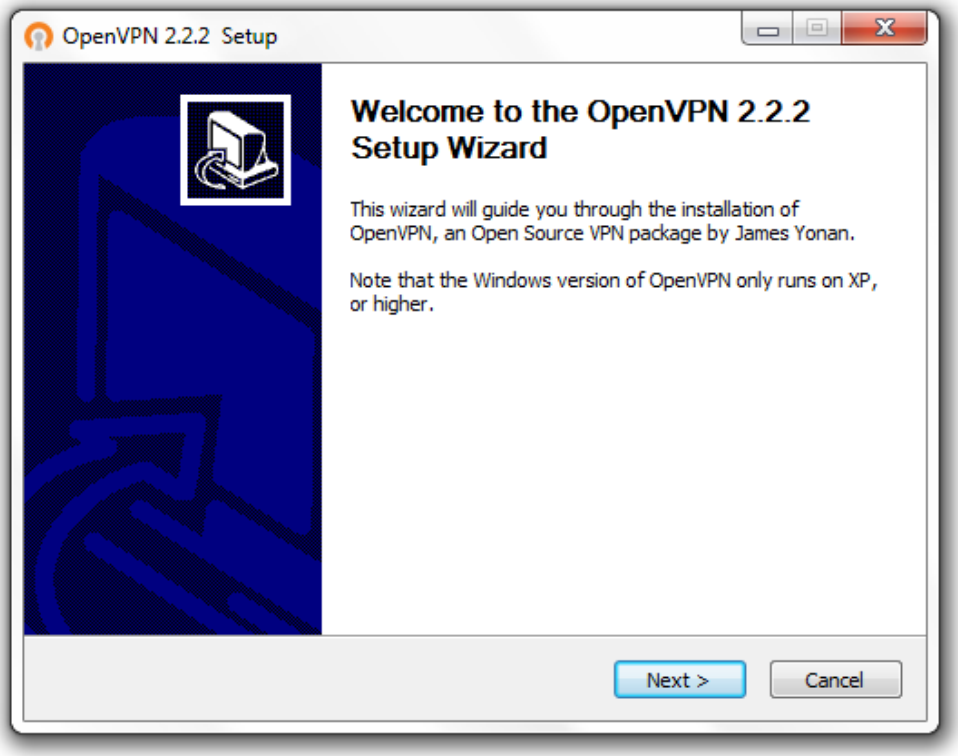


Ilustración 3-7 - Instalación de Openvpn en Windows (Wizard Setup)

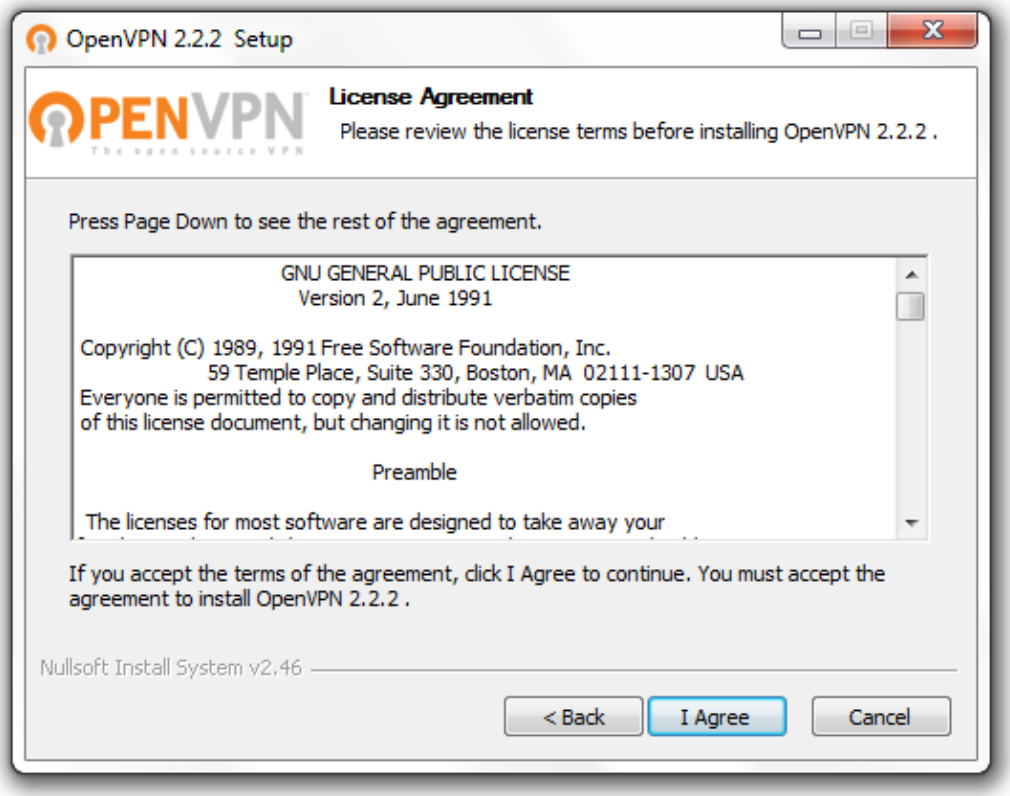


Ilustración 3-8 - Instalación de Openvpn en Windows (Licencia de Producto)

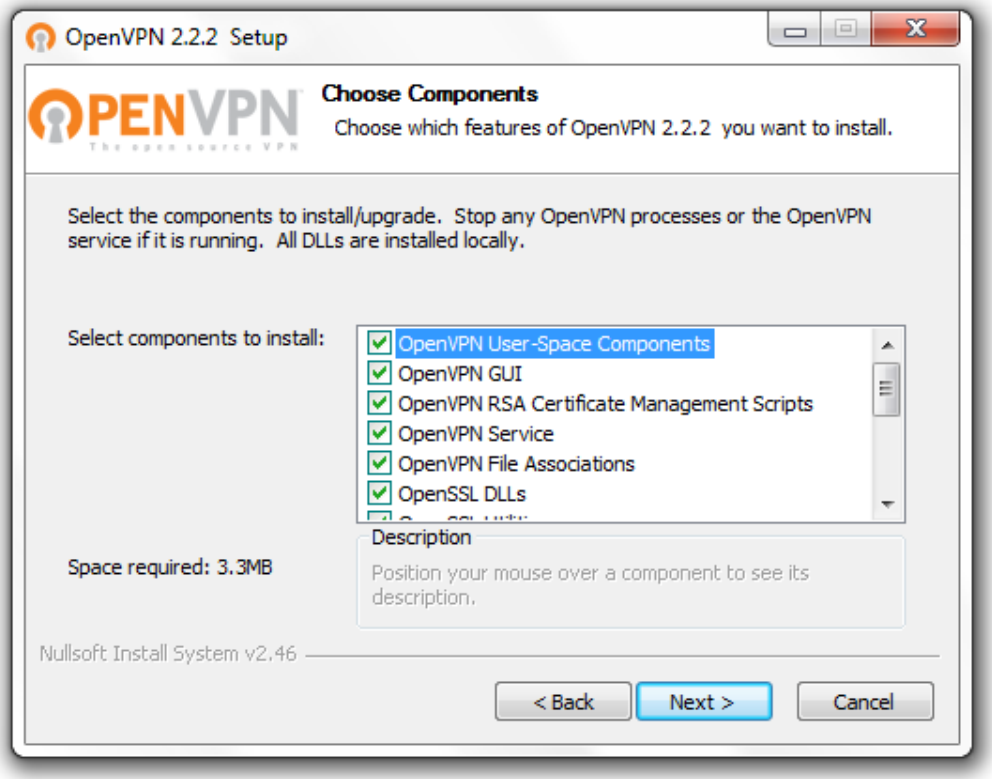


Ilustración 3-9 - Instalación de Openvpn en Windows (Componentes a instalar)

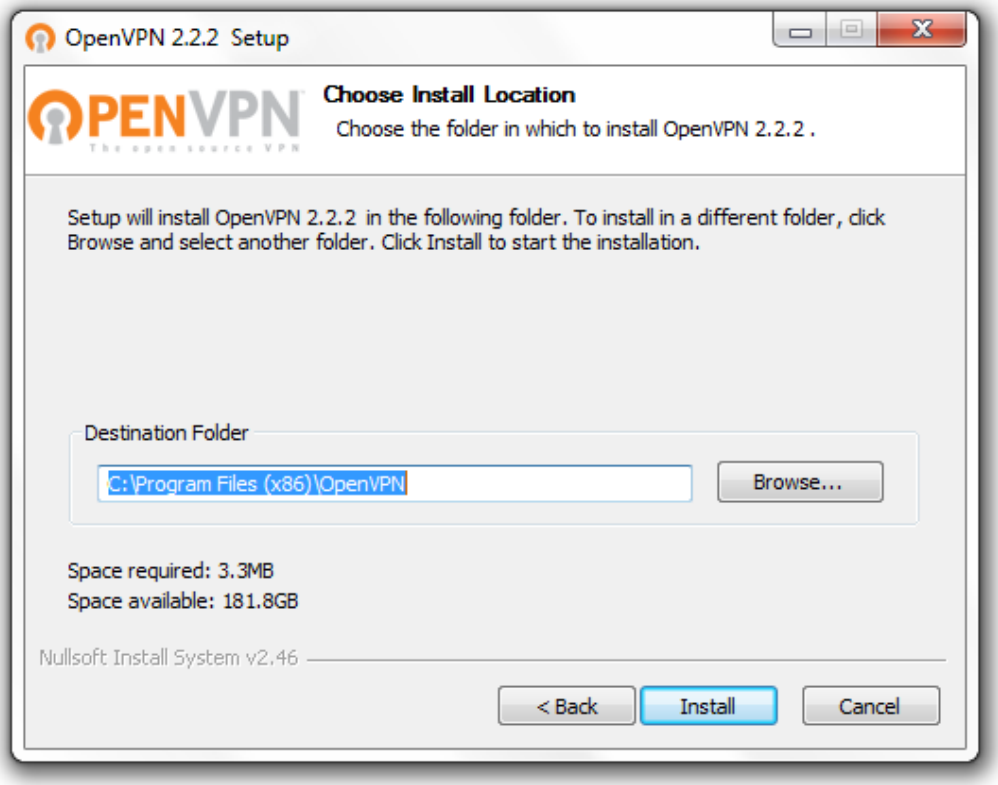


Ilustración 3-10 - Instalación de OpenVpn en Windows (ubicación de archivos a instalar)

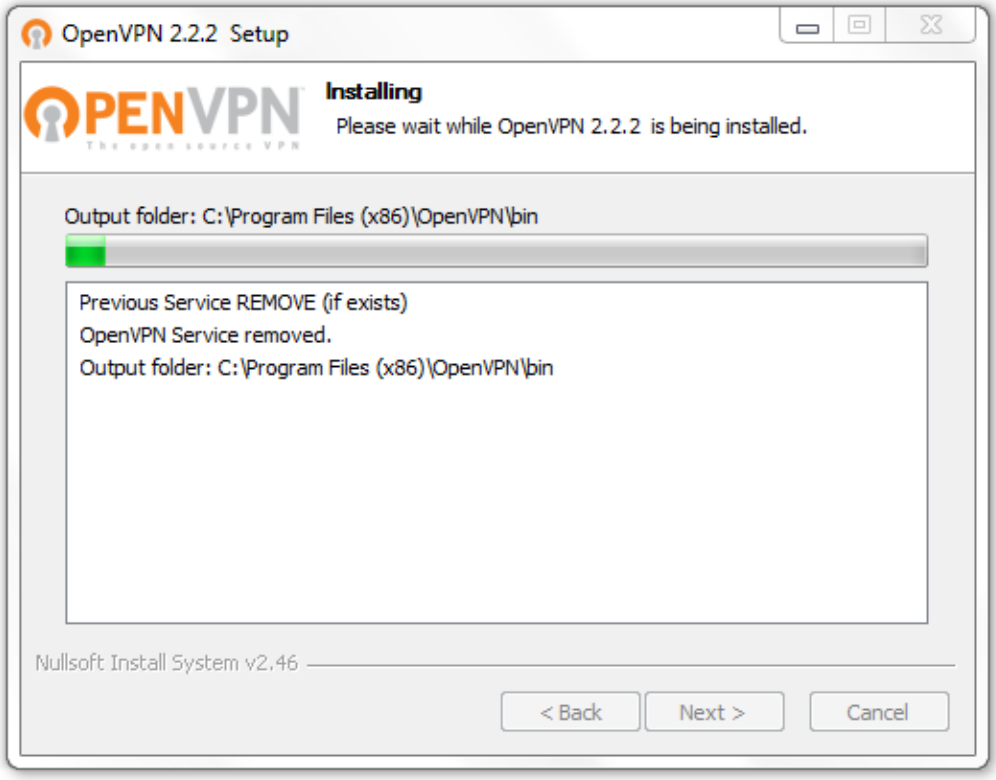


Ilustración 3-11 - Instalación de OpenVpn en Windows (Progreso de instalación)

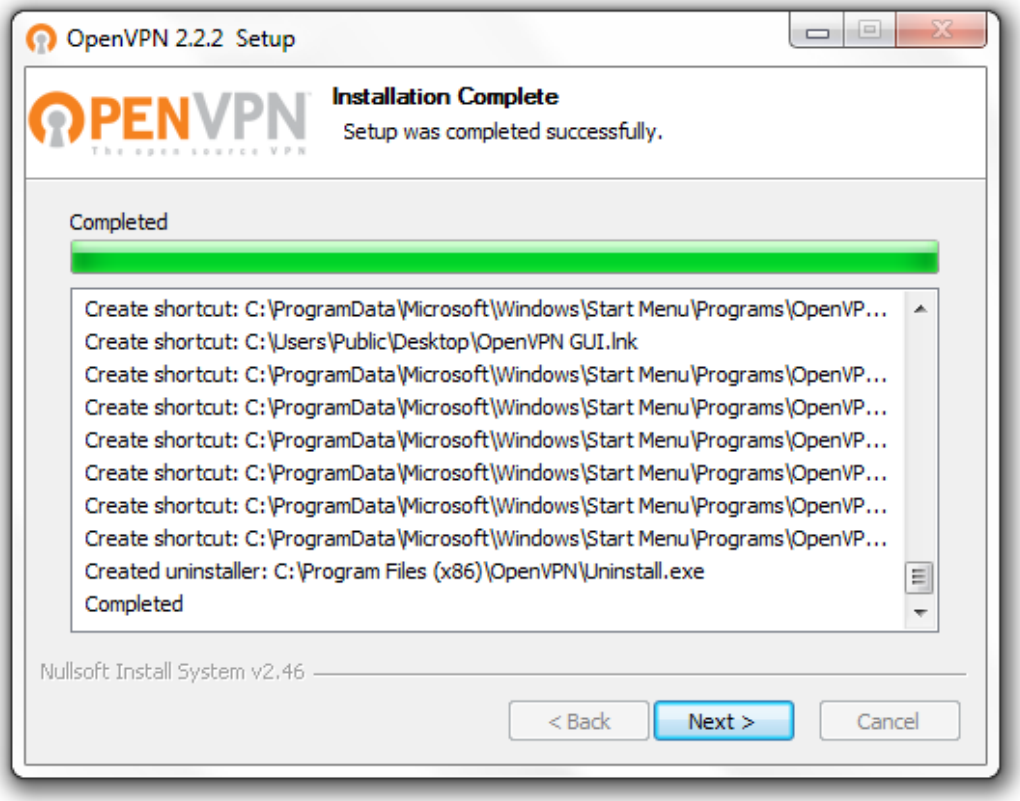


Ilustración 3-12 - Instalación de OpenVpn en Windows (Progreso de instalación)

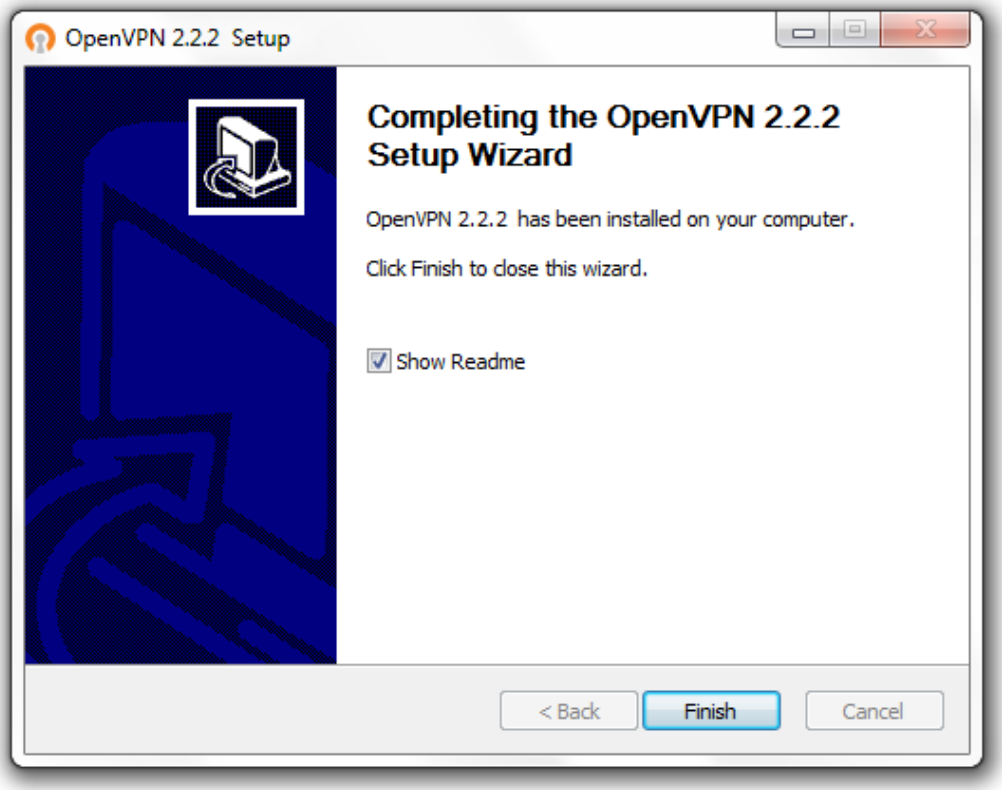


Ilustración 3-13 - Instalación de OpenVpn en Windows (Finalización de instalación)

Ejecutar OpenVpn con privilegios de administrador.

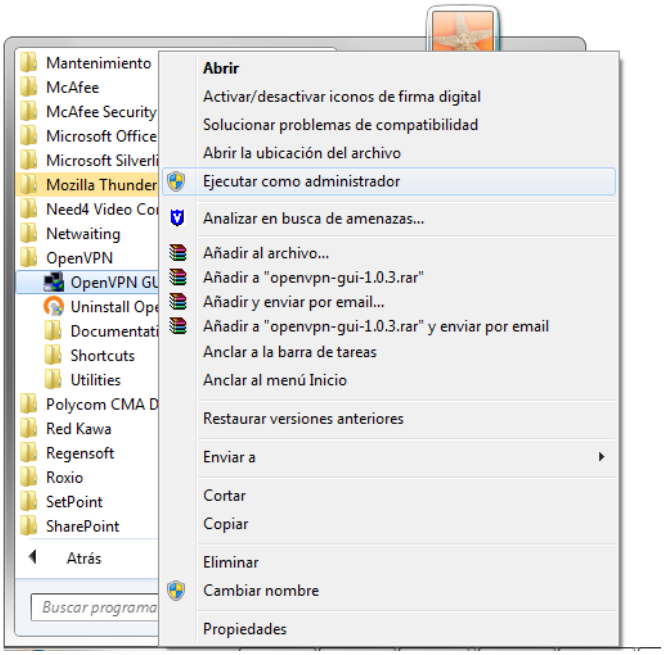


Ilustración 3-14 -Configuración de OpenVpn (Ubicación del ejecutable)

Editar el archivo de configuración de OpenVpn en el cliente

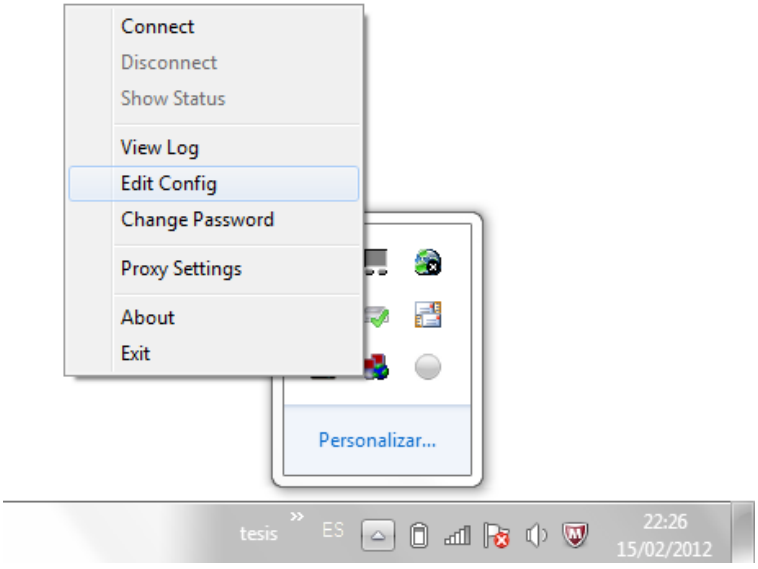


Ilustración 3-15 - Configuración de OpenVpn

3.3.3.1.4.8.2 Archivo de configuración del cliente

El archivo de configuración completo está descrito en el ANEXO 6 y debe tener la extensión".ovpn"
Los parámetros de configuración son los siguientes:

- Especificar que se está trabajando como cliente

  client

- Tipo de interface virtual que utilizará el cliente OpenVpn, configurar el que se especificó en el servidor

  dev tun

- Especificar el protocolo de conexión

  proto udp

- Indicar al cliente seguir intentando indefinidamente resolver el nombre del servidor VPN, muy útil para clientes con laptops.

  resolv-retry infinite

- No unirse a un puerto local

  nobind

- Tratar de preservar el estado después de un reinicio de conexión

  persist-key
  persist-tun

- Ubicación de la autoridad certificadora (ca) y de la clave y certificado del cliente, estos archivos fueron generados por el servidor

ca "C:\\Program Files (x86)\\OpenVPN\\config\\ca.crt"
cert "C:\\Program Files (x86)\\OpenVPN\\config\\gleon.crt"
key "C:\\Program Files (x86)\\OpenVPN\\config\\gleon.key"

- Activar la compresión en la conexión VPN

  comp-lzo

- Activar el nivel de verbosidad

  verb 3

3.3.4 DHCP

El servicio DHCP permite la configuración automática de los parámetros de red en los hosts cliente, servicio muy útil para redes grandes, ya que evita cambios en la configuración de la máquina del cliente lo cual le permite a la misma, ingresar a otra red sin la necesidad de cambios en su configuración.

3.3.4.1 Instalación

yum install dhcp

3.3.4.2 Archivo de configuración

El archivo de configuración se encuentra en la siguiente ruta:

/etc/dhcpd.conf

3.3.4.3 Manejo del servicio

Inicio del servicio: service dhcpd start
Reiniciar el servicio: service dhcpd restart
Detener el servicio: service dhcpd stop
Estado del servicio: service dhcpd status

3.3.4.4 Implementación

El archivo de configuración completa se encuentra en el ANEXO 7, los parámetros a configurar con son siguientes:

- Indicar el método de actualización automática DNS automática con los valores de la IP asignados por DHCP

  ddns-update-style interim;

- Ignorar las peticiones de máquinas clientes con direcciones IP antes asignadas

  ignore client-updates;

- Parámetro para la rápida propagación de los servicios de red

  authoritaive;

- Declaración de subred compartida

  shared-network miredlocal {

- Declaración de la red y máscara de red

  subnet 192.168.2.0 netmask 255.255.255.0 {

- Declaración del default gateway

  option routers 192.168.2.1;

- Declaración de la máscara de subred

  option subnet-mask 255.255.255.0;

- Declaración de la dirección de broadcast

  option broadcast-address 192.168.2.255;

- Declaración del dominio a utilizar

  option domain-name "proteco-coasin.com";

- Declaración de los servidores DNS

  option domain-name-servers 192.168.2.1, 192.168.2.206;

- Declaración de servidores Wins

  option netbios-name-servers 192.168.2.1;

- Rango de asignación de direcciones IP

  range 192.168.2.100 192.168.2.130;

- Determinar el tiempo para la nueva asignación de direcciones IP

  default-lease-time 21600;

- Determinar el tiempo de vigencia de la dirección IP de cada equipo

  max-lease-time 43200;

  Por motivos de seguridad se trabajará con un servidor DHCP estático mediante la asignación de direcciones IP a una dirección MAC determinada, esto se realizará con todos los equipos de red.

```
host pro_tec_gleon {
        option host-name "pro_tec_gleon";
        hardware ethernet 00:16:D3:1E:BA:11;
        fixed-address 192.168.2.6;
                }
```

3.3.5 DNS

El servidor de nombres de dominio Bind (Berkeley Internet Name Domain) será utilizado para la implementación del protocolo DNS. Bind es una aplicación que nos permite utilizar varios servicios de nombres de dominio en forma libre.

3.3.5.1 Instalación

3.3.5.1.1 Sustento lógico necesario.

Existen varios paquetes necesarios y útiles para la configuración de DNS

Paquete.	Descripción.
• **bind**	Incluye el **Servidor DNS** (**named**) y herramientas para verificar su funcionamiento.
• **bind-libs**	Biblioteca compartida que consiste en rutinas para aplicaciones para utilizarse cuando se interactúe con **Servidores DNS**.
• **bind-chroot**	Contiene un árbol de ficheros que puede ser utilizado como una jaula *chroot* para **named** añadiendo seguridad adicional al servicio.
• **bind-utils**	Colección de herramientas para consultar **Servidores DNS**.
• **caching-nameserver**	Ficheros de configuración que harán que el **Servidor DNS** actúe como un caché para el servidor de nombres.

3.3.5.1.2 Instalación a través de yum.

La utilización de yum facilitará en gran forma la instalación del protocolo DNS.

```
yum -y install bind bind-chroot bind-utils caching-nameserver
```

3.3.5.1.3 Ubicación de archivo de configuración

El archivo de configuración del servidor DNS se encuentra en la siguiente ruta:

/var/named/chroot/etc/named.conf

3.3.5.1.4 Manejo del servicio

Inicio del servicio: service named start
Reiniciar el servicio: service named restart
Detener el servicio: service named stop
Estado del servicio: service named status

3.3.5.2 Implementación

3.3.5.2.1 Servidor DNS de caché.

El archivo de configuración completo se describe en el ANEXO 8, los parámetros de configuración para el servidor DNS de caché que se implementará en el mismo equipo que el firewall son los siguientes:

- Especificar el directorio que contiene los archivos con los datos de la zona.

  directory "/var/named/";

- Definir el archivo donde se almacenará la información del cache

  dump-file "/var/named/data/cache_dump.db";

- Archivo para control mediante estadísticas

  statistics-file "/var/named/data/named_stats.txt";

- Especificar a qué direcciones IP se le permite la recursión.

  allow-recursion {

```
127.0.0.1;
192.168.2.0/24;
};
```

- Permitir a las redes realizar consultas DNS mediante este servidor.

```
allow-query {
192.168.2.0/24;
127.0.0.1;
10.8.0.0/24; };
```

- Especificar los servidores DNS a donde redirigir las peticiones, generalmente los DNS del proveedor de servicio.

```
forwarders {
190.108.65.3;
190.108.64.2;
};
```

- Reenviar las consultas antes de tratar de resolverlas mediante un root name server

```
forward first;
```

- Indicar qué interface de red escucha solicitudes.

```
listen-on { 192.168.2.1; };
```

- Declaración de zona: indicar que esta zona se administra en este servidor local mediante el parámetro “master”. Indicar la ubicación del fichero de configuración de la zona mediante “file” y no permitir el acceso de escritura desde el exterior a los datos de zona mediante “allow-update {none};.

```
zone "proteco-coasin.com" {
type master;
file "proteco-coasin.com.zone";
allow-update { none; };
};
```

- Declaración de la zona inversa para proteco-coasin.com

```
zone "10.168.192.in-addr.arpa" {
type master;
file "10.168.192.in-addr.arpa.zone";
allow-update { none; };
};
```

3.3.5.2.1.1 Archivo de zona proteco-coasin.com

La ubicación del archivo de zona es:
/var/named/chroot/var/named/proteco-coasin.com.zone

Contenido:

```
$TTL 86400
@ IN SOA ns.proteco-coasin.com. gleon.proteco-coasin.com. (
                    2012022301; número de serie
                    28800 ; tiempo de refresco
                    7200 ; tiempo entre reintentos de consulta
                    604800 ; tiempo tras el cual expira la zona
                    86400 ; tiempo total de vida
)
@ IN NS ns
@ IN MX 5 mail.proteco-coasin.com.
@ IN A 192.168.3.202
www         IN A 192.168.3.211
ftp         IN A 192.168.3.203
mail        IN A 192.168.3.202
```

3.3.5.2.1.2 Archivo de zona inversa para proteco-coasin.com

La ubicación del archivo de zona es:

/var/named/chroot/var/named/10.168.192.in-addr.arpa.zone

Contenido:

```
$TTL 86400
@ IN SOA mail.proteco-coasin.com. gleon.proteco-coasin.com. (
                    2012022501 ; número de serie
                    28800 ; tiempo de refresco
                    7200 ; tiempo entre reintentos de consulta
```

```
                    604800 ; tiempo tras el cual expira la zona
                    86400 ; tiempo total de vida
)
@ IN NS ns.proteco-coasin.com.
1 IN PTR ns.proteco-coasin.com.
202  IN PTR mail.proteco-coasin.com.
203  IN PTR ftp.proteco-coasin.com.
211  IN PTR www.proteco-coasin.com.
```

3.3.6 Correo Electrónico

En la implementación del servidor de correo electrónico se utilizará como MTA al servidor Sedmail y como servidor IMAP y POP3 a Dovecot

3.3.6.1 Instalación a través de yum

Los paquetes necesarios para la configuración del servidor de correo electrónico se los puede descargar mediante la herramienta yum.

yum -y install sendmail sendmail-cf dovecot m4 make

3.3.6.2 Configuración

3.3.6.2.1 Dominios a administrar

Los dominios a ser administrados se especifican en el archivo /etc/mail/local-host-names.

vi /etc/mail/local-host-names

Contenido:

```
# local-host-names - include all aliases for your machine here.
proteco-coasin.com
ns.proteco-coasin.com
mail.proteco-coasin.com
```

Establecer los dominios que tendrán permitido re-transmitir correo electrónico desde el servidor generando el fichero /etc/mail/relay-domains

vi /etc/mail/relay-domains

Contenido:

```
mail.proteco-coasin.com
ns.proteco-coasin.com
proteco-coasin.com
192.168.3.
10.8.0.
```

3.3.6.2.2 Control de acceso

Definir los dominios o conjunto de direcciones IP que podrán hacer uso del servidor de correo.

vi /etc/mail/access

Contenido:

```
Connect:localhost.localdomain          RELAY
Connect:localhost                       RELAY
Connect:127.0.0.1                       RELAY
# Dirección IP del propio servidor.
Connect:192.168.3.1                     RELAY
Connect:10.8.0.1                        RELAY
proteco-coasin.com                      RELAY
# Bloques de Asia Pacific Networks, ISP desde el cual se emite la mayor
# parte del Spam del mundo
222                 REJECT
221                 REJECT
220                 REJECT
219                 REJECT
218                 REJECT
212                 REJECT
211                 REJECT
210                 REJECT
203                 REJECT
202                 REJECT
140.109             REJECT
```

```
133             REJECT
61              REJECT
60              REJECT
59              REJECT
58              REJECT
```

3.3.6.2.3 Configuraciones de Sendmail

Para definir, cambiar, o añadir funciones a sendmail se lo realiza en el archivo /etc/mail/sendmail.mc, el archivo de configuración completo esta descrito en el ANEXO 9

vim /etc/mail/sendmail.mc

Los parámetros de configuración establecidos son los siguientes:

- Ocultar la versión de sendmail y dar un mensaje de bienvenida al establecer conexión con el servidor

  define(`confSMTP_LOGIN_MSG',`$j Sendmail; $b')dnl

- Permitir a sendmail escuchar peticiones de la LAN mediante la opción DAEMON_OPTIONS, para esto es necesario borrar la dirección de lookback en la siguiente línea:

  DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
  de esta forma se obtendrá:

  DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl

- Negar el envío de correos a dominios inexistentes comentando la siguiente opción:

  dnl FEATURE(`accept_unresolvable_domains')dnl

- Definir la máscara que utilizará el servidor

  MASQUERADE_AS(`proteco-coasin.com')dnl

FEATURE(masquerade_envelope)dnl
FEATURE(masquerade_entire_domain)dnl

- Establecer el número máximo de destinatarios a 20

define(`confMAX_RCPTS_PER_MESSAGE', `20')dnl

- Posterior al cambio en el archivo de configuración es necesario compilar el archivo con el siguiente comando:

cd /etc/mail/
m4 sendmail.mc > sendmail.cf

3.3.6.2.4 Configuración de Dovecot

El archivo de configuración se encuentra en la ruta /etc/dovecot.conf, se debe habilitar los servicios POP e IMAP.

protocols = imap pop3

3.3.6.2.4.1 Manejo del servicio

Inicio del servicio:	service dovecot start
Reiniciar el servicio:	service dovecot restart
Detener el servicio:	service dovecot stop
Estado del servicio:	service dovecot status

3.3.6.2.5 MailScanner

La implementación de MailScanner tiene por objetivo el control de virus y el spam de todos los correos electrónicos que son enviados hacia y desde el dominio proteco.coasin.com, los correos serán analizados por MailScanner en donde se utilizarán 3 herramientas primordialmente: el antivirus clamav, la herramienta antispam llamada spamassasin, y el MTA sendmail.

3.3.6.2.5.1 Instalación

La última versión de MailScanner se puede obtener de la página del proyecto en la sección de descargas:
http://www.mailscanner.info/downloads.html

Es necesaria la instalación de las dependencias para la correcta instalación de MailScanner:

yum –y install rpm-build gcc

Posterior a la instalación de paquetes necesarios para la instalación, descomprimir el archivo tar.gz descargado, ingresar a la carpeta descomprimida y ejecutar el script para instalación:

./install.sh

Al terminar la instalación el servicio podrá ser utilizado, para esto el servido de sendmail debe estar apagado ya que este es manejado directamente por MailScanner el cual será iniciado y configurado para que arranque con el inicio del sistema.

service sendmail stop
chkconfig sendmail off
service MailSScanner start
chkconfig MailScanner on

3.3.6.2.5.2 Configuración

El archivo de configuración de MailScanner se encuentra en la ruta:

/etc/MailScanner/MailScanner.conf

La configuración es la siguiente:

- Colocar los mensajes de detección de MailScanner a español.

  %report-dir% = /etc/MailScanner/reports/es

- Definir el nombre de la organización, nombre completo de la compañía, y su sitio Web

  %org-name% = Proteco-Coasin
  %org-long-name% = Proteco-Coasin S.A.
  %web-site% = www.proteco-coasin.com.ec

- Definir el antivirus a utilizar

  Virus Scanners = clamav

- Activar el uso de SpamAssasin y definir la calificación para etiquetar o no el correo masivo no deseado.

  Use SpamAssassin = yes
  Required SpamAssassin Score =3.9
  High SpamAssassin Score = 6
- Reenvío del correo calificado como spam a una cuenta de correo spam@proteco-coasin.com ,creada explícitamente para ésto:

  Spam Actions = store forward spam@proteco-coasin.com

- Eliminar el correo si la calificación iguala o sobrepasa el valor determinado en el parámetro High Scoring Spam Actions

  High Scoring Spam Actions = delete

- Posterior a los cambios realizados en necesario el reinicio de MailScanner con el siguiente comando:

  service MailSScanner restart

3.3.7 Servidor de archivos

El servidor de archivos lo manejará Samba mediante el protocolo SMB. Cada departamento en la empresa tendrá unidades de red centralizadas en donde podrán compartir información y archivos de gran tamaño, cada unidad de red tendrá permisos específicos de lectura y escritura para cada cliente en cada unidad de red.

La integración de Samba con un controlador de dominio mediante Winbind facilitará el acceso a los usuarios, manteniendo un control y la confidencialidad de la información

3.3.7.1 Samba

SAMBA es un conjunto de programas, originalmente creados por Andrew Tridgell y actualmente mantenidos por The SAMBA Team, bajo la Licencia Pública General GNU, y que implementan en sistemas basados sobre UNIX® el protocolo **SMB**. Sirve como reemplazo total para Windows® NT, Warp®, NFS® o servidores Netware®.

3.3.7.2 Instalación a través de yum

yum –y install samba samba-client samba-common

3.3.7.3 Archivos de configuración

El archivo de configuración de Samba se encuentra en la ruta:

/etc/samba/smb.conf

El archivo de configuración de LDAP se encuentra en la ruta:

/etc/ldap.conf

El archivo de configuración de NSS se encuentra en la ruta:

/etc/nsswitch.conf

El archivo de configuración de PAM se encuentra en la ruta:

/etc/pam.d/system-auth-ac

El archivo de configuración de Kerberos se encuentra en la ruta:

/etc/krb5.conf

3.3.7.4 Manejo del servicio

Manejo del servicio Samba:

service smb start	Inicio del servicio
service smb stop	Detener el servicio
service smb status	Estado del servicio

Manejo del servicio winbind

service winbind start	Inicio del servicio
service winbind stop	Detener el servicio
service winbind status	Estado del servicio

3.3.7.5 Implementación

Para la implementación del servidor Samba y la integración con un servidor Active Directory de Microsoft, al cliente Linux se lo configura como cliente de cuentas mediante la biblioteca NSS y cliente de autenticación mediante la biblioteca PAM de los controladores de dominio a través del protocolo LDAP.

Los servidores Windows utilizan Kerberos para la autenticación de los usuarios, por este motivo se utilizará la biblioteca PAM para que realice la autenticación mediante la utilización de Kerberos.

3.3.7.5.1 Configuración e Integración con Domain Controler de Microsoft Windows Server

3.3.7.5.1.1 Configuración de LDAP

Se comenzó con la configuración de LDAP, el archivo de configuración completo se encuentra en el ANEXO 10.

Se ingresó al archivo de configuración con el siguiente comando:

vi /etc/ldap.conf

Los parámetros configurados son los siguientes:

- Indicar la dirección del Servidor de Dominio

  host 192.168.3.206

- Especificar el nombre completo de la base de búsqueda, en este caso el dominio es proteco.local

  base dc=proteco,dc=local

- Establecer el identificador uniforme de recurso es una alternativa de identificar al servidor LDAP.

  uri ldap://dcp.proteco.local/

- Especificar el usuario de Active Directory con el que se realizarán consultas desde Linux, el usuario es Linux, pertenece a la Unidad organizativa TECNOLOGIA, en el dominio proteco.local

  binddn cn=linux,ou=TECNOLOGIA,dc=proteco,dc=local

  Especificar la clave del usuario que realizará las consultas en el servidor de dominio.

  bindpw gl*2012

- Especificar el tiempo límite para realizar una consulta

  timelimit 120
  bind_timelimit 120
  idle_timelimit 3600

- Especificar en qué contenedores se ubican las cuentas de usuario y grupo

  nss_base_passwd dc=proteco,dc=local?sub
  nss_base_shadow dc=proteco,dc=local?sub
  nss_base_group dc=proteco,dc=local?sub

- Especificar la adecuada asociación de los atributos de las cuentas de usuario y grupo a sus correspondientes del Directorio Activo

  nss_map_objectclass posixAccount User
  nss_map_objectclass shadowAccount User
  nss_map_objectclass posixGroup Group
  nss_map_attribute uid sAMAccountName
  nss_map_attribute uidNumber uidNumber
  nss_map_attribute gidNumber gidNumber
  nss_map_attribute loginShell loginShell
  nss_map_attribute uniqueMember member
  nss_map_attribute homeDirectory unixHomeDirectory
  nss_initgroups_ignoreusers
  root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mailman,nscd,gdm

- Configurar PAM ara que sea compatible con el servicio de Active Directory

  pam_login_attribute msSFU30Name
  pam_filter objectclass=User
  pam_password md5

- No utilizar SSL

  ssl no

3.3.7.5.1.2 Configuración de NSS

Se ingresó al archivo de configuración con el siguiente comando:

vi /etc/nsswitch.conf

El archivo de configuración completo se encuentra en el ANEXO 11, los parámetros configurados son:

- Especificar de donde leer la lista de usuarios, contraseñas y grupos.

```
passwd:     files winbind
shadow:    files
group:       files winbind
```

3.3.7.5.1.3 Configuración de PAM

Para la configuración de PAM se utilizó la herramienta authconfig que configura automáticamente los 4 módulos presentes en el archivo de configuración, auth, account, password, y session para utilizar winbind como alternativa. El archivo de configuración se encuentra en la siguiente ruta:
vi /etc/pam.d/system-auth-ac

El archivo de configuración completo se encuentra en el ANEXO 12, los parámetros configurados son:

```
auth sufficient /lib/security/$ISA/pam_winbind.so
auth sufficient /lib/security/$ISA/pam_unix.so nullok_secure use_first_pass
auth required   /lib/security/$ISA/pam_deny.so

account sufficient /lib/security/$ISA/pam_winbind.so
account required   /lib/security/$ISA/pam_unix.so

password requisite  /lib/security/$ISA/pam_cracklib.so retry=3
password sufficient /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
password required   /lib/security/$ISA/pam_deny.so

session  required   /lib/security/$ISA/pam_mkhomedir.so skel=/etc/skel umask=0077
session  required   /lib/security/$ISA/pam_limits.so
session  required   /lib/security/$ISA/pam_unix.so
```

3.3.7.5.1.4 Configuración de Kerberos

Se ingresó al archivo de configuración con el siguiente comando:

vi /etc/krb5.conf

El archivo de configuración completo se encuentra en el ANEXO 13, los parámetros configurados son:

- Especificar el lugar en donde se guardaran los log de logging

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log
```

- Especificar los valores que serán utilizados por las librerías de Kerberos V5.

```
[libdefaults]
 default_realm = PROTECO.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes
```

- Especificar donde encontrar los servidores Kerberos

```
[realms]
PROTECO.LOCAL = {
kdc = dcp.proteco.local
admin_server = dcp.proteco.local:749
  default_domain = proteco.local
 }
```

- Especificar las relaciones que se asignan los subdominios y nombres de dominio de Kerberos

```
[domain_realm]
 .proteco.local = PROTECO.LOCAL
 proteco.local = PROTECO.LOCAL
```

- Valores por defecto que serán utilizados por las aplicaciones de Kerberos V5

```
[appdefaults]
 pam = {
```

```
  debug = false
  ticket_lifetime = 36000
  renew_lifetime = 36000
  forwardable = true
  krb4_convert = false
}
```

3.3.7.5.1.5 Obtener y almacenar en cache el ticket inicial de concesión para el administrador

kinit gleon@PROTECO.LOCAL

3.3.7.5.1.6 Configuración de Samba

Se ingresó al archivo de configuración con el siguiente comando:

vi /etc/samba/smb.conf

El archivo de configuración completo se encuentra en el ANEXO 14, los parámetros configurados son:

- Especificar parámetros globales para el servidor samba

  [global]

- Especificar el nombre de NETBIOS con él se va a trabajar

  workgroup = PROTECO

- Especificar el nombre DNS de dominio con el que se va a trabajar, cuando samba trabaja con Active Directory este valor se muestra en mayúsculas.

  realm = PROTECO.LOCAL

- Especificar el Netbios del servidor local

  netbios name = server1

- Parámetro de carácter descriptivo, se lo utiliza para dar una descripción del servidor

  server string = Servidor de Archivos Proteco Coasin

- Especificar que el servidor se una al dominio de Windows como un miembro nativo de Active Directory.

  security = ads

- Especificar que redes o equipos tienen acceso al servidor.

  hosts allow = 192.168. 127. 10.

- Por defecto las impresoras del sistema son localizables para los clientes, al no ser el equipo un servidor de impresión y no tener impresoras configuradas en éste, la carga por defecto de impresoras es desactivada mediante el parámetro:

  load printers = no

- Mantener log separados por cada cliente que se conecta al servidor.

  log file = /var/log/samba/%m.log

- Controlar que los clientes Samba intenten utilizar una autenticación simple o protegida, SPENGO[11] utiliza un protocolo para determinar cuál mecanismo GSSAPI[12] está disponible.

  client use spnego = yes

[11] Simple and Protected GSSAPI Negotiation Mechanism
[12] Generic Security Services Application Program Interface

- Establecer el tamaño máximo de los archivos de log, este parámetro se especifica en kilobytes, Samba periódicamente revisa el tamaño de los archivos de log, y de ser necesario los renombra para así mantener un histórico de los sucesos.

  max log size = 50

- Establecer la cantidad de mensajes de depuración que se envían al archivo de registro que. La escala va de 0 a 3, en donde 0 es ninguno y 3 es considerable, el valor por defecto es 1.

  log level = 1

- Especificar el nombre del servidor de Dominio Activo de Windows.

  password server = DCP.PROTECO.LOCAL

- Especificar el rango de UID[13] de usuario que se reservan para asociar usuarios UNIX con SID de usuarios Windows. Este rango de UID de usuarios no debería tener usuarios locales o NIS o pueden surgir conflictos.
  idmap uid = 10000 – 20000

- Especificar el rango de GID[14] de usuario que se reservan para asociar usuarios UNIX con GID de usuarios Windows. Este rango de GID de usuarios no debería tener usuarios locales o NIS o pueden surgir conflictos.

  idmap gid = 10000 – 20000

- Permitir la enumeración de usuarios y grupos mediante el grupo de llamadas al sistema getpwent[15], setpwent [16]y endpwent[17].
  winbind enum users = yes
  winbind enum groups = yes

[13] UID.-. User identifier. En sistemas UNIX los usuarios son identificados por un identificador de usuario normalmente abreviado User ID.
[14] GID.-. Group identifier. En sistemas Unix multiples usuarios pueden ser categorizados en grupos, normalmente abreviado Group ID.
[15] La Función getpwent() devuelve un puntero a una estructura que contiene los campos de una línea de /etc/passwd. La primera vez que se la llama devuelve la primera entrada; a partir de ahí, devuelve las entradas sucesivas.
[16] La función setpwent() rebobina el indicador de posición del fichero para ponerlo apuntando al principio de /etc/passwd.
[17] La función endpwent() cierra el fichero /etc/passwd.

- Especificar el tiempo en segundos que el demonio Windbind mantendrá en caché la información del usuario y contraseña antes de consultar al servidor de dominio.

  winbind cache time = 10

- Permitir grupos anidados

  winbind nested groups = yes

- Incluir el prefijo del dominio al iniciar sesión.

  winbind use default domain = no

- Especificar el directorio personal del usuario.

  template homedir = /home/%U

- Especificar el Shell de login

  template shell = /bin/bash

- Utilizar DNS si no se encuentra en nombre mediante el servidor Samba WINS.

  dns proxy = no

- Samba se encuentra integrado un dominio de Active Directory por lo cual no es un controlador de dominio.

  domain master = no

- Establecer si samba es o no el examinador principal de listas para su grupo de trabajo o dominio, es recomendable utilizar este parámetro conjuntamente con domain master = yes.

  preferred master = no

Configuración de carpetas compartidas.

3.3.7.5.1.7 Comprobar los parámetros de configuración de Samba

testparm /etc/samba/smb.conf

3.3.7.5.1.8 Integrar el equipo al dominio de Windows mediante un usuario con permisos administrativos

net ads join -U gleon

3.3.7.5.1.9 Enlistar los usuarios de Active Directory, comprobando que el servidor está unido al dominio de Windows.

wbinfo –u

3.3.7.5.1.10 Enlistar los grupos de Active Directory, comprobando que el servidor está unido al dominio de Windows

wbinfo -g

3.3.8 Servidor WEB

El servidor web lo maneja el servidor Apache, instalado en Centos 5

3.3.8.1 Servidor Web Apache

3.3.8.2 Instalación a través de yum

yum –y install httpd

3.3.8.3 Archivo de configuración

El archivo de configuración principal de Apache httpd.conf se encuentra en la ruta

/etc/httpd/conf/httpd.conf

La carpeta donde se encuentran los ficheros de configuración de los dominios virtuales está en la siguiente ruta:

/etc/httpd/conf.d/

3.3.8.4 Manejo del servicio

Inicio del servicio: service httpd start
Recargar el servicio: service httpd reload
Reiniciar el servicio: service httpd restart
Detener el servicio: service httpd stop

3.3.8.5 Implementación

El servidor WEB principalmente cubrirá las necesidades de la intranet de la empresa, básicamente se trabajará con 2 dominios virtuales internos, los parámetros cambiados en el archivo de configuración para lograr esta configuración fueron los siguientes:

3.3.8.5.1 Ingresar al archivo de configuración con el editor vi:

vi /etc/httpd/conf/httpd.conf

3.3.8.5.2 Indicar la dirección IP y puerto por dónde escuchan los servidores virtuales.

NameVirtualHost 192.168.3.218:80

3.3.8.5.3 Configuración dominio Virtual intranet.proteco-coasin.com y software.proteco-coasin.com

Para que los usuarios puedan acceder al dominio se deben configurar correctamente los registros en el servidor DNS, los registros aumentados son los siguientes:
En el servidor DNS en la zona proteco-coasin.com en el archivo ubicado en /var/named/chroot/var/named/proteco-coasin.com.zone se añadió:

```
intranet        IN    A    192.168.3.218
software        IN    A    192.168.3.218
```

En el servidor DNS en la zonainversa 10.168.192.in-addr.arpa.zone en el archivo ubicado en /var/named/chroot/var/named/10.168.192.in-addr.arpa.zone se añadió:

```
218   IN    PTR   intranet.proteco-coasin.com
218   IN    PTR   software.proteco-coasin.com
```

En el archivo de configuración del servidor Apache se añadió para cada dominio:

```
<VirtualHost intranet.proteco-coasin.com:80>
   ServerAdmin guillermo.leon@proteco-coasin.com
   DocumentRoot /var/www/intranet.proteco-coasin.com
   ServerName intranet.proteco-coasin.com
   ErrorLog logs/intranet.proteco-coasin.com-error_log
   CustomLog logs/intranet.proteco-coasin.com-error_log common
</VirtualHost>
```

```
<VirtualHost software.proteco-coasin.com:80>
   ServerAdmin guillermo.leon@proteco-coasin.com
   DocumentRoot /var/www/software.proteco-coasin.com
```

```
    ServerName software.proteco-coasin.com
    ErrorLog logs/intranet.proteco-coasin.com-error_log
    CustomLog logs/intranet.proteco-coasin.com-error_log common
</VirtualHost>
```

En donde los parámetros:

ServerAdmin: especifica la dirección de correo a la que se deben enviar los problemas de uso del servidor Web

DocumentRoot: indicar doónde se almacenan los documentos del sitio WEB.

ServerName: especificar el nombre y el puerto que el servidor utiliza para identificarse.

ErrorLog: indica la ubicación del registro de errores en consultas.

CustomLog: especificar el fichero donde se anotan las peticiones hechas al servidor.

3.3.9 Servidor FTP

El servicio de FTP lo maneja el servidor VSFTP[18], actualmente es considerado unos de los servidores FTP más seguros y sencillos de administrar.

El servicio de FTP será utilizado por clientes externos e internos de la empresa, los cuales necesiten obtener o enviar información que por su contenido o tamaño no pueda ser enviada por correo electrónico, por exceder el tamaño de 14 MB configurado en el servidor Sendmail, por seguridad se encapsulará a los usuarios en su home para que no acceden a información de otros usuarios o configuraciones del servidor.

Para solventar en gran medida el problema de seguridad que presenta FTP al enviar la información desde el inicio de sesión y transferencia de archivos en texto plano, se utilizará FTPS[19] Explícito sobre TLS, donde el cliente realiza la conexión normal a través del puerto 21 y posterior se realiza la conexión TLS.

Al utilizar FTPS, se requiere el uso de clientes FTP que soporten FTPS sobre TLS como Filezilla, Winscp.

[18] VSFTP: Very Sure File Tranfer Protocol
[19] FTPS: (Explicit FTPS o FTPES) método recomendado por la RFC 4217

3.3.9.1 Instalación a través de yum

yum install vsftpd

3.3.9.2 Archivo de configuración

El archivo de configuración del servidor se encuentra en la siguiente ruta:

/etc/vsftpd/vsftpd.conf

El archivo en donde se listaran los usuarios a ser enjaulados se encuentra en la siguiente ruta:

/etc/vsftpd/chroot_list

3.3.9.3 Manejo del servicio

El servidor es manejado por el demonio VSFTPD

Inicio del servicio: service vsftpd start
Recargar el servicio: service vsftpd reload
Reiniciar el servicio: service vsftpd restart
Detener el servicio: service vsftpd stop

3.3.9.4 Implementación

Para la implementación del servidor FTP, se integró la máquina al servidor de Dominio Activo de Microsoft Windows con el procedimiento realizado para el servidor de archivos, descrito en capítulo 3 Implementación, subcapítulo 3.4.7 Servidor de archivos, numeral 3.4.7.5.1.

Además de la configuración descrita se editó el archivo de configuración /etc/pam.d/vsftpd indicando que VSFTP autenticada también por winbind.

3.3.9.4.1 Configuración /etc/pam.d/vsftpd

Para la edición del archivo se utilizó el editor de texto vi.

vi /etc/pam.d/vsftpd

El contenido del fichero es el siguiente:

```
#%PAM-1.0
session sufficient pam_winbind.so
auth sufficient pam_winbind.so
auth required pam_listfile.so item=user sense=deny file=/etc/vsftpd/ftpusers onerr=succeed
auth sufficient pam_shells.so debug
auth include system-auth
account sufficient winbind.so
account include system-auth
session include system-auth
session required pam_loginuid.so
```

3.3.9.4.2 Configuración /etc/vsftpd/vsftpd.conf

El archivo de configuración completo se encuentra en el ANEXO 15, los parámetros de configuración son los siguientes:

- No permitir usuarios Anonimos

  anonymous_enable=NO

- Permitir el ingreso a usuarios locales

  local_enable=YES

- Permitir que los usuarios tengan permisos de escritura:

  write_enable=YES

- Establecer el directorio home de los usuarios como jaula, los usuarios solo podrán tener acceso a su directorio home.

  chroot_list_enable=YES
  chroot_list_file=/etc/vsftpd/chroot_list

- Especificar rango arbitrario, de puertos para conexiones pasivas.

  pasv_min_port=35004
  pasv_max_port=35009

- Habilita el soporte de TLS/SSL

  ssl_enable=YES

- Deshabilitar o habilitar utilizar TLS/SSL con usuarios anónimos

  allow_anon_ssl=NO

- Obligar a utilizar TLS/SSL para todas las operaciones, es decir, transferencia de datos y autenticación de usuarios locales.

  force_local_data_ssl=YES
  force_local_logins_ssl=YES

- Especifciar TLSv1 sobre SSLv2, y SSLv3

  ssl_tlsv1=YES
  ssl_sslv2=NO
  ssl_sslv3=NO

- Epecificar las rutas del certificado y firma digital

  rsa_cert_file=/etc/pki/tls/certs/vsftpd.crt
  rsa_private_key_file=/etc/pki/tls/private/vsftpd.key

3.3.9.4.3 Fichero /etc/vsftpd/chroot_list

En el fichero se especifican los usuarios de enjaulamiento, por motivos de implemntación y pruebas se crearon 3 usuarios en Active Directory los cuales son parte de este fichero:

proteco\proyecto.peru
proteco\proyecto.ecuador
proteco\proyecto.argentina

Es necesario crear la carpeta en donde se guardará la información de cada usuario, se crearon las carpetas:

mkdir /home/proyecto.ecuador
mkdir /home/proyecto.peru
mkdir /home/proyecto.argentina

3.3.10 Servidor de respaldos

El servicio de respaldos los maneja la aplicación Backuppc, el servidor fue instalado sobre Ubuntu server versión 10.11.

3.3.10.1 Backuppc

Es un potente sistema de respaldos multiplataforma con una interface Web muy sencilla y manejable, permite hacer respaldos mediante SMB y SSH+rsync a clientes Linux, Unix y Windows.

Los respaldos de la información tanto de los servidores como equipos en red se realizarán mediante esta herramienta

3.3.10.2 Instalación a través de apt-get

apt-get install backuppc

3.3.10.3 Archivo de configuración

El archivo de configuración (ver ANEXO 16) se encuentra en la siguiente ubicación:
/etc/backuppc/config.pl

3.3.10.4 Manejo del servicio

Inicio del servicio: service backuppc start
Reiniciar el servicio: service backuppc restart
Detener el servicio: service backuppc stop

3.3.10.5 Implementación

Posterior a la instalación y resolución de dependencias, la configuración y manejo de equipos a respaldar se lo realizará mediante la interface Web.

Los parámetros cambiados en el archivo de configuración son los siguientes:

- Especificar el usuario administrador del sistema

  $Conf{CgiAdminUsers} = 'backuppc'

- Especificar el nombre del equipo anfitrión

  $Conf{ServerHost} = 'backup-server';

- Definir el URL de la herramienta de administración

  $Conf{CgiURL} = 'http://backup-server/backuppc/index.cgi'

- Definir el idioma de la herramienta de administración

  $Conf{Language} = 'es'

3.3.10.6 Cambio de contraseña de usuario backuppc

Para cambiar la contraseña del usuario administrador para acceder a la herramienta web utilizados:

htpasswd /etc/backuppc/htpasswd backuppc

3.3.10.7 Manejo de herramienta mediante interface WEB.

Para ingresar a la herramienta de configuración de backuppc, se puede utilizar un navegador WEB, como el internet Explorer, Firefox, Chorme, etc a la siguiente dirección:

http://192.168.3.217/backuppc/

Usar el usuario backuppc y la contraseña especificada en 3.4.9.6.

3.3.10.8 Respaldos de equipos Linux.

Se realizarán 2 tipos de respaldos, totales e incrementales.
Los respaldos totales se los realizará 1 vez cada 15 días y se guardará los 2 últimos respaldos totales realizados.

Los respaldos incrementales se los realizará cada 3 días y se guardarán los 5 últimos respaldos incrementales realizados.

3.3.10.8.1 Interface web de Backuppc

Para acceder a la interface gráfica del servidor backuppc se ingresa a la dirección IP del equipo donde se encuentra instalado el servidor, o a la dirección establecida en 3.4.9.5.

http://192.168.3.217/backuppc/

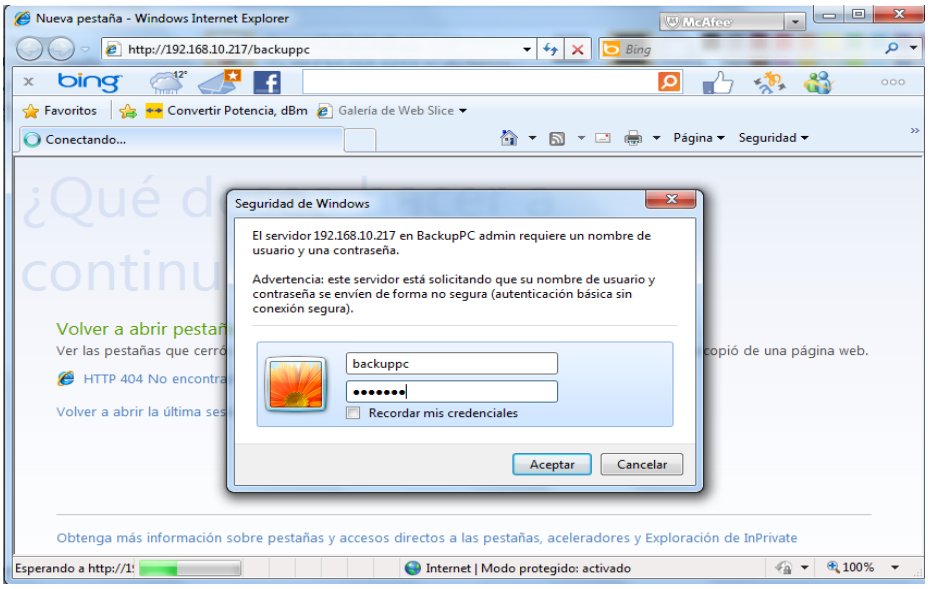


Ilustración 3-16 - Ingreso interface Web de Backuppc

Se debe utilizar el usuario y contraseña especificados en 3.4.9.6.

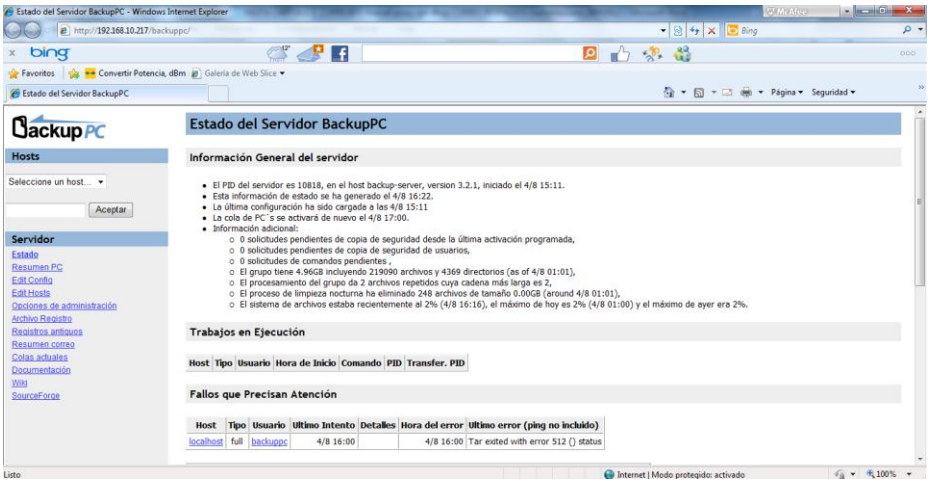


Ilustración 3-17 - Interface Web Servidor Backuppc

CAPÍTULO IV

4.1 PRUEBAS DE FUNCIONAMIENTO

4.1.1 Introducción

Las pruebas que se llevaron a cabo para comprobar el correcto estado y funcionamiento de los servicios implementado, servirá en gran medida a conocer más a fondo su funcionamiento, se realizarán pruebas prácticas y explicativas las cuales aclararán cualquier duda sobre la operatividad de los servicios.

4.1.2 Comprobación operatividad del Firewall

4.1.2.1 Bloqueo Intento de conexiones externas.

Para esta prueba utilizaremos el servicio SSH que fue configurado para trabajar en el puerto 1983, como una medida de seguridad no es posible hacer login directamente como usuario root, primero se debe hacer login con el usuario especificado en el parámetro AllowUsers en el archivo de configuración de SSH.

4.1.2.1.1 Escenario 1

Una persona externa a la red intenta intenta conectarse a vía SSH al servidor firewall.

El firewall fue configurado para permitir conexiones vía SSH, este servicio fue configurado en el puerto 1983,

Por motivos de prueba se guardan los logs de conexiones al puerto SSH, agregando la línea resaltada en el archivo de configuración del firewall.

```
# ssh
$IPTABLES -A INPUT -p tcp --dport 1983 -j LOG
$IPTABLES -A INPUT -p tcp --dport 1983 -j ACCEPT
```

La prueba de conexión se realizó desde un terminal DOS con el comando que se muestra a continuación:

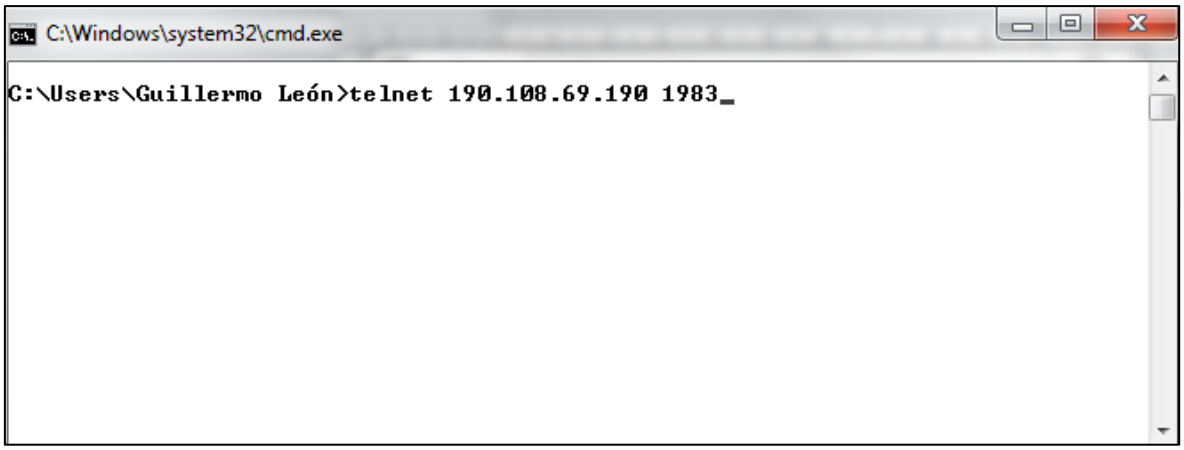


Ilustración 4-1 - Prueba de Firewall mediante Telnet

La conexión fue exitosa como se muestra en la siguiente figura:

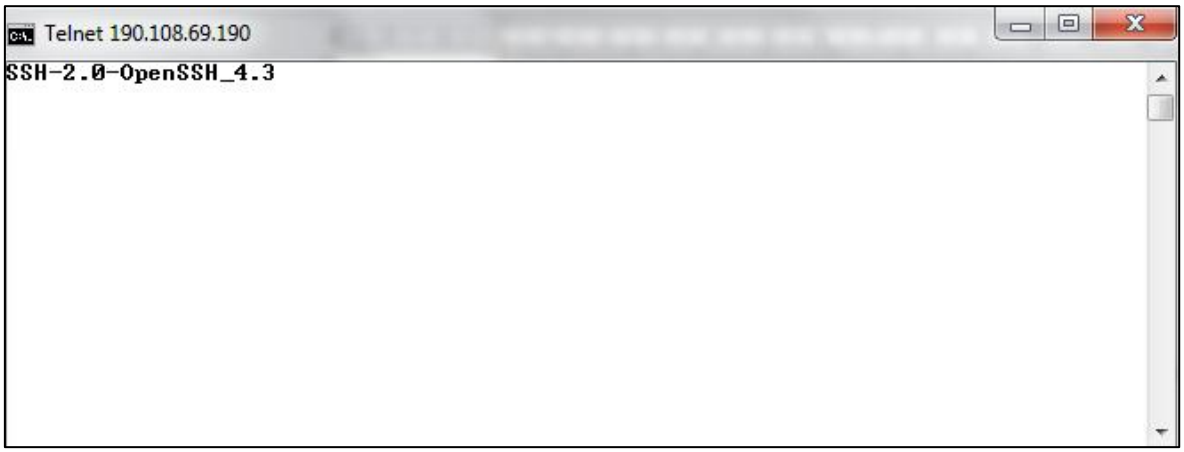


Ilustración 4-2 - Conexión SSH exitosa

El log es guardado en el archivo /var/log/messages del servidor Firewall, para el seguimiento se utilizó el siguiente comando:

tail -f /var/log/messages | grep DPT:1983

Se obtuvo el siguiente resultado:

Apr 15 21:38:06 firewall kernel: IN=eth0 OUT= MAC=00:11:43:58:88:14:00:30:da:51:43:80:08:00 SRC=186.42.219.245 DST=190.108.69.190 LEN=52 TOS=0x00 PREC=0x00 TTL=118 ID=32647 DF PROTO=TCP SPT=25629 DPT=1983 WINDOW=8192 RES=0x00 SYN URGP=0

Se puede observar en la salida del comando que la petición la realiza una máquina con dirección IP 186.42.219.245, a la interface ETH0 del servidor Firewall que tiene una dirección IP 190.108.69.190 al puerto 1983.

Para comprobar el funcionamiento de las reglas descritas en el firewall, se negarán las peticiones al puerto 1983, y estas serán guardas en logs del sistema, cambiando lo siguiente en el archivo de configuración del Firewall:

```
# ssh
$IPTABLES -A INPUT -p tcp --dport 1983 -j LOG
$IPTABLES -A INPUT -p tcp --dport 1983 –j DROP
```

La prueba de conexión se realizó desde un terminal DOS con el comando que se muestra a continuación:

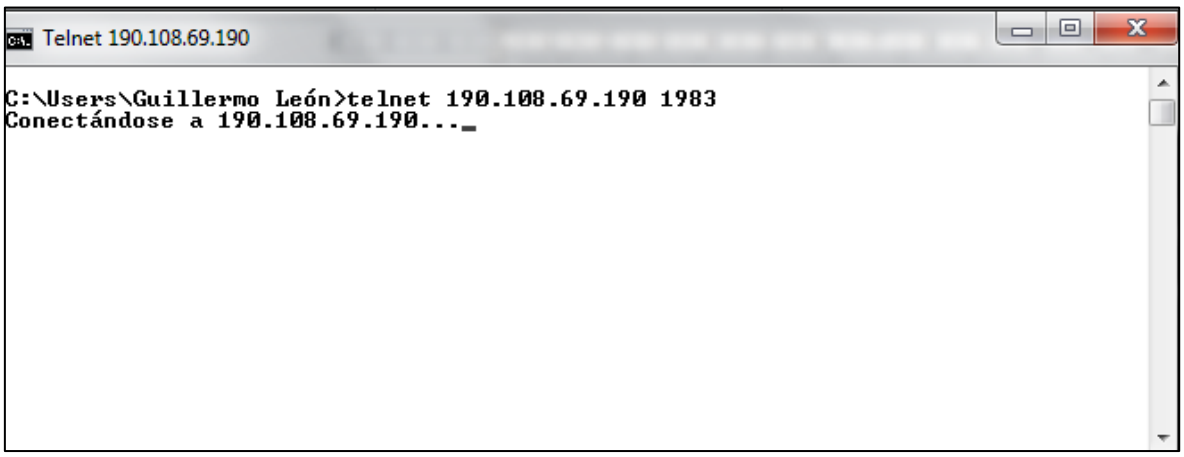


Ilustración 4-3 - Intento de conexión Telnet puerto 1983

El resultado de la petición fue el siguiente: “No se puede abrir la conexión al host, en puerto 1983: Error en la conexión”, como se puede observar en el siguiente gráfico.

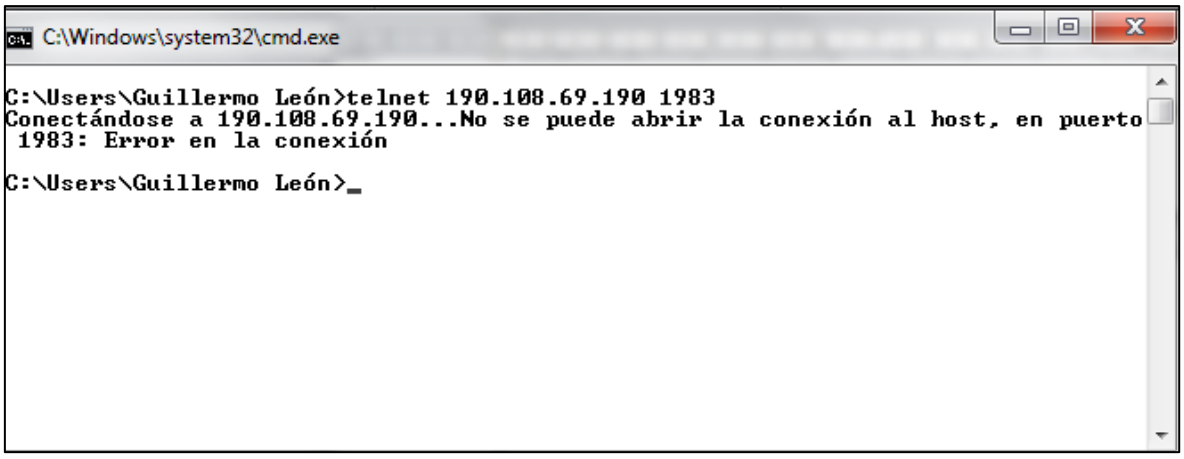


Ilustración 4-4 - Conexión a puerto 1983 fallida

4.1.3 Comprobación operatividad servidor proxy caché

Todo el tráfico web de la red local pasa por el proxy caché squid, para comprobar su funcionamiento se realizarán 3 pruebas en donde:

- Se demostrará que el tráfico de la red local cruza por el proxy.

  El archivo de log de acceso de Squid se encuentra en: /var/log/squid/access, para observar las peticiones que está realizando un cliente se utilizará el siguiente comando:

  tail -f /var/log/squid/access.log | grep 192.168.3.205

  En donde se observa la navegación de la máquina con la dirección IP 192.168.3.205; el resultado obtenido:

  1334550990.658 209 192.168.3.205 TCP_MISS/200 704 GET http://metrics.polycom.com/b/ss/polycomsupport/1/H.22.1/s94703072749063? - DIRECT/66.235.143.118 image/gif

  1334550994.314 3868 192.168.3.205 TCP_HIT/200 465989 GET http://supportdocs.polycom.com/PolycomService/support/global/documents/support/user/products/video/hdxtouch_qt.pdf - NONE/- application/pdf

  1334550998.517 132 192.168.3.205 TCP_MISS/200 649 GET http://pt200206.unica.com/ntpagetag.gif? - DIRECT/184.30.34.24 image/gif

1334550998.659 365 192.168.3.205 TCP_MISS/503 1493 GET http://ehg-interwoven.hitbox.com/HG? - DIRECT/205.216.15.71 text/html

1334551002.793 4134 192.168.3.205 TCP_HIT/200 2494341 GET http://supportdocs.polycom.com/PolycomService/support/global/documents/support/user/products/video/hdxtouch_ug.pdf - NONE/- application/pdf

1334551007.933 155 192.168.3.205 TCP_MISS/200 649 GET http://pt200206.unica.com/ntpagetag.gif? - DIRECT/184.30.34.24 image/gif
1334551008.006 318 192.168.3.205 TCP_MISS/503 1493 GET http://ehg-interwoven.hitbox.com/HG? - DIRECT/205.216.15.71 text/html

1334551008.045 215 192.168.3.205 TCP_MISS/200 703 GET http://metrics.polycom.com/b/ss/polycomsupport/1/H.22.1/s94164461310908? - DIRECT/66.235.143.121 image/gif

1334551014.449 6631 192.168.3.205 TCP_HIT/200 2494341 GET http://supportdocs.polycom.com/PolycomService/support/global/documents/support/user/products/video/hdxtouch_ug.pdf - NONE/- application/pdf

Para analizar de una forma más sencilla y clara los log de Squid se utilizará un sistema de reportes llamado SARG[20], el cual utiliza las bitácoras de Squid para generar reportes detallados de la actividad de los equipos y usuarios de la red local.

- Se demostrará el funcionamiento de las reglas de control de acceso

Se crearon listas de control de acceso para permitir o no la navegación de los usuarios a ciertos sitios Web.

Para comprobar que las listas están funcionando de manera correcta se utilizará la máquina con dirección IP 192.168.3.205 a la cual no se le permitirá el acceso a redes sociales.

Actualmente esta máquina se encuentra en la lista de control de acceso /etc/squid/reglas/sin_restriccion, esta lista de acceso permite la navegación sin ningún tipo de bloqueo al usuario:

[20] SARG .- Squid Analysis Report Generator

Ilustración 4-5 - Acceso a redes sociales

Para probar el funcionamiento de las listas de acceso se debe cambiar a la dirección IP de esta máquina a una lista con restricción a redes sociales:

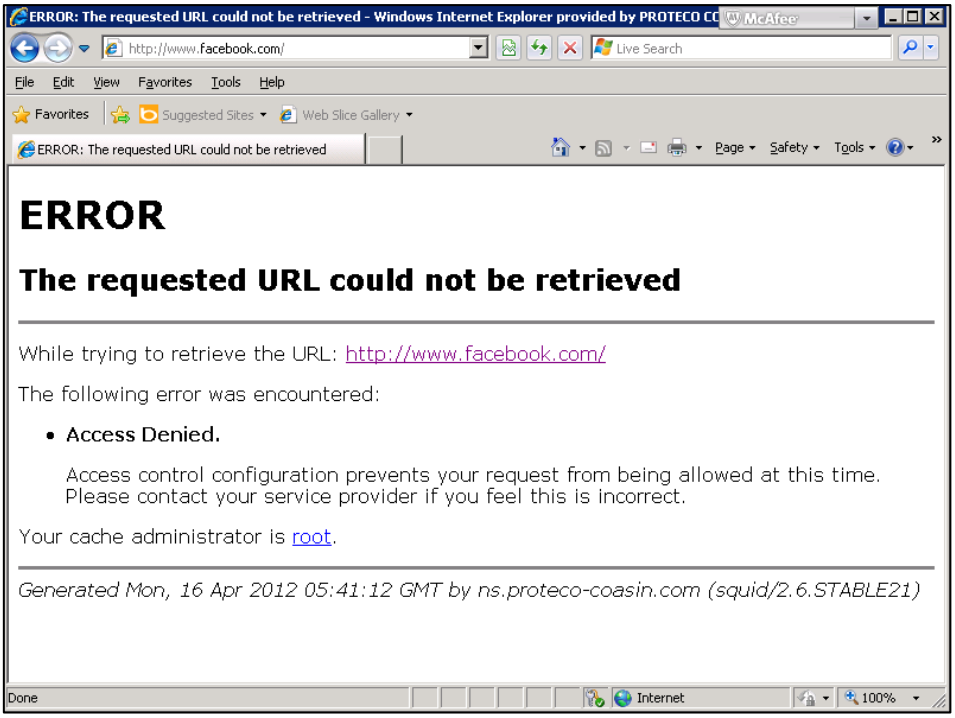


Ilustración 4-6 - Restricción a redes sociales

4.1.4 Comprobación operatividad de VPN

Las pruebas de operatividad de la VPN, se realizarán desde una red externa a la empresa, desde la cual se establecerá la conexión y comprobará el funcionamiento mediante la conectividad a un equipo de la red interna.

La configuración de red de la máquina remota es la siguiente:

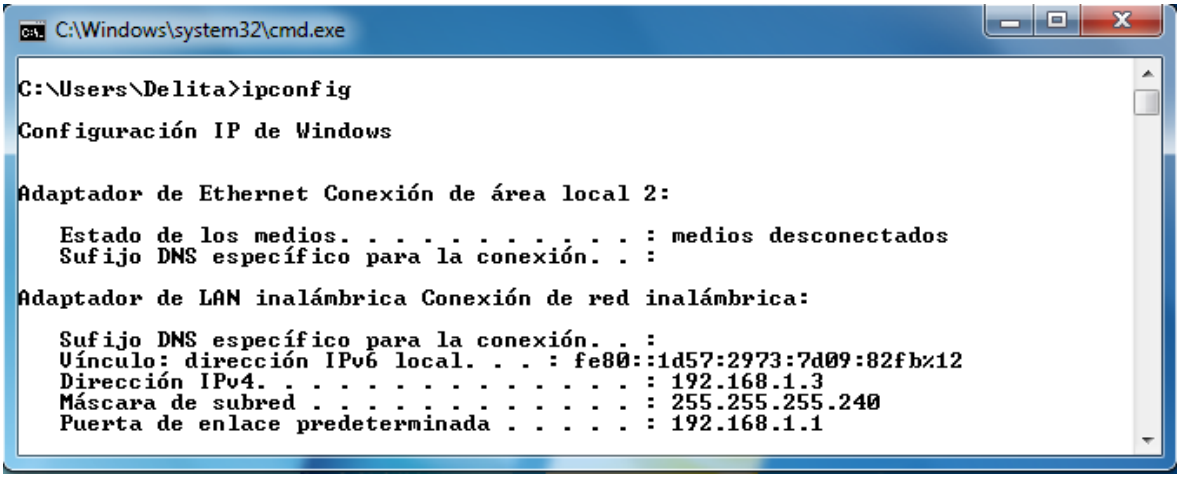


Ilustración 4-7 - Configuración de red de máquina remota

Se realizó un ping a una dirección IP interna de la empresa sin tener éxito:

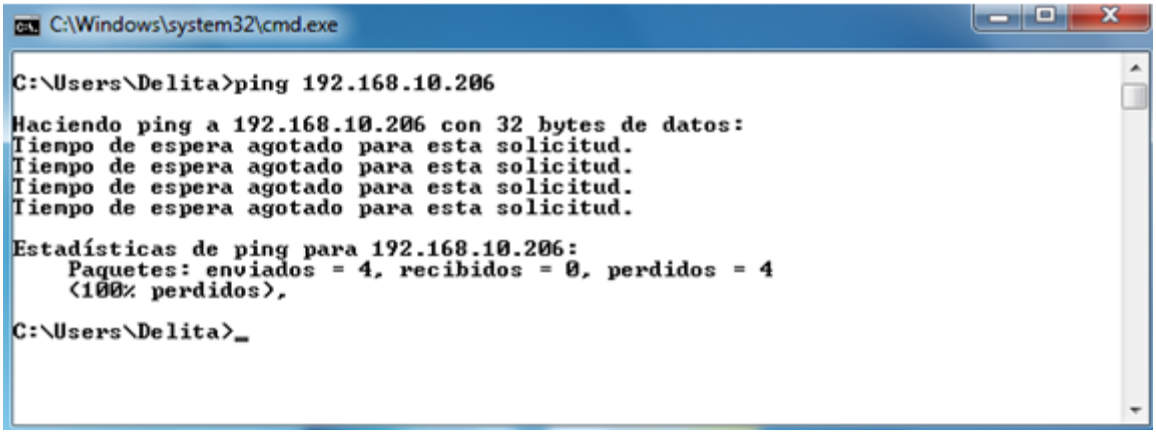


Ilustración 4-8 - Ping a dirección interna de la empresa sin éxito

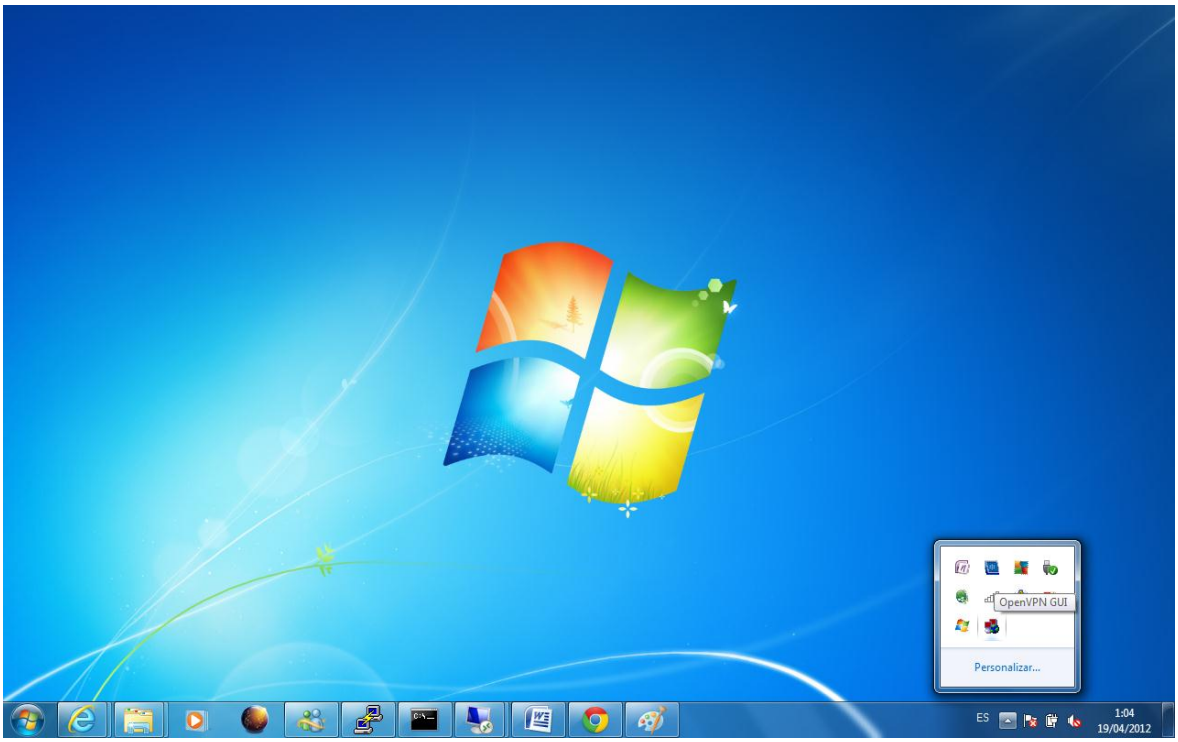


Ilustración 4-9 -Conexión a la red empresarial mediante OPENVPN

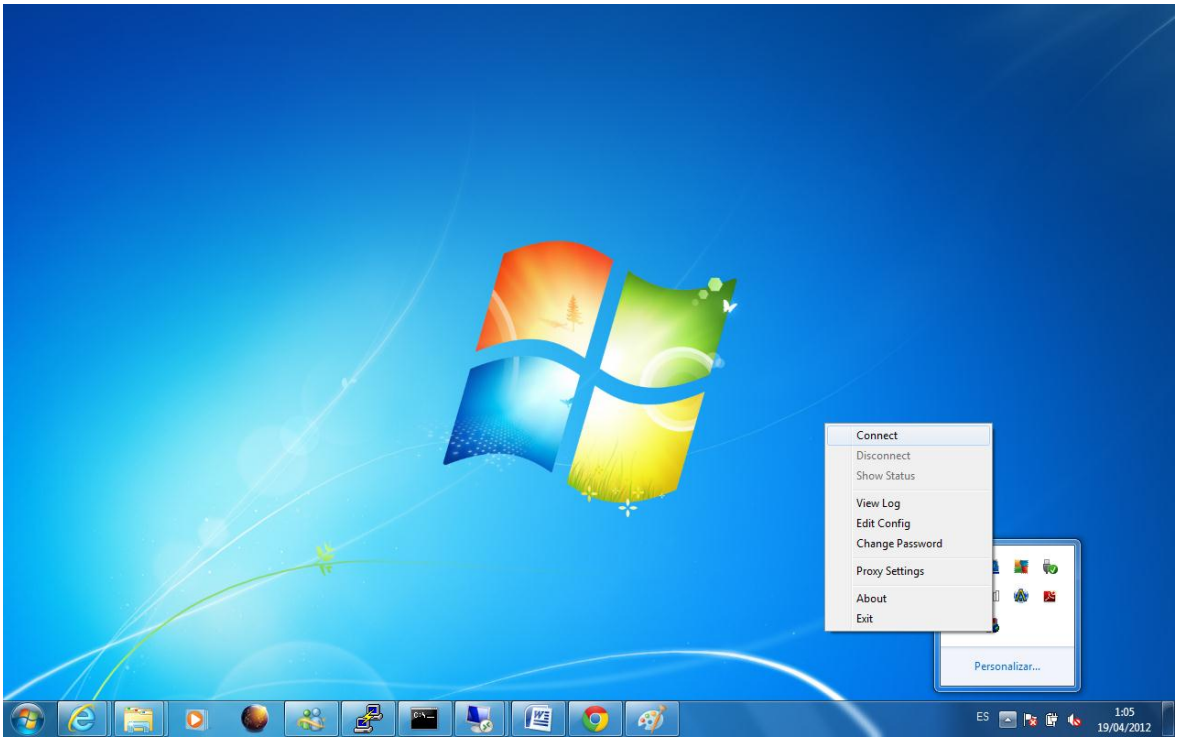


Ilustración 4-10 - Conexión a la red empresarial mediante OPENVPN

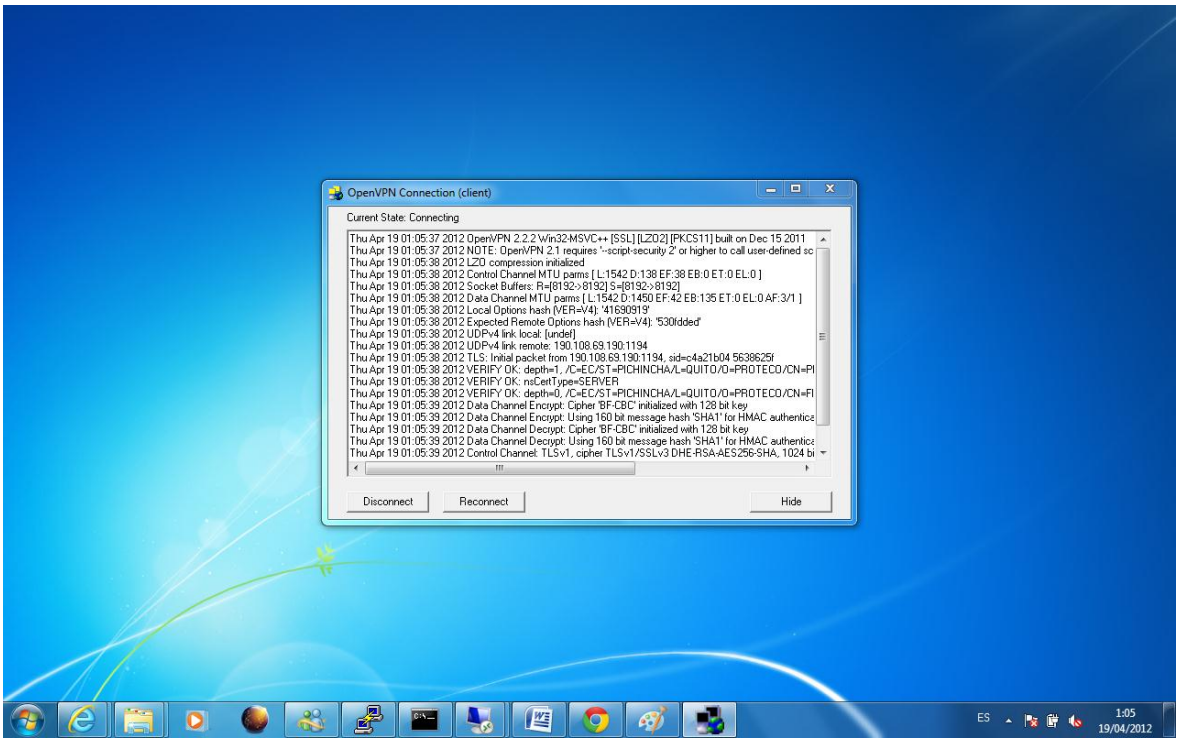


Ilustración 4-11 - Estado de conexión a red empresarial mediante OPENVPN

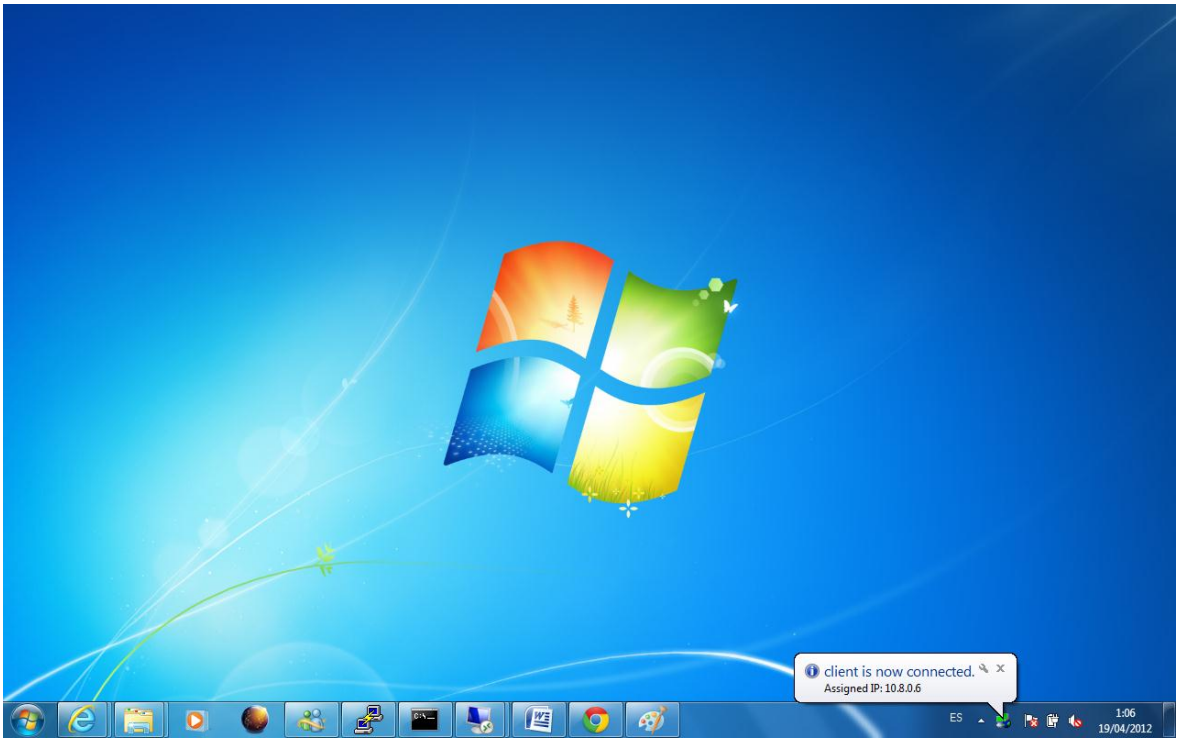


Ilustración 4-12 - Asignación de dirección IP

La configuración IP actual del cliente remoto es:

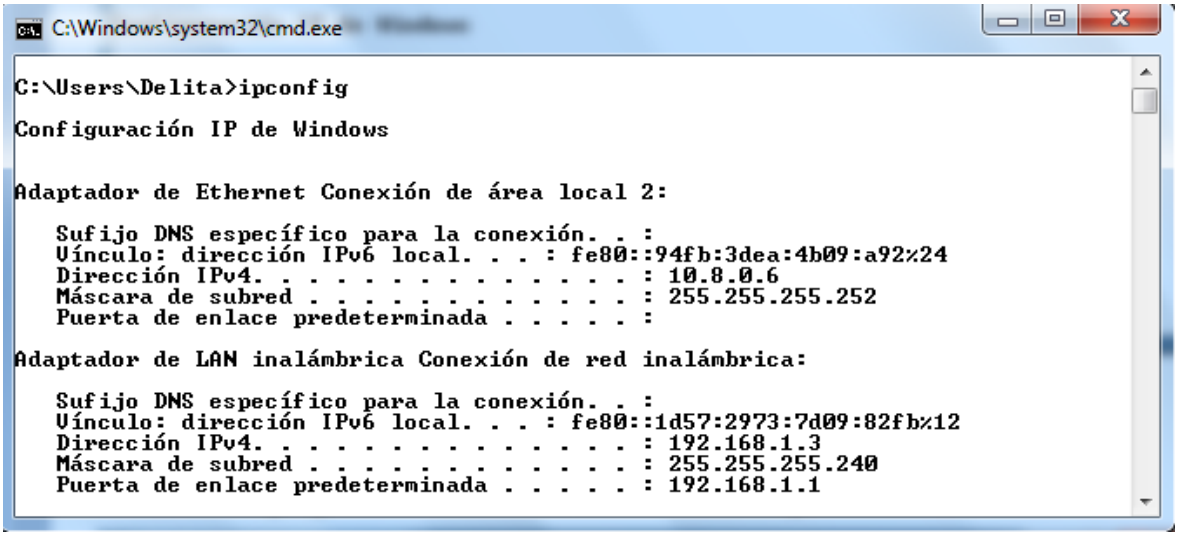


Ilustración 4-13 -Configuración IP del cliente remoto

Para comprobar la conectividad con la red interna se realizó un ping a la máquina con la dirección IP: 192.168.3.206

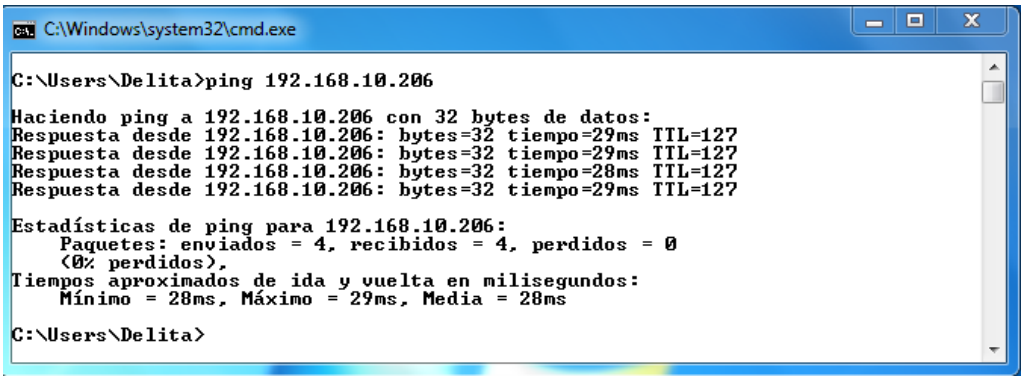


Ilustración 4-14 - Conectividad con máquina en la red interna.

4.1.5 Comprobación operatividad servidor DHCP

Para comprobar el funcionamiento del servidor DHCP en la red, se listó la configuración del equipo con dirección IP 192.168.3.205, como se mencionó en el capítulo 3, subcapítulo 3.1 Implementación, numeral 3.4.4.4, por motivos de seguridad se reservará a cada equipo mediante su dirección MAC una dirección IP determinada.

En este caso la reserva se realizó de la siguiente manera:

```
host pcuio-storage {
        option host-name "PCUIO-STORAGE";
        hardware ethernet 78:AC:C0:9C:6B:B6;
        fixed-address 192.168.3.205;
        }
```

Al listar la configuración del equipo cliente se puede observar que opción de DHCP está activa y que la dirección del servidor DHCP es la 192.168.3.218.

Los parámetros de red como Dirección IP, Gateway y DNS son los especificados en la configuración global del servidor DHCP.

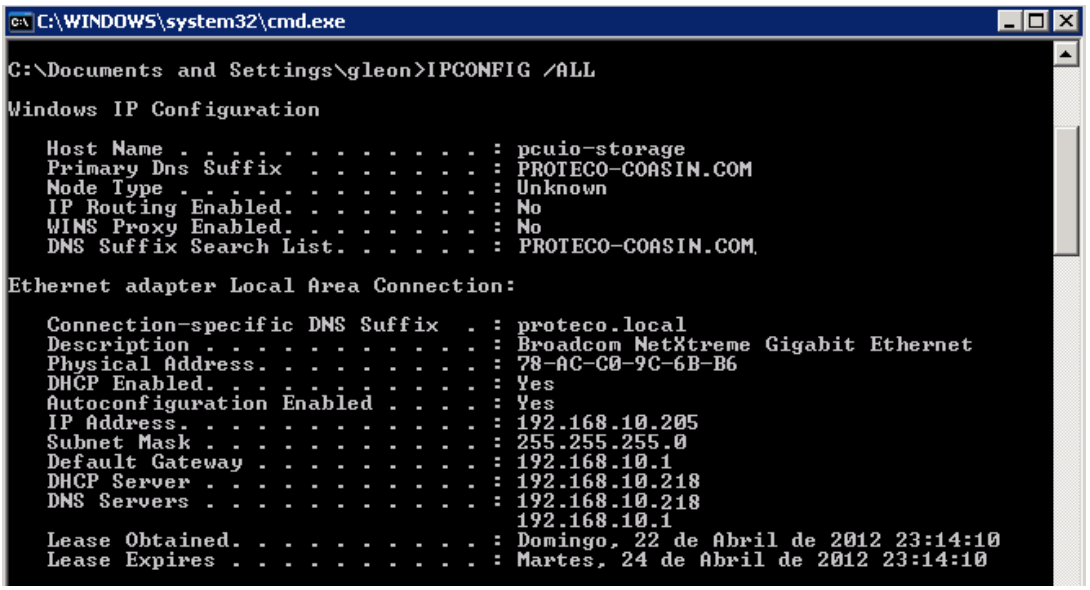


Ilustración 4-15 - Configuración IP de servidor PCUIO-STORAGE

4.1.6 Comprobación operatividad DNS

Para comprobar el funcionamiento del servidor DNS se utilizará conjuntamente el servidor WEB y el host desde un cliente Linux.

- El servidor web se encuentra en la dirección 192.168.3.217, se accede mediante la dirección http://intranet.proteco-coasin.com.

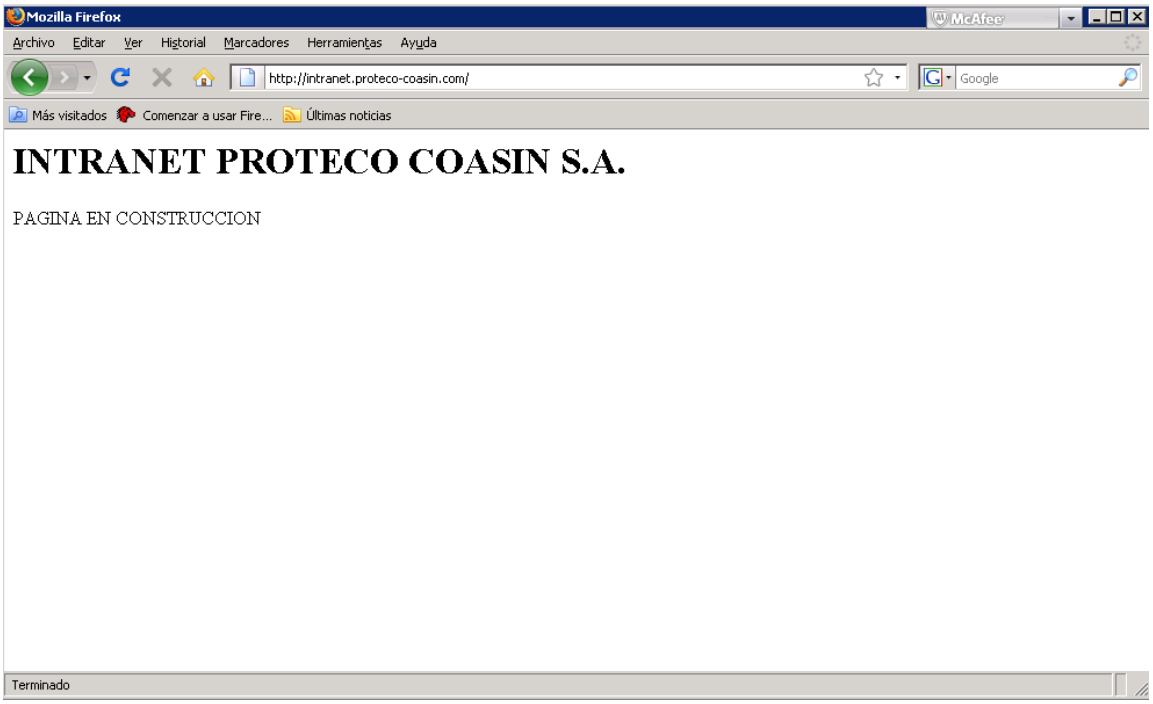


Ilustración 4-16 - Página en construcción Proteco Coasin S.A.

Con el comando host desde un cliente Linux se podrá consultar qué equipo es el que está manejando los DNS del dominio consultado.

En la siguiente gráfica se consulta al dominio proteco-coasin.com, el cual es manejado por server1.proteco.coasin.com.ec

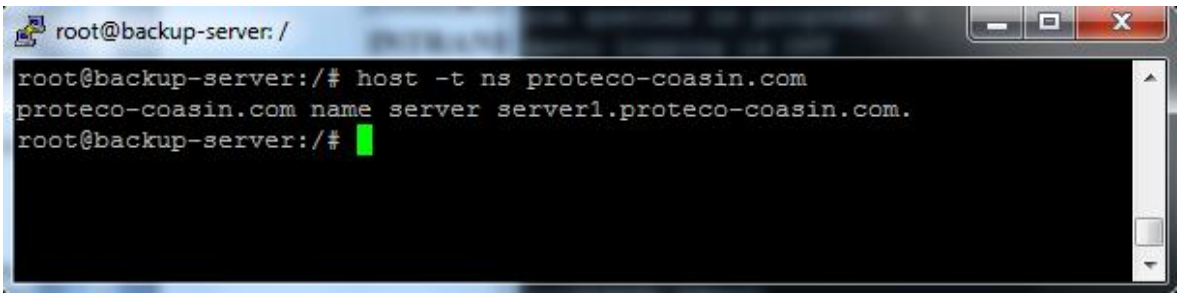


Ilustración 4-17 - Consulta del servidor que maneja el dominio PROTECO-COASIN.COM

Como se puede observar el equipo server1.proteco-coasin.com tiene la dirección IP 192.168.3.218 la cual fue asignada al servidor DNS.

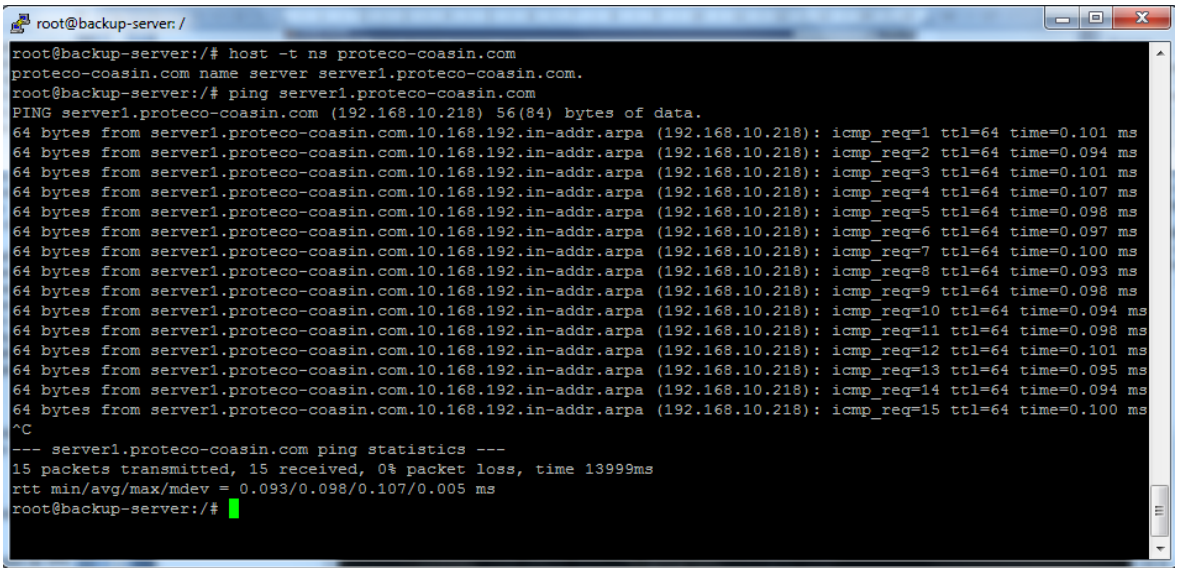


Ilustración 4-18 - Verificación de dirección IP de server1.proteco-coasin.com

4.1.7 Comprobación operatividad Correo Electrónico

Para la comprobación de operatividad del servicio de correo electrónico se lo realizará enviando y recibiendo correo desde y hacia diferentes dominios mediante el cliente de correo electrónico Microsoft Outlook y el webmail.

4.1.7.1 Configuración en cliente de correo electrónico.

En el cliente de correo electrónico del usuario se configurará una nueva cuenta de correo electrónico, mediante el protocolo de la oficina de correo POP3 o IMAP.

El dominio proteco-coasin.com está siendo manejado por el servidor mail.proteco-coasin.com el cual tiene la dirección IP pública 190.108.69.190.

Los datos para la configuración son los siguientes:

Dirección de correo electrónico: guillermo.leon@proteco-coasin.com
Servidor de correo entrante: mail.proteco-coasin.com
Servidor de correo Saliente: mail.proteco-coasin.com
Usuario: guillermo.leon
Password: *guillermo/
Puerto del servidor SMTP: 587

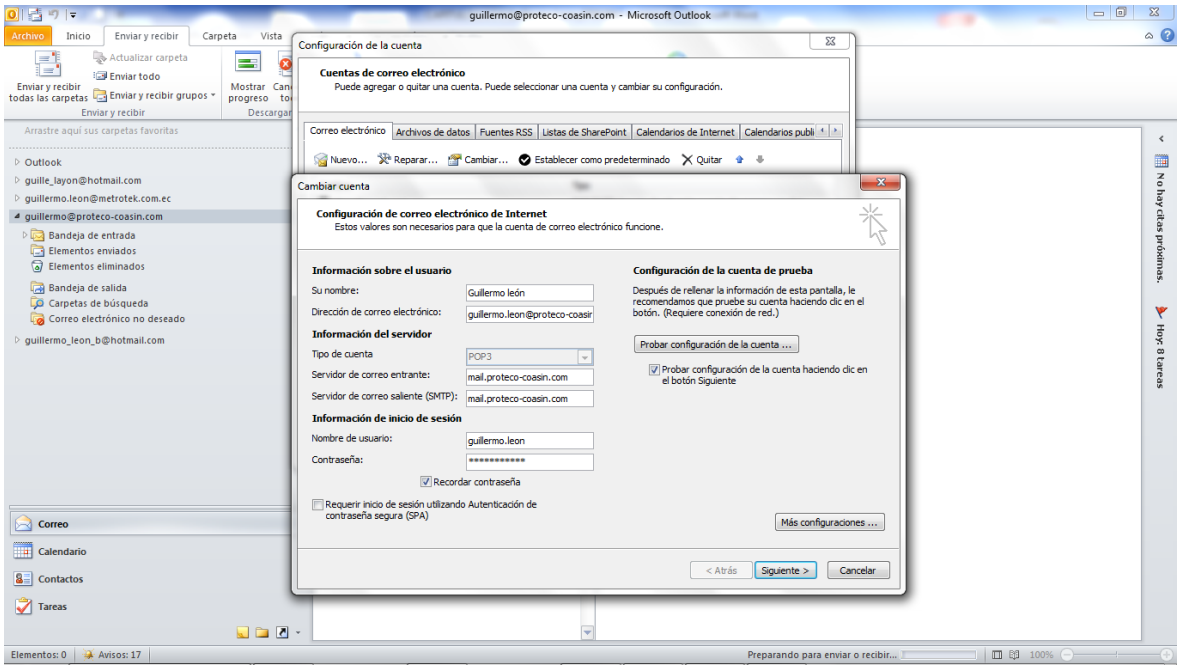


Ilustración 4-19 - Configuración nueva cuenta de correo electrónico

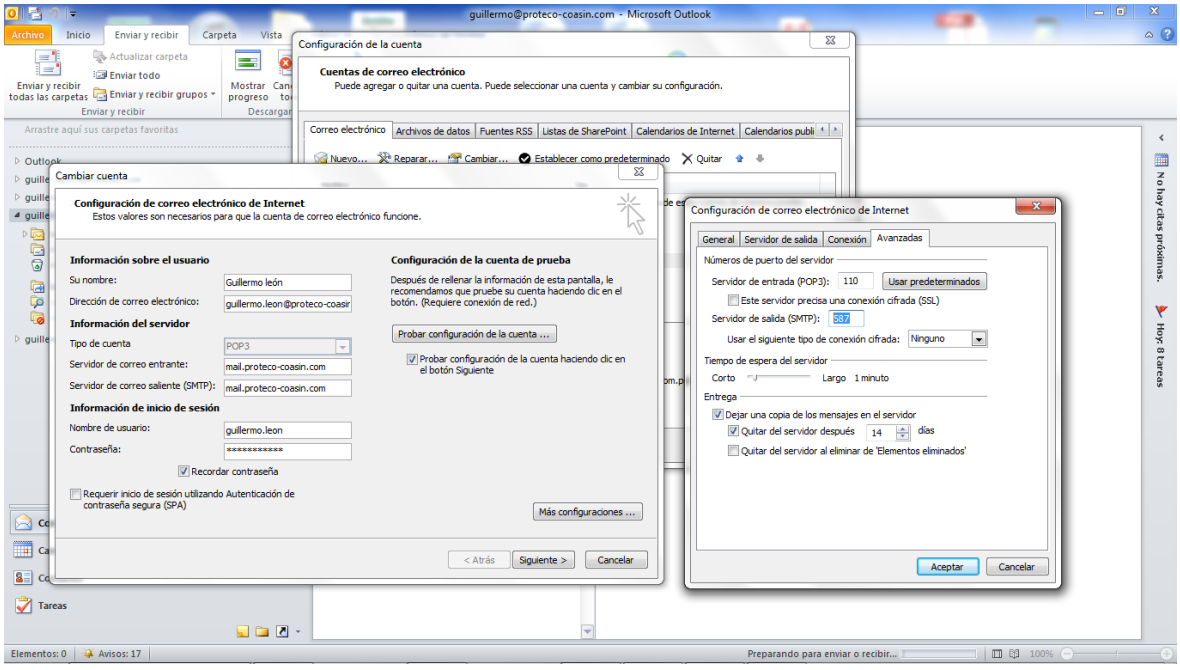


Ilustración 4-20 - Cambio de puerto de servidor SMTP

Al finalizar la configuración es recomendable comprobar la configuración de la cuenta de correo electrónico creada:

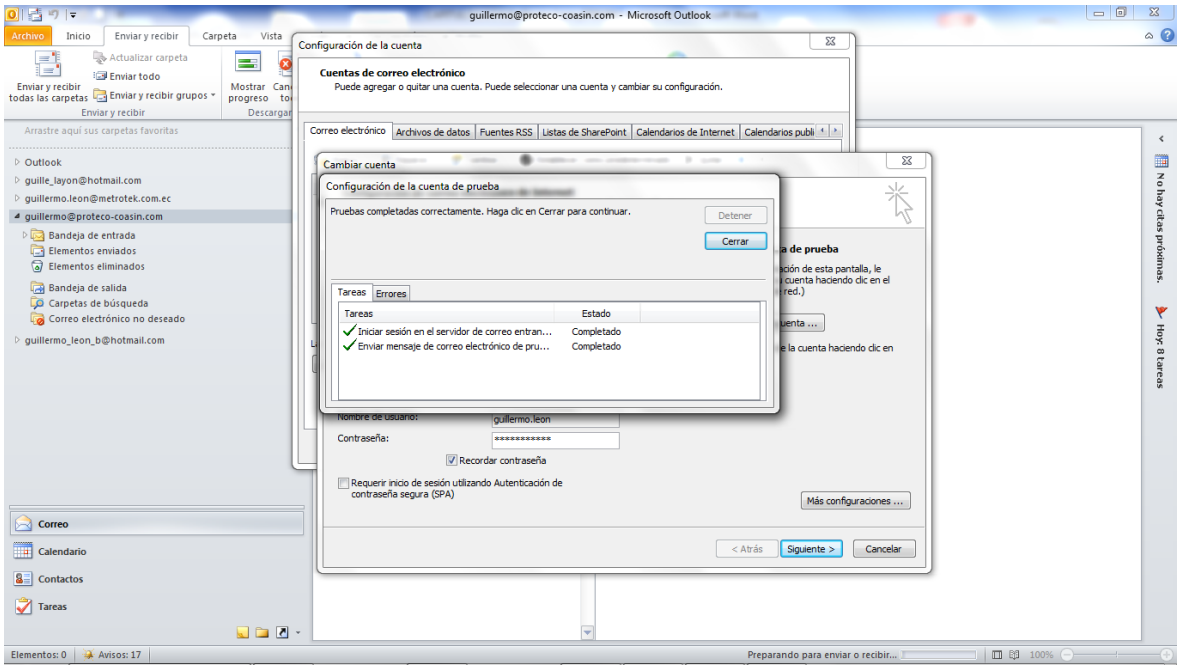


Ilustración 4-21 - Comprobación de configuración de cuenta de correo electrónico creada

4.1.7.2 Envió de correo electrónico a dominios externos.

Envío de correo electrónico a cuenta de HOTMAIL guillermo_leon_b@hotmail.com

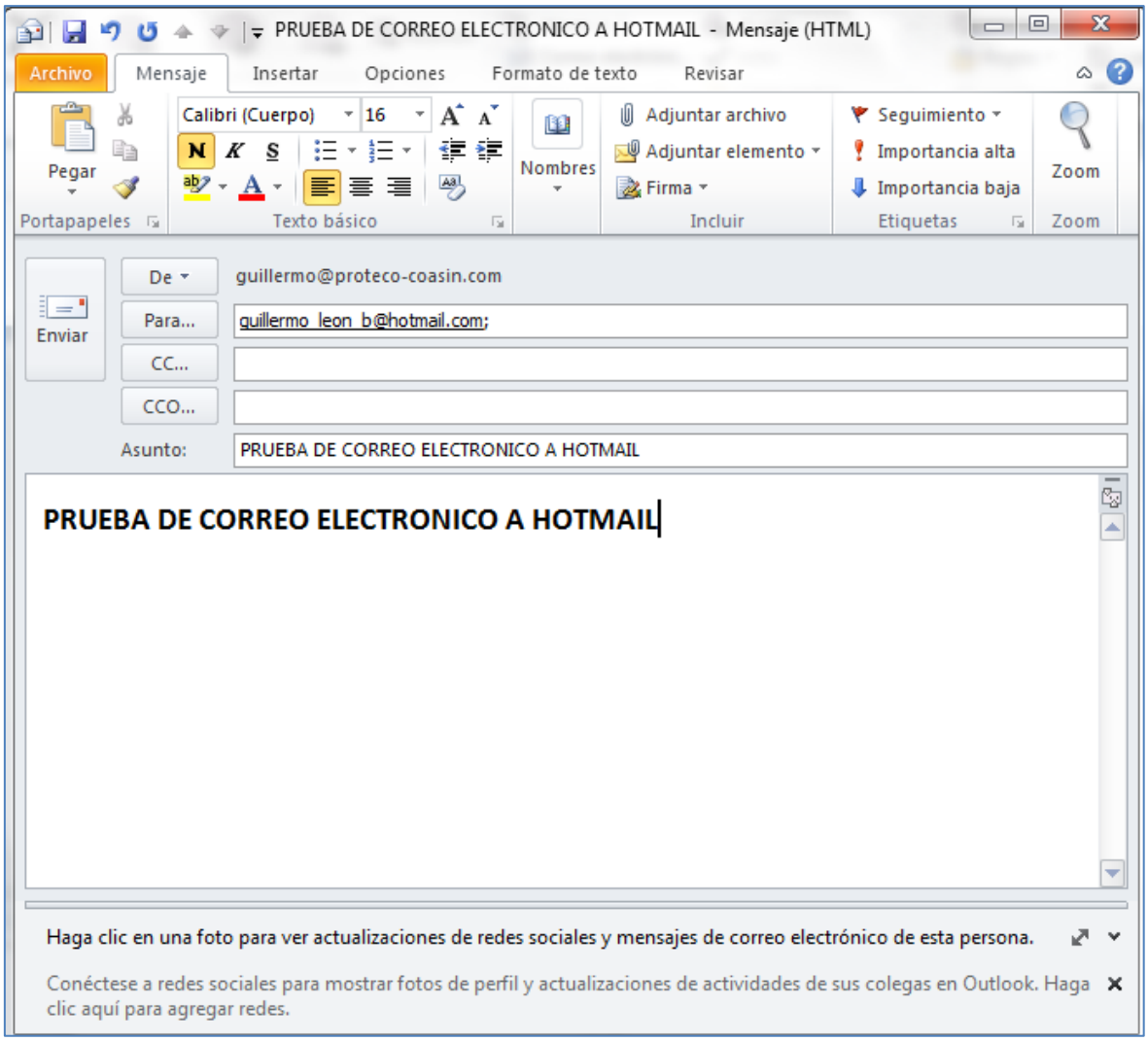


Ilustración 4-22 - Mail a correo de Hotmail

En el log de Sendmail se puede observar el envío del correo y la actuación de MailScanner.

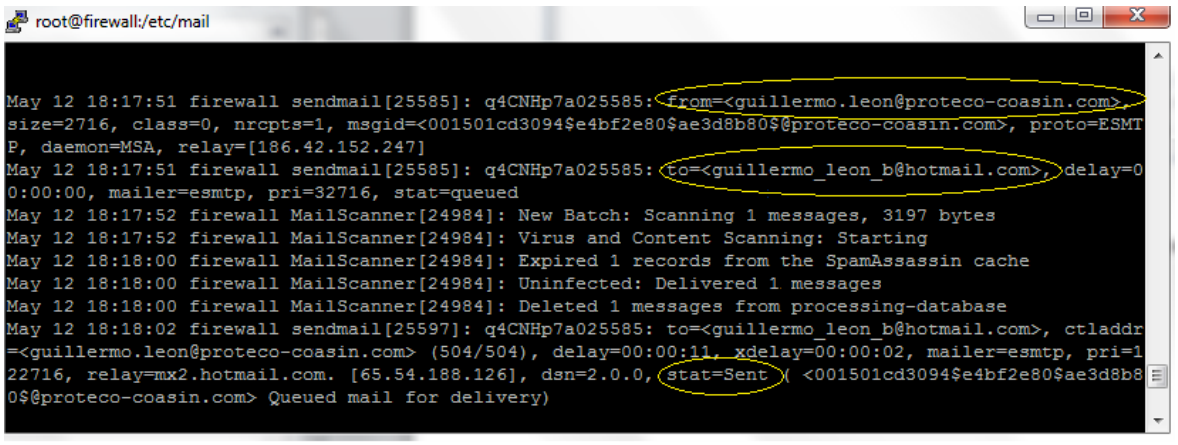


Ilustración 4-23 - Log de Sendmail

En el buzón de la cuenta guillermo_leon_b@hotmail.com se lista el correo recibido.

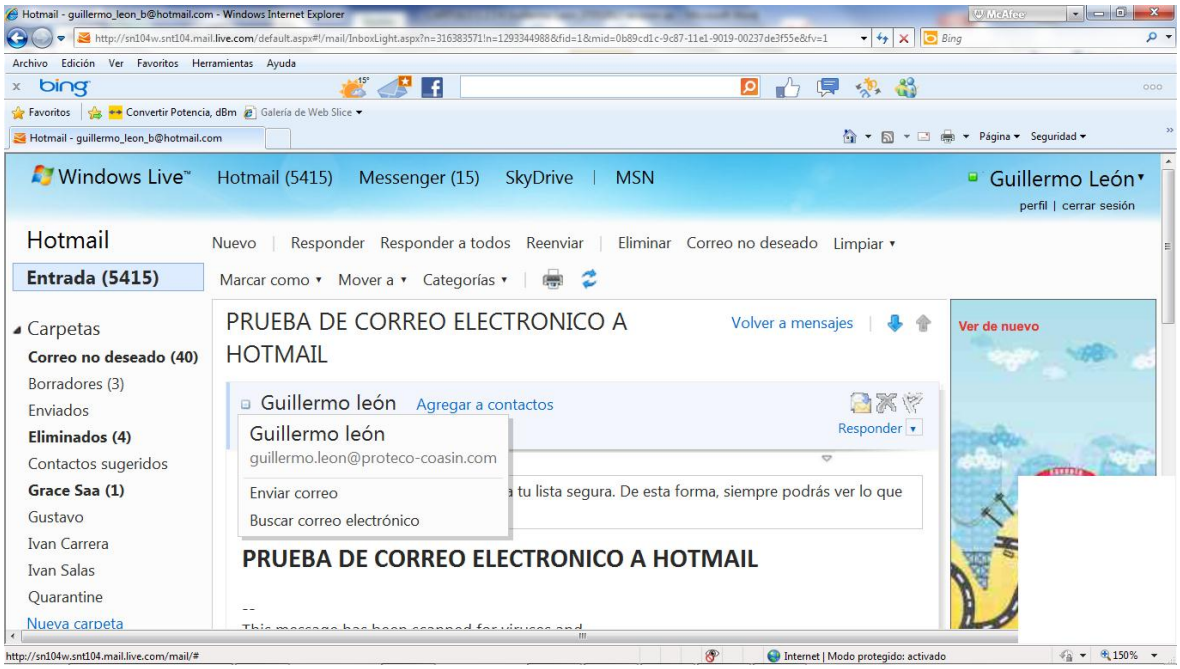


Ilustración 4-24 - Buzón de la cuenta guillermo_leon_b@hotmail.com

4.1.7.3 Recepción de correo electrónico desde GMAIL, cuenta lgleon.b@gmail.com

Para la prueba de recepción y análisis de MailScanner se envió un correo desde una cuenta de GMAIL, lgleo.b@gmail.com:

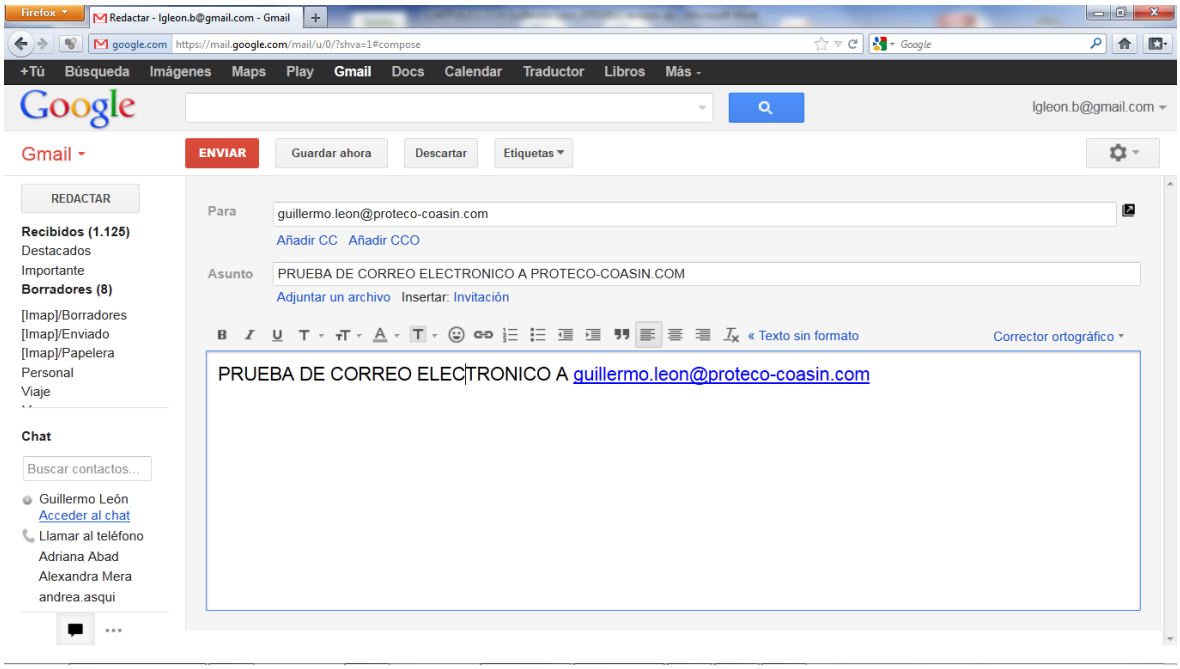


Ilustración 4-25 - Envió de correo electrónico desde cuenta de GMAIL lgleon.b@gmail.com a guillermo.leon@proteco-coasin.com

En los log del servidor se puede observar el correo entrante proveniente desde al cuenta lgleon.b@gmail.com dirigida a la cuenta Guillermo.leon@proteco-coasin.com

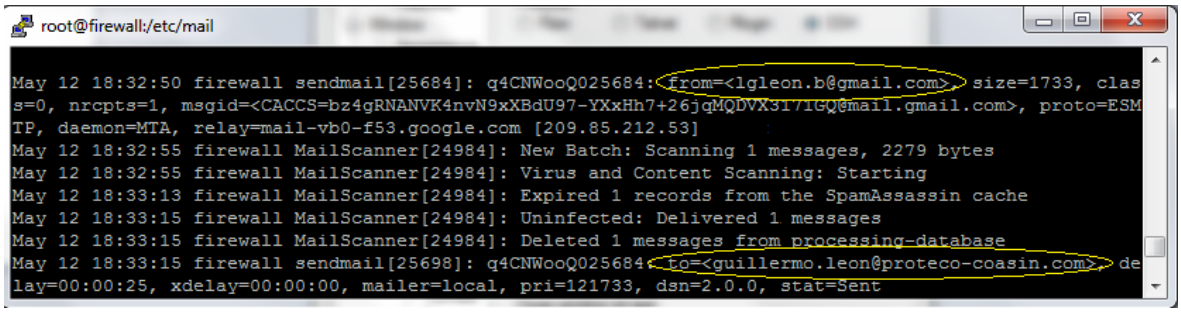


Ilustración 4-26 - Log de Sendmail en recepción de correo

En el cliente de correo electrónico en donde se configuró la cuenta guillermo.leon@proteco-coasin.com se puede observar la recepción del correo:

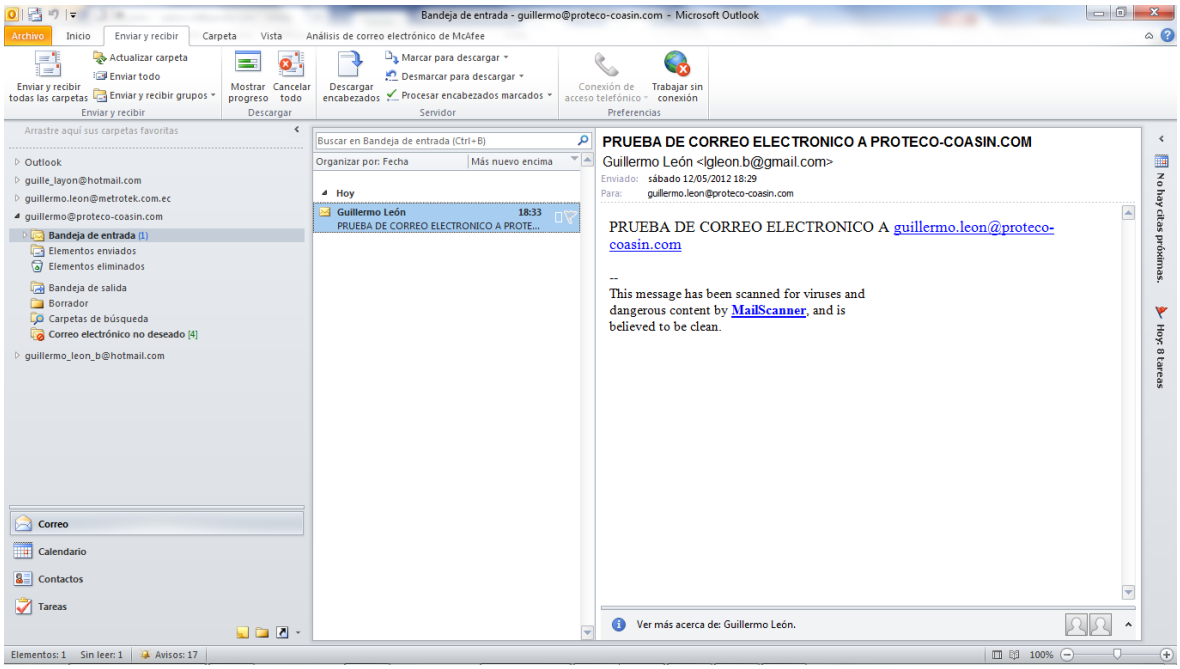


Ilustración 4-27 - Buzón de la cuenta guillermo.leon@proteco-coasin.com

4.1.8 Comprobación operatividad Samba

La comprobación del servicio Samba se realizará accediendo a las carpetas compartidas creadas en el servidor, se utilizará un usuario de dominio de Active Directory para comprobar la integración al mismo.

Para acceder a las carpetas compartidas del servidor se puede utilizar la ruta:

\\server1

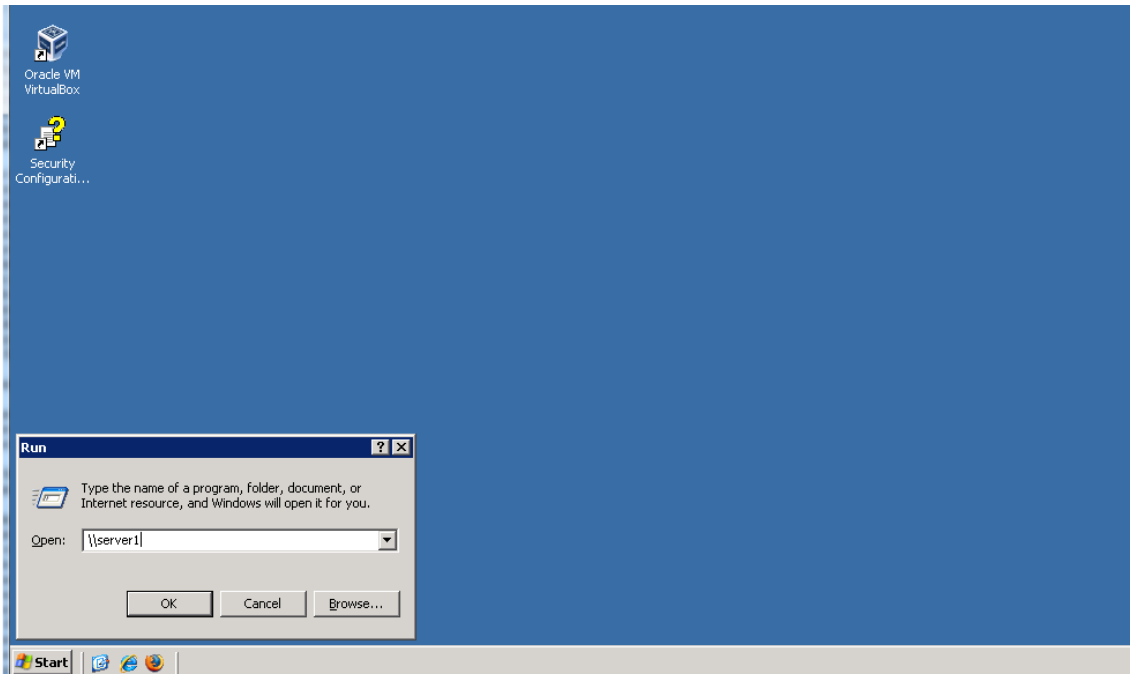


Ilustración 4-28 - Conexión con equipo SERVER1

Por motivos de pruebas se crearon 3 carpetas de operatividad, a las cuales se les asignó los siguientes permisos:

Departamento1.- permiso de acceso, lectura y escritura a usuario gleon
Departamento 2.- permiso de lectura a usuario gleon
Departamento 3.- permiso de acceso, lectura y escritura a usuario abolanos,

La máquina en la que se está realizando las pruebas, se autenticó con el usuario de dominio de Active Directory: gleon.

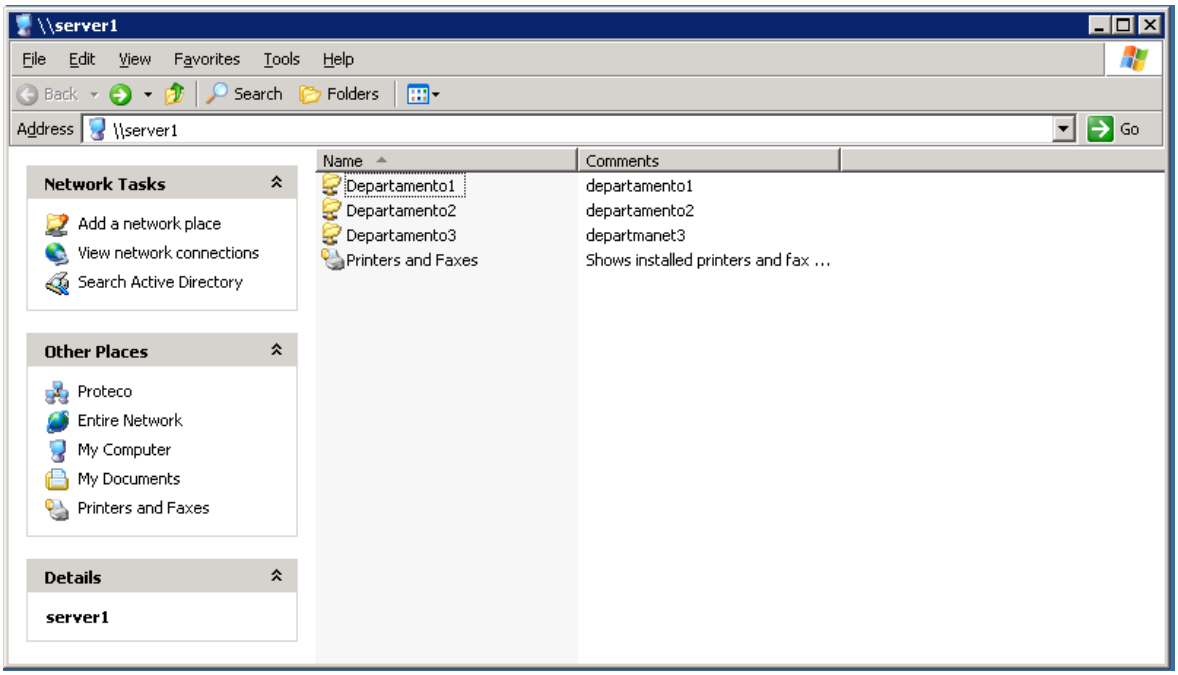


Ilustración 4-29 - Lista de carpetas compartidas en equipo SERVER1

- Departamento1.- permiso de acceso, lectura y escritura a usuario gleon

  Se ingresó a la carpeta Departamento 1

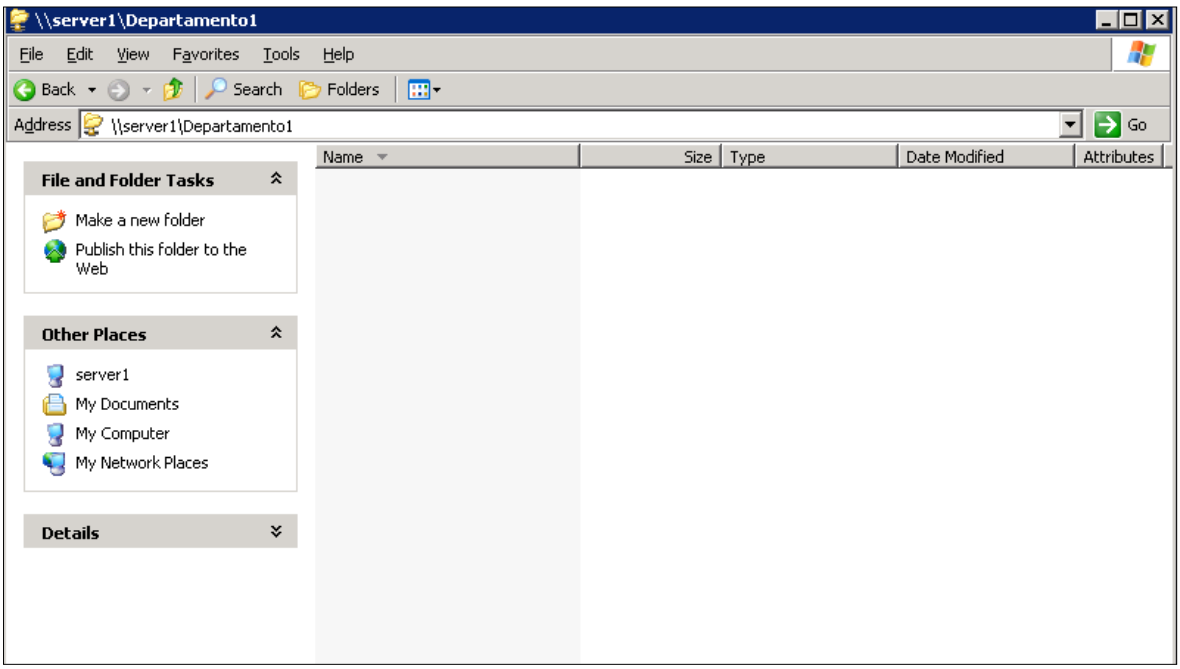


Ilustración 4-30 - Directorio Departamento1 en SERVER1

Sr creó una carpeta de prueba llamada “prueba de escritura”

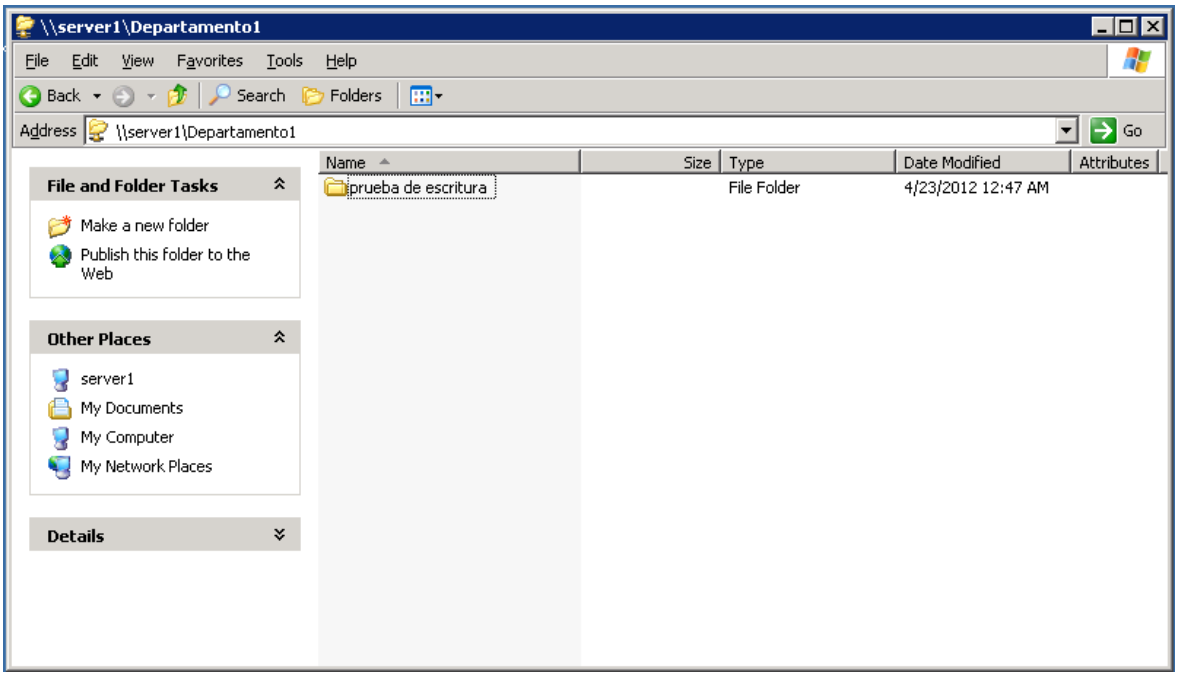


Ilustración 4-31 - Prueba de escritura en directorio Departamento1 en SERVER1

- Departamento 2.- permiso de lectura a usuario gleon

  Se ingresó a la carpeta Departamento 2

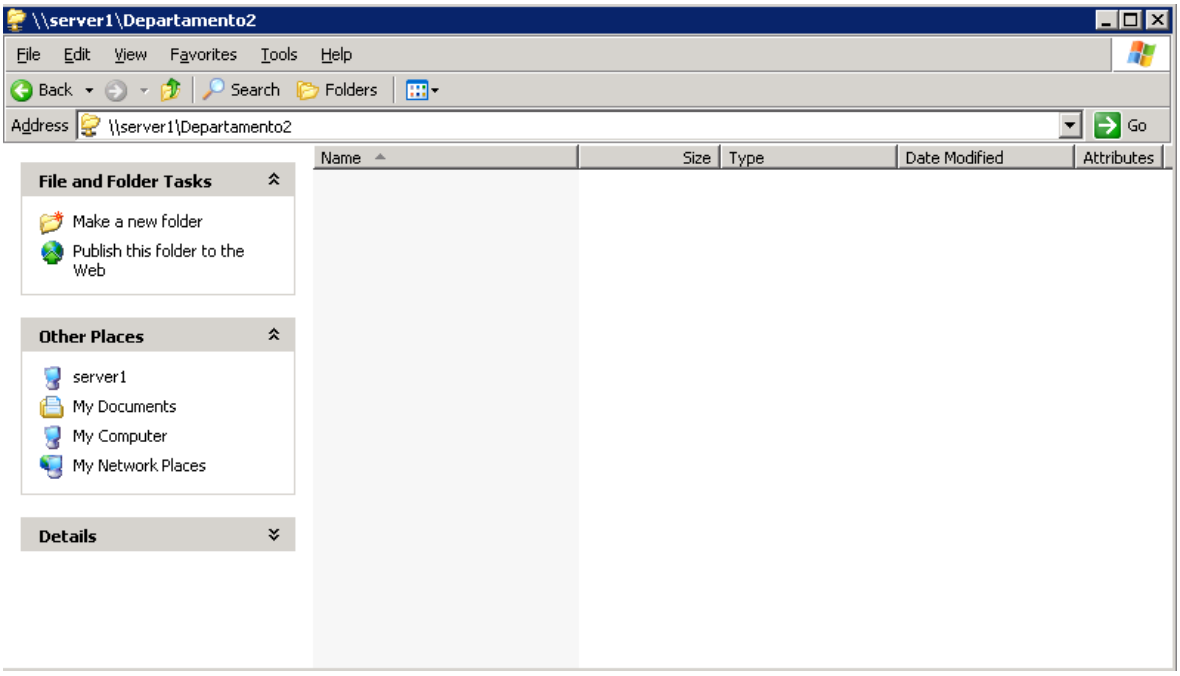


Ilustración 4-32 - Directorio Departamento2 en SERVER1

Al intentar crear una carpeta de prueba, el servidor devolvió el mensaje de acceso denegado.

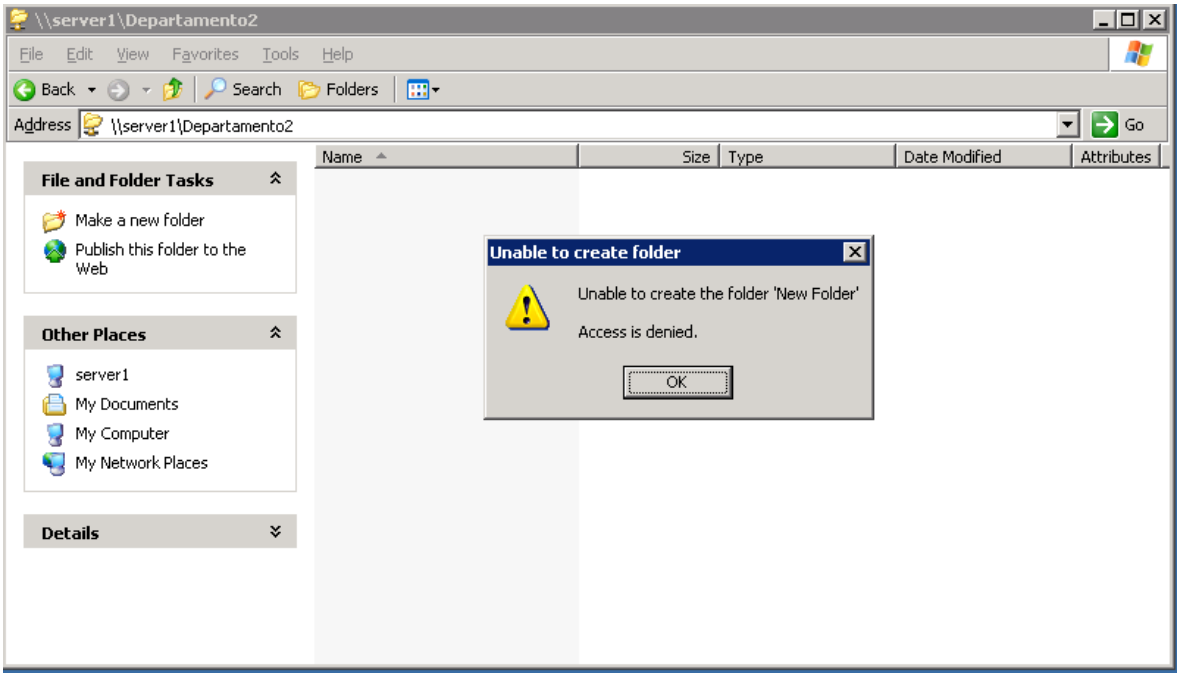


Ilustración 4-33 - Prueba de escritura en directorio Departamento2 en SERVER1

- Departamento 3.- permiso de acceso, lectura y escritura a usuario abolanos,

  El usuario gleon no tiene acceso a la carpeta Departamento3, por lo cual al tratar de ingresar el servidor pedirá verificar las credenciales de inicio de sesión, se utilizarán las credenciales del usuario abolanos el cual tiene acceso a esta carpeta compartida.

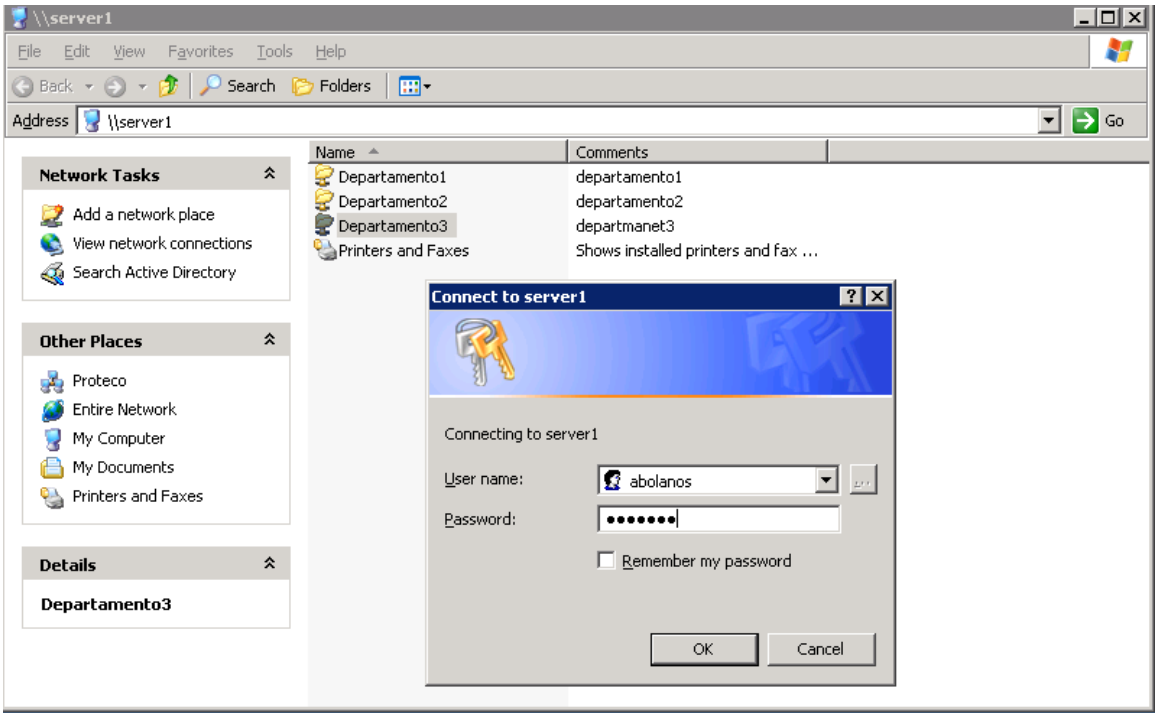


Ilustración 4-34 - Prueba de ingreso en directorio Departamento3 en SERVER1

Al ingresar las credenciales del usuario abolanos, la autenticación es correcta y es permitido el acceso a la carpeta compartida.

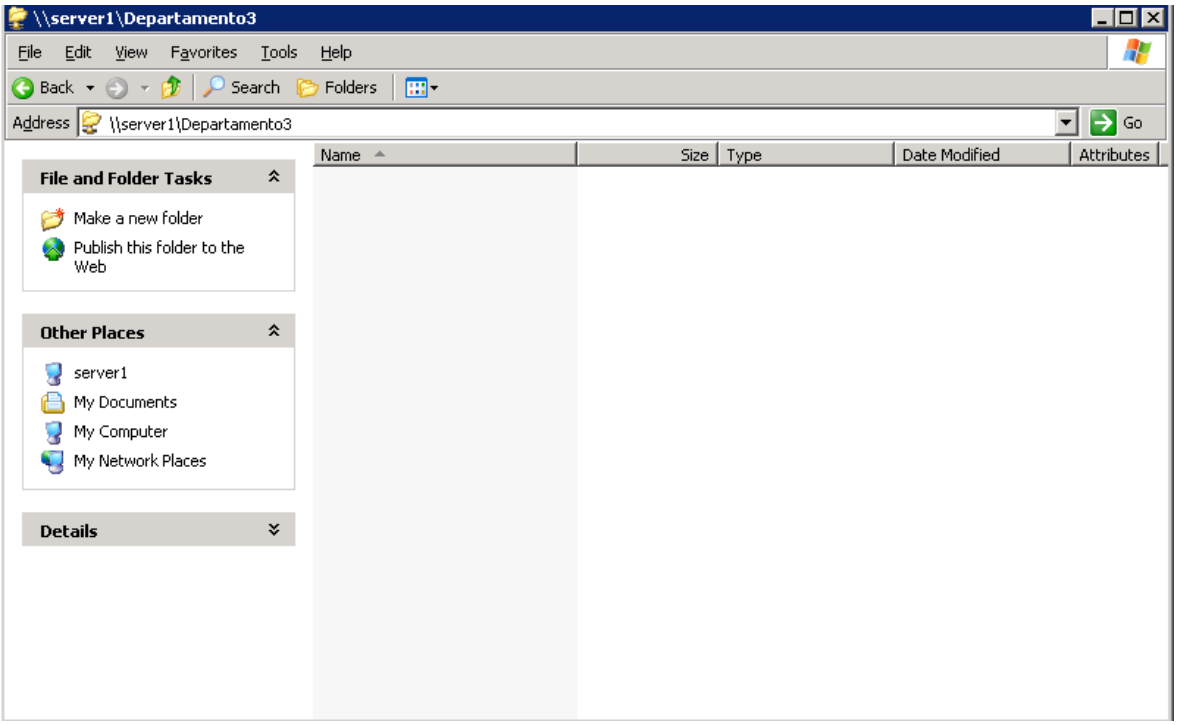


Ilustración 4-35 - Ingreso a directorio Departamento3 en SERVER1 con usuario abolanos

4.1.9 Comprobación operatividad Servidor WEB

Para la comprobación de operatividad del servidor WEB se configuró 2 páginas de prueba en el servidor, una para el dominio intranet.proteco-coasin.com y la otra para el dominio software.proteco-coasin.com.

Desde el navegador de un computador en la red interna se accedió a cada dominio obteniendo estos resultados:

4.1.9.1 Ingreso a intranet.proteco-coasin.com

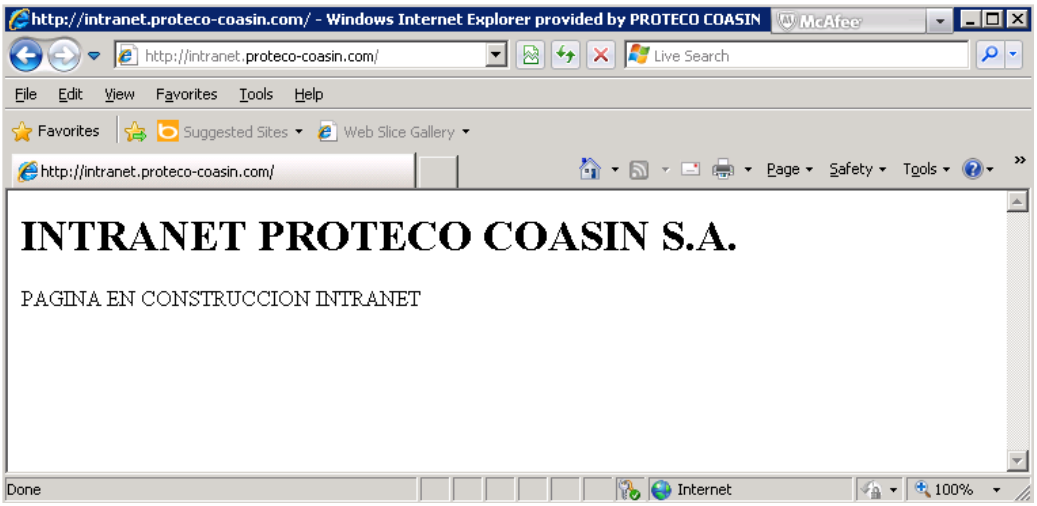


Ilustración 4-36 - Ingreso a intranet.proteco-coasin.com

4.1.9.2 Ingreso a software.proteco-coasin.com

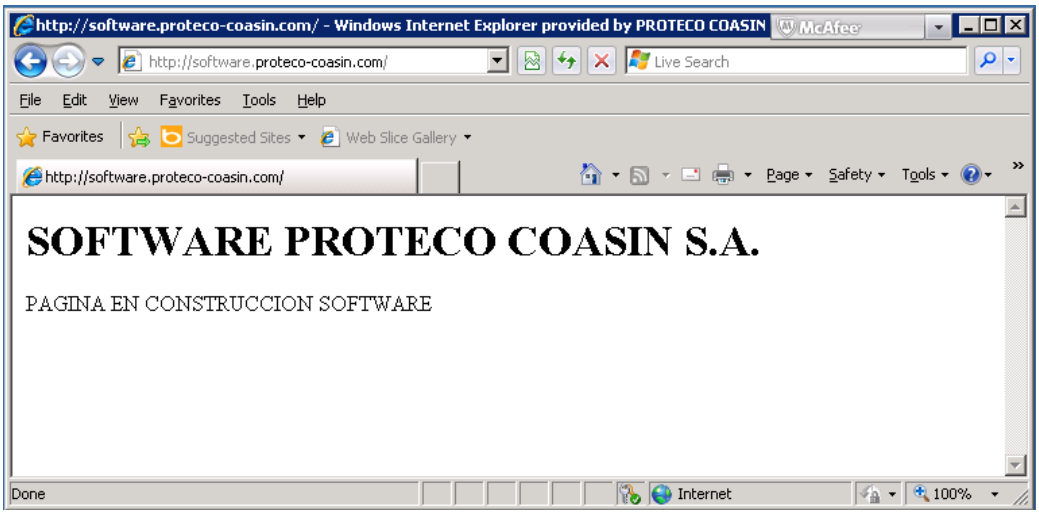


Ilustración 4-37 - Ingreso a software.proteco-coasin.com

4.1.10 Comprobación operatividad Servidor FTP

La verificación de la operatividad del servidor FTP se realizará mediante la aplicación Filezilla versión 3.5.2.

4.1.10.1 Comprobación de operatividad Servidor FTP mediante Filezilla

Posteior a la instalación del cliente FTP Filezilla se realizan las configuraciones necesarias para la conexión como se muestraen la siguiente figura.

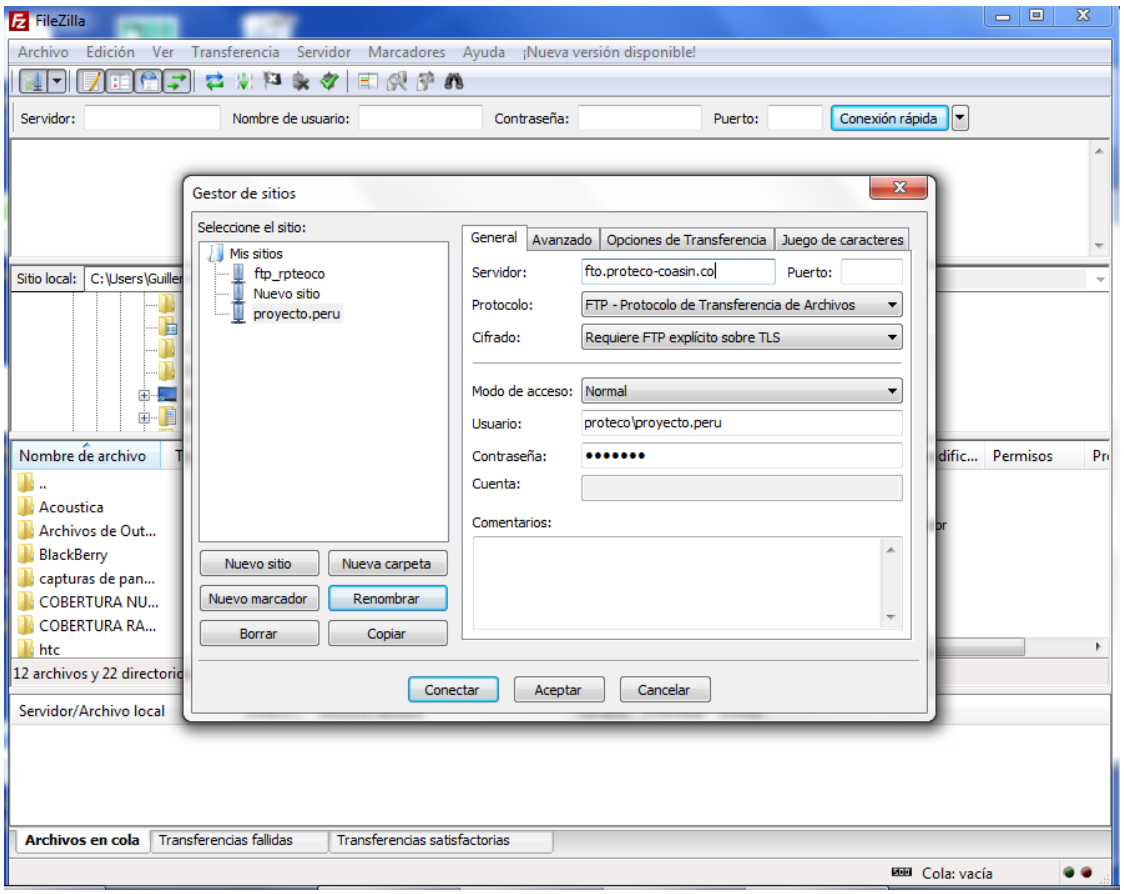


Ilustración 4-38 – Configuración Filezilla

Los parámetros configurados en el cliente son:

Servidor:	ftp:proteco-coasin.com o 190.108.69.190
Protocolo:	FTP protocolo de transferencia de archivos
Cifrado:	Requiere FTP Explícito sobre TLS
Modo de acceso:	Normal
Usuario:	proyecto.peru
Contaseña:	password

Por motivos de pruebas de funcionamiento se crearon 3 usuarios proyectos.ecuador, proyectos.peru y proyectos.argentina en Active Directory y el servidor de FTP se crearon las carpetas donde se guardará la información de cada usuario encapsulado.

mkdir /home/proyecto.ecuador
mkdir /home/proyecto.peru
mkdir /home/proyecto.argentina

Posterior al ingreso de la información necesaria, el servidor devolverá el mensaje del certificado a utilizar:

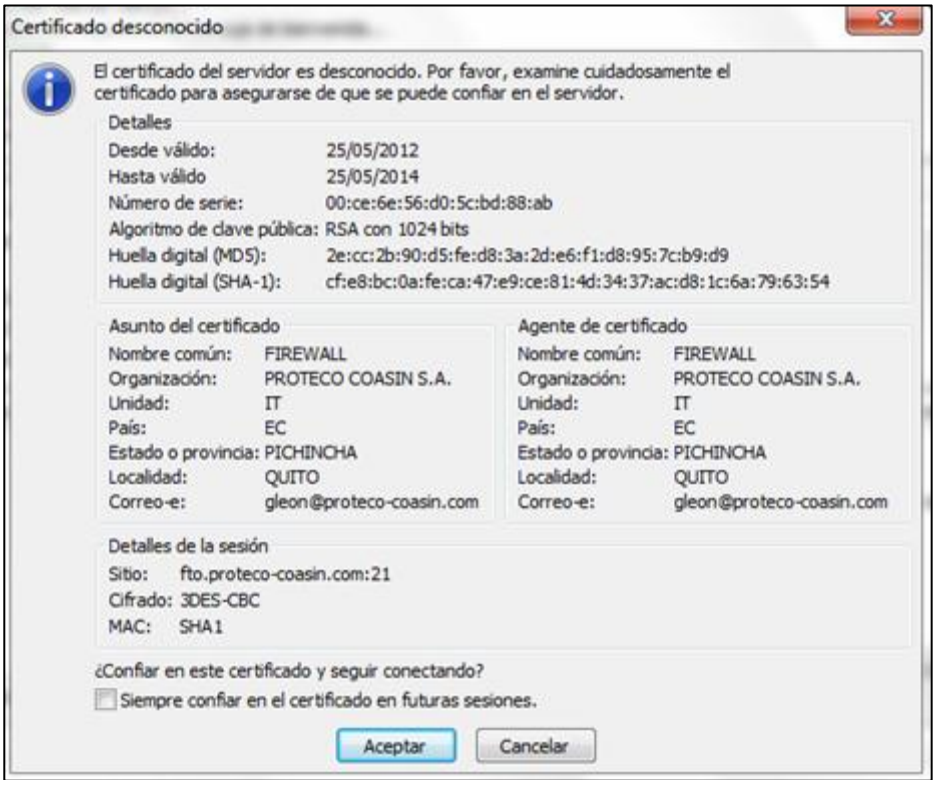


Ilustración 4-39 – Certificado para conexión

Posterior a aceptar el certificado la aplicación indicará que la conexión fue exitosa y se listará el contenido de la carpeta de usuario.

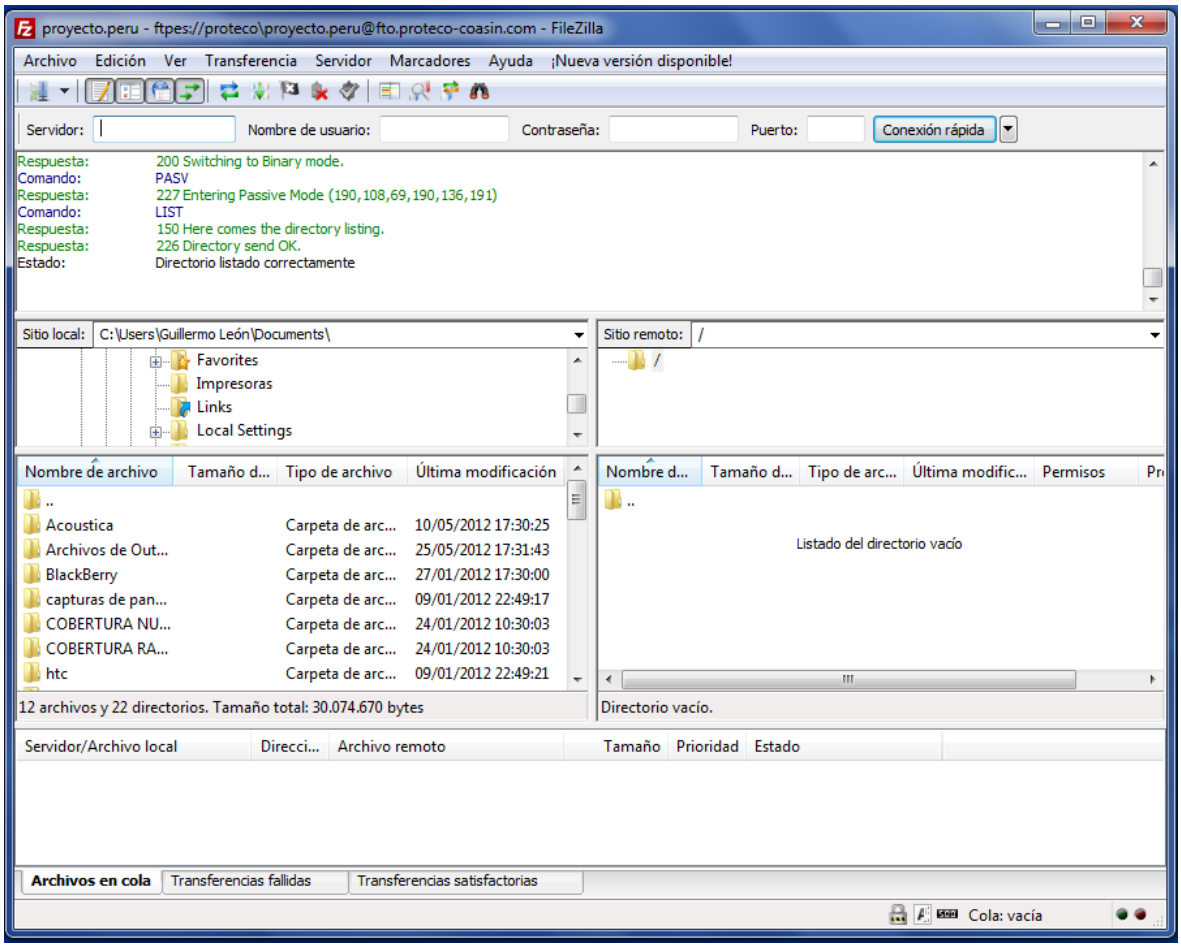


Ilustración 4-38 – Conexión exitosa desde cliente Filezilla a servidor FTP

La conexión al servidor FTP se lo podrá realizar mediante aplicaciones como Filezilla o Winscp que soporten SFTP.

4.1.11 Comprobación operatividad Servidor de respaldos.

Para la verificación del servidor de respaldos Backuppc, se utilizaron 2 máquinas pertenecientes al dominio PROTECO.LOCAL.

Fue necesaria la creación de un usuario en Active Directory, el cual tendrá los permisos necesarios para acceder a la información de los clientes y respaldar la misma.

El usuario creado en Active Directory es backuppc, en cada máquina cliente a respaldar la información del usuario se compartió la carpeta de perfil del mismo, pero se dio permiso de acceso solamente al usuario creado en Active Directory "backuppc".

Mediante las credenciales de este usuario, el servidor de respaldos Backuppc podrá acceder a la información necesaria que va ser respaldada.

4.1.11.1 Configuración de cliente a respaldar.

Datos del equipo:

Nombre del equipo: pro_con01
Usuario: Alexandra Mera
IP asignada: 192.168.3.30

4.1.11.1.1 Agregar un nuevo host

Conocer los datos del equipo a respaldar es necesario, con estos datos se podrá brindar la información necesaria a Backuppc para que pueda acceder a la información a ser respaldada.

En el menú “edit host” se debe ingresar la dirección IP del equipo o el nombre de la máquina y el nombre de usuario de la misma.

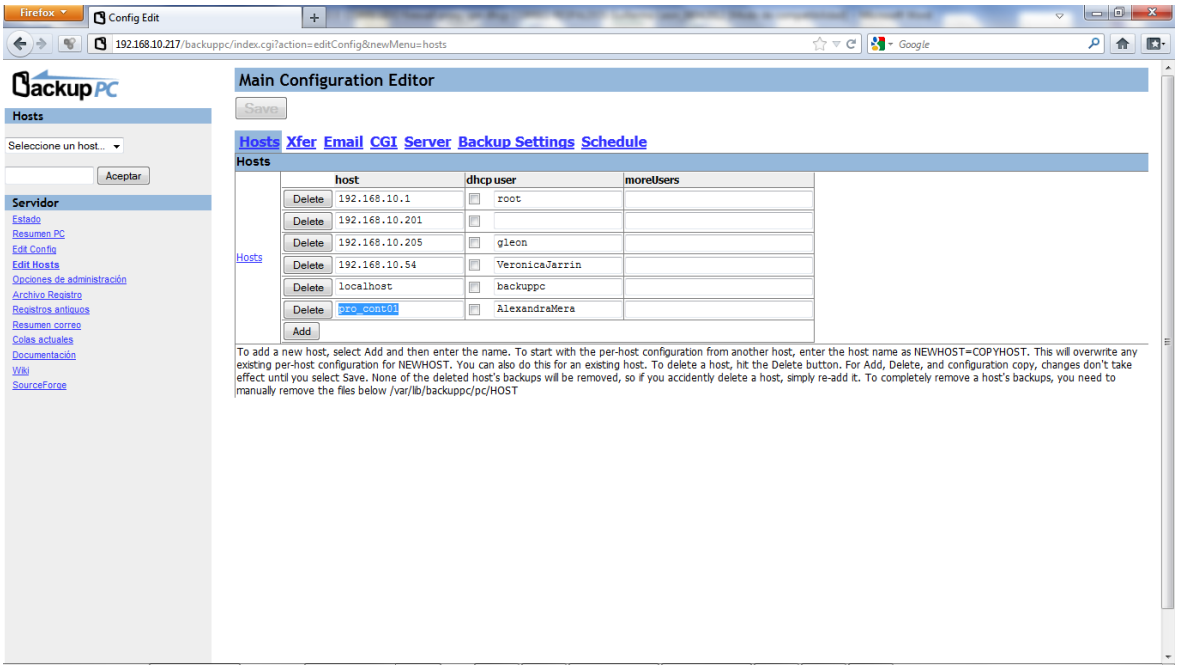


Ilustración 4-390 - Agregar Host a ser respaldado

4.1.11.1.2 Configuración del host a respaldar

En el menú host se debe escoger el equipo para editar su configuración.

Las configuraciones establecidas para los equipos clientes

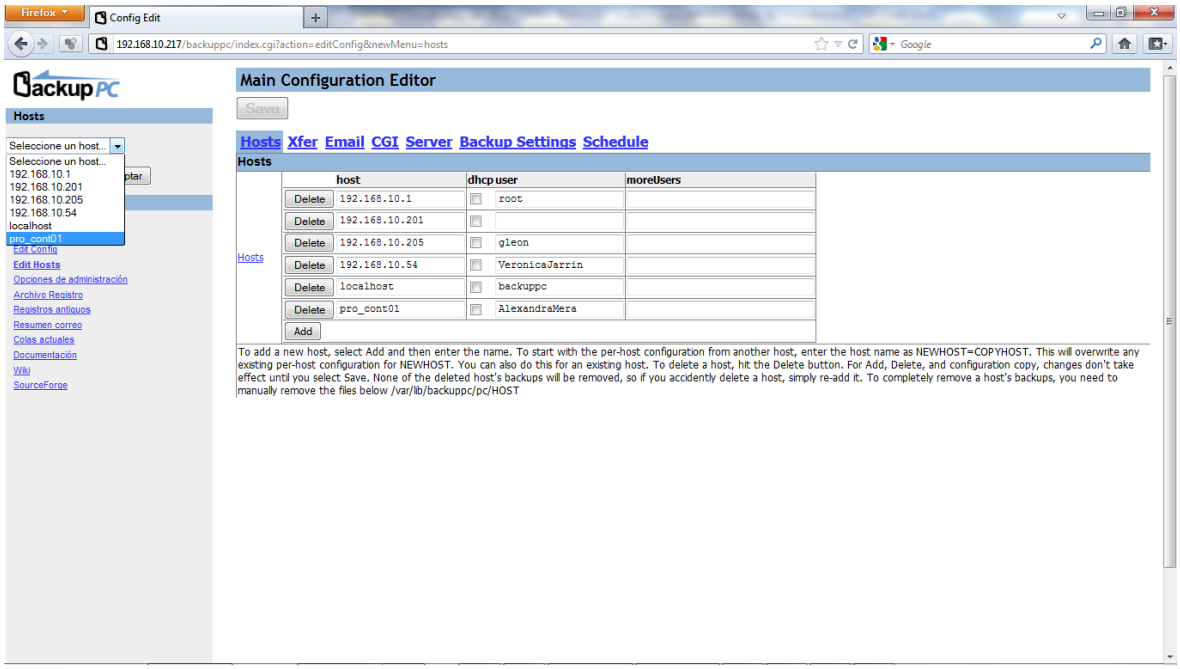


Ilustración 4-41 - Selección de Host a ser respaldado

En el menú de configuración en la pestaña XFER, se debe ingresar el método de compartir la información, en el caso de clientes con sistema operativo Windows es SMB, el nivel de verbosidad es suficiente con 1.

En el parámetro SmbShareName se especifica el nombre de la carpeta compartida creada, en este caso al haberse compartido el perfil de usuario, se respaldará todo lo que contiene ese directorio.

El parámetro SmbShareUserName se especifica el nombre de usuario que tiene acceso a la carpeta compartida creada, como se explicó anteriormente el usuario creado para la creación de respaldos es “backuppc”. El usuario se debe especificar con el nombre del dominio al que pertenece proteco\backuppc

En el parámetro SmbSharePasswd se especifica la contraseña del usuario del dominio.

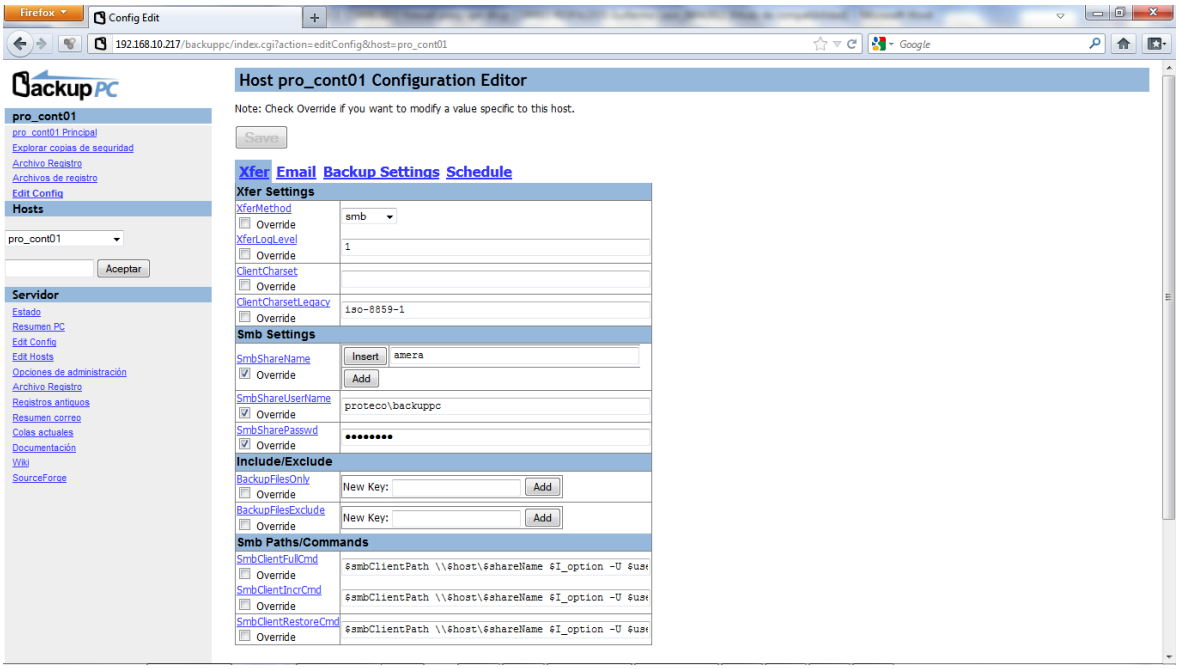


Ilustración 4-402 - Configuración de Host a ser respaldado

Para indicar el número de backups totales e incrementales y los días que se requieren respaldar la información, se lo realiza en la pestaña Schedule la interface Web.

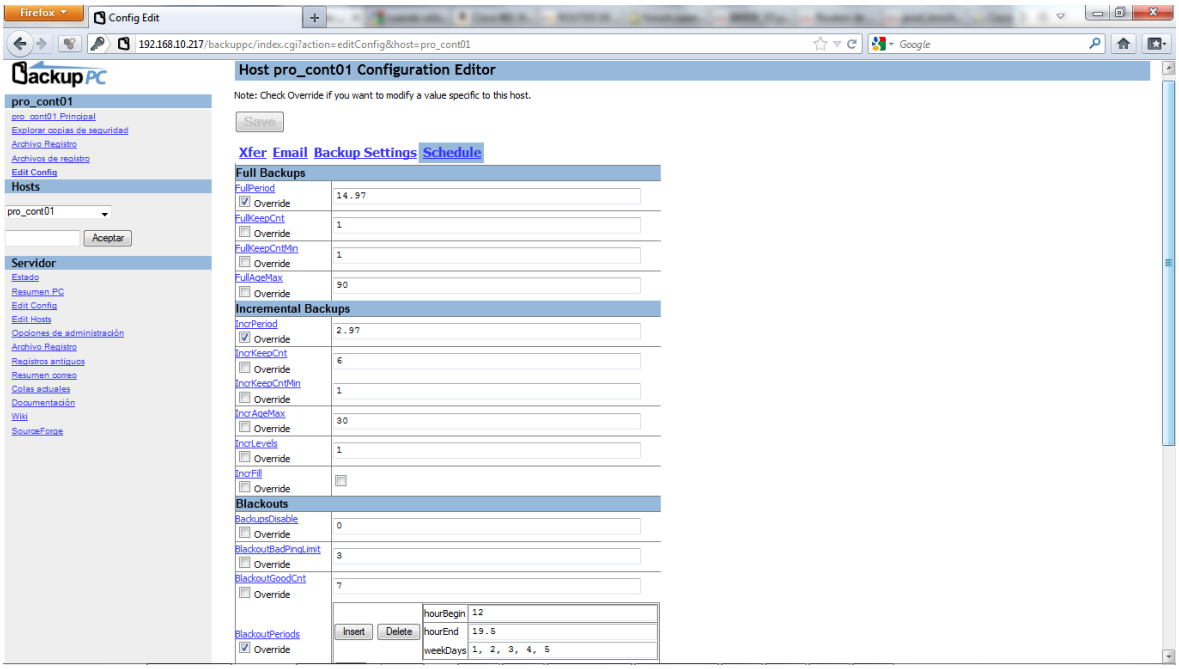


Ilustración 4-413 - Configuración de horario de backups de Host a ser respaldado

Con el parámetro FullPeriod se especifica la periodicidad con la que los respaldos totales se van a realizar, la configuración adoptada fue 15 días.

En el parámetro FullKeepCnt se especifica el número de backups totales que se van a guardar. Se guardarán los 2 últimos backups totales realizados.

El tiempo máximo que un backup total puede ser guardado se especifica en el parámetro FullAgeMax.

Los backups incrementales se los realizará cada 3 días, en el parámetro IncrPeriod se especifica los días.

El número de backups incrementales que se guardarán serán el especificado en el parámetro IncrKeepCnt

Los días y la hora en que se realiza el backup se especifica en el parámetro BlackoutPeriods, se optó por respaldar los equipos a partir de 1 PM, horario en el cual la mayoría de usuarios no ocupan sus máquinas.

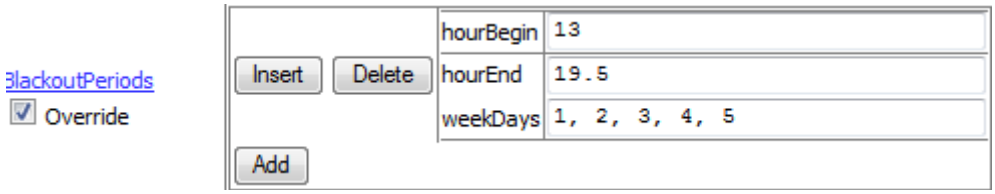


Ilustración 4-424 - Configuración de horarios de Host a ser respaldado

Los respaldos obtenidos se pueden observar en la página principal de cada cliente:

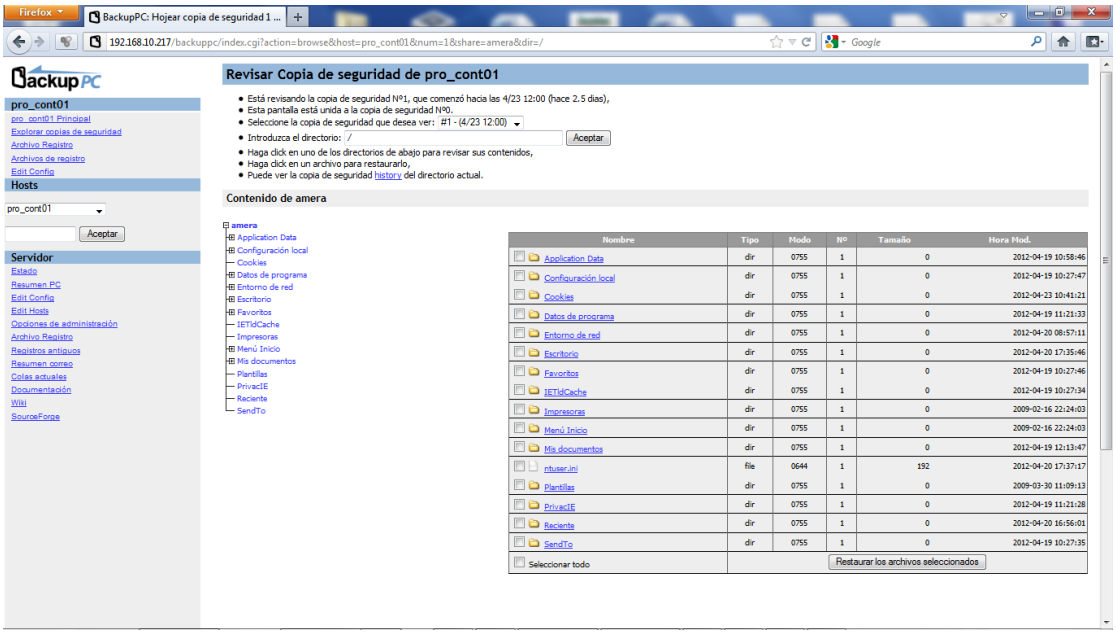


Ilustración 4-435 - Comprobación de respaldo realizado a equipo pro_cont01

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La solución a los problemas detectados en la infraestrutura de red actual y que mediante la implementación de servicios basados en Linux han mejorado el rendimiento y la administración son:

    1. Saturación del canal de internet.- mediante la implementación del proxy de caché Squid junto con herramientas de monitoreo que utilizan la información obtenida por el proxy, actualmente se puede determinar qué equipo en la red se encuentra saturando el canal de internet en tiempo real mediante la herramienta Sqstat y logs de navegación por usuario en días anteriores mediante la herramienta Sarg, los cuales ayudan a determinar sitios web que corroboren en la saturación del canal de internet y que no tengan relación con el entorno laboral.

    2. La implementación y administración local del servidor de correo electrónico ayudará en gran medida a aumentar la confidencialidad de la información mantenida en el servidor, el filtro antispam y MailScanner contribuirá de gran forma a filtrar correo electrónico no desedo en el buzón de los usuarios.

    3. La implementación del servicio DHCP estático y la asignación de rangos específicos de direcciones IP para servidores y equipos de red, facilita completamente la administración de los equipos y servicios en la red, de igual forma la asignación de un rango especifico de direcciones IP para las máquinas de usurios visitantes, permitirá al administrador conocer de una manera presisa qué dispositivo de red tiene problemas de conectividad o se encuentra saturando el canal de internet.

    4. La integración de los servicos de FTP y SAMBA con Active directory permitirá una administración de usaurios centralizada, manteniendo con ésto un mayor control de estos servicios.

- Las aplicaciones de software libre implementadas consumen muy pocos recursos de memoria, procesador y espacio en disco del compitador, permitiedo la reutilización de recursos y disminución de gastos por parte de la empresa al no tener que adquirir nuevos equipos.

- Mediante la implementación del proxy de caché Squid que permite el filtrado de contenidos y por su capacidad de hacer caché, se logró aumentar el tiempo de respuesta en la navegación y evitar saturación del canal de internet, manteniendo un monitoreo en tiempo real y estadísticas diarias de navegación.

- A partir de la implementación del servidor de respaldos automáticos, se consiguió:

    1. Aumentar la disponibilidad de la información de los servidores de red basados en Linux y equipos clientes basados en Windows, sin presentar molestias ni retardos para los usuarios.

    2. Disminuir en gran manera la responsabilidad del administrador de realizar respaldos manuales de cada equipo en la red.

- La implementación de los servicios de red, son la base para comenzar con una infraestructura estable y confiable manteniendo una adecuada utilización de los recursos de trabajo que satisfaga las necesidades de los usuarios

- La integración de los servicios de red implementados bajo CENTOS 5 y Active Directory permitirá a los usuarios mantener un solo usuario y contraseña para acceder a varios servicios como los que presta el servidor de archivos y FTP.

- El servicio de FTP será utilizado por clientes externos e internos de la empresa, no se permitirá el acceso a usuarios anónimos. El servicio fue implementado con soporte TLS, y no se permitirá que existan conexiones no seguras al servidor FTP. Se deberán utilizar clientes FTP como Filezilla o Winscp que soporten TLS sobre FTP para asi conseguir que la información de usuario y contraseña este segura.

5.2 RECOMENDACIONES

- Es de suma importancia mantener la satisfacción del cliente interno a través del correcto funcionamiento de los servicios de red, por tanto es recomendable continuar con el desarrollo de servicios tales como la intranet de la empresa.

- Realizar mantenimientos preventivos y correctivos de hardware, por lo menos 3 veces al año, para evitar problemas con la disponibilidad de los servicios.

- El monitoreo de los log de cada servicio es recomendable hacerlo periódicamente evitando la saturación de discos y fallas inesperadas en el sistema. Ayudaría en gran forma con el monitoreo de servicios y monitoreo de conectividad de equipo de red, la implementación de herramientas que realicen automáticamente el monitoreo e informen de manera automática y oportuna del problema al administrador de la red, ya sea por medio de correo electrónico o mensaje de texto.

- Es necesario implementar políticas de restricción de navegación para algunos sitios en internet evitando con esto la saturación del canal.

- Concienciar a los usuarios del manejo adecuado de los equipos de trabajo y servicios de red para evitar pérdida de información y saturación de servicios que pueda afectar a los clientes internos de la empresa.

- Es recomendable realizar capacitaciones frecuentes sobre software de ofimática y seguridad de información a usuarios de la empresa para que tengan los conocimientos básicos necesarios para el manejo adecuado de las herramientas de trabajo.

BIBLIOGRAFÍA

Itsecureadmin. (4 de Junio de 2008). Recuperado el 23 de 11 de 2011, de http://itsecureadmin.com/wiki/index.php/Integrate_Linux_with_Active_Directory

Barrios, J. (23 de Mayo de 2012). *Alcance Libre*. Recuperado el 12 de Mayo de 2012, de http://www.alcancelibre.org/staticpages/index.php/manuales-indice

Barrios, J. (24 de Mayo de 2012). *Alcance Libre*. Recuperado el 25 de Mayo de 2012, de http://www.alcancelibre.org/staticpages/index.php/09-como-vsftpd

Barrios, J. (23 de Mayo de 2012). *Alcance Libre*. Recuperado el 23 de Abril de 2012, de http://www.alcancelibre.org/staticpages/index.php/como-dhcp-lan

Cedillo, I. E. (5 de Octubre de 2010). *Linux para todos*. Recuperado el 4 de Fecbrero de 2012, de www.linuxparatodos.net

Cedillo, I. E. (3 de Junio de 2010). *Linux para todos*. Recuperado el 14 de Diciembre de 2011, de http://www.linuxparatodos.net/web/comunidad/base-de-conocimiento?p_p_id=36&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=2&_36_struts_action=%2Fwiki%2Fview_page_details&p_r_p_185834411_nodeName=Base+de+Conocimiento&p_r_p

Cisco. (s.f.). CCNA-EXPLORATION1. En Cisco, *CCNA-EXPLORATION1*.

Fortunecity. (s.f.). *Tipos de Redes*. Recuperado el 15 de Octubre de 2011, de http://members.fortunecity.es/elcastillodelainformatica/tiposderedes.htm

Garay, W. W. (27 de Marzo de 2006). *Maestros del la web*. Recuperado el 14 de Enero de 2012, de http://www.maestrosdelweb.com/editorial/host/

Gite, V. (2 de Octubre de 2006). *Cyberciti*. Recuperado el 17 de Noviembre de 2001, de http://www.cyberciti.biz/faq/howto-set-date-time-from-linux-command-prompt/

Jeff. (16 de Octubre de 2008). *Kioskea*. Recuperado el 01 de Abril de 2012, de http://es.kioskea.net/contents/wireless/wlan.php3

Lopez, R. (23 de Diciembre de 2008). *Sistemas blogspot*. Recuperado el 14 de Febrero de 2012, de http://rlt-sistemas.blogspot.com/2008/12/vsftp-directorio-activo.html

Todos, L. P. (12 de Marzo de 2012). *Linux para todos*. Recuperado el 15 de Abril de 2012, de http://www.linuxparatodos.net/web/comunidad/base-de-conocimiento

Todos, P. L. (26 de Junio de 2010). *Linux para todos*. Recuperado el 15 de Noviembre de 2011, de http://www.linuxparatodos.net/web/comunidad/base-de-conocimiento/-/wiki/Base+de+Conocimiento/Servidor+Firewall

Wikipedia. (28 de Marzo de 2012). *Correo Electrónico*. Recuperado el 15 de Octubre de 2011, de Wikipedia: http://es.wikipedia.org/wiki/Correo_electr%C3%B3nico

Wikipedia. (21 de Marzo de 2012). *Servidor HTTP Apache*. Recuperado el 15 de Octubre de 2011, de http://es.wikipedia.org/wiki/Servidor_HTTP_Apache

ANEXOS

ANEXO 1 SCRIPT DE CONFIGURACIÓN DE FIREWALL

```
#!/bin/sh

# Informacion de Red

#Interface Enterna
INTERNALIF="eth1"
#Red interna
INTERNALNET="192.168.3.0/24"
#Broadcast de la red
INTERNALBCAST="192.168.3.255"
#Interface Externa
EXTERNALIF="eth0"
#IP EXTERNA
MYADDR="190.108.69.190"

# Caminos - No tocar si no se conoce.
DMESG="/bin/dmesg"
IPTABLES="`which iptables`"
MODPROBE="/sbin/modprobe"

REDHAT="YES"
# Llamar al scrip con los parametros: start/stop/restart
if [ X"$REDHAT" = X"YES" ]; then
        . /etc/rc.d/init.d/functions
        case "$1" in
                stop)
                        action "Shutting down firewall:" echo
                        $IPTABLES -F
                        $IPTABLES -P FORWARD DROP
                        exit 0
```

```
                ;;
        status)
                echo "The status command is not supported for iptables"
                exit 0
                ;;
        restart|reload)
                $0 stop
                exec $0 start
                ;;
        start)
                action "Starting Firewall:" echo
        ;;
    *)
        echo "Usage: firewall (start|stop|restart)"
        exit 1
  esac
fi


#####################################################################

#Insertando los modulos
/sbin/modprobe ip_tables
/sbin/modprobe iptable_filter
/sbin/modprobe ip_conntrack
/sbin/modprobe ip_conntrack_ftp


#Vaciar las reglas que puedan existir

# Paquetes provenientes del exterior
$IPTABLES -F INPUT
# Paquetes de la red interna hacia el exterior
```

```
$IPTABLES -F OUTPUT
# Forwarding/enmascaramiento
$IPTABLES -F FORWARD
#Tabla de NAT
$IPTABLES -t nat -F



#No responder a pings de broadcast
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

#No responder a los pings - Activar si se requiere
echo "0" > /proc/sys/net/ipv4/icmp_echo_ignore_all

#Habilitando el forwarding
echo 1 >/proc/sys/net/ipv4/ip_forward

#Anular los TimeStamps. Se puede averiguar el uptime de un sistema
echo 0 > /proc/sys/net/ipv4/tcp_timestamps

#Habilitar SYN Cookies, previene algunos DoS
echo 1 > /proc/sys/net/ipv4/tcp_syncookies

#Dehabilitar redirects. Habilitar si no se actua como router
echo 0 >/proc/sys/net/ipv4/conf/all/accept_redirects

#Habilitar proteccion contra mensaje invalido
echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

#Definir rango de puertos locales a ser usados por nuestras aplicaciones
echo "32768 61000" >/proc/sys/net/ipv4/ip_local_port_range

#Reducir posibilidad de DoS al reducir los timeouts
```

```
#Tiempo en el que linux tratar de finalizar una conexion
echo 30 > /proc/sys/net/ipv4/tcp_fin_timeout

#Tiempo para finalizar una conexi n no activa
echo 1800 > /proc/sys/net/ipv4/tcp_keepalive_time
echo 1 > /proc/sys/net/ipv4/tcp_window_scaling
echo 0 > /proc/sys/net/ipv4/tcp_sack

#Maximo de conexiones SYN
echo 1280 > /proc/sys/net/ipv4/tcp_max_syn_backlog

##Activando reglas basicas

#Matar paquetes con combinaciones de banderas invalidas
$IPTABLES -A INPUT -m state --state INVALID -j DROP
$IPTABLES -A FORWARD -m state --state INVALID -j DROP

# Permitir todas las conexiones en la interfaz local
$IPTABLES -A INPUT -i lo -j ACCEPT

#Eliminar conexiones a la interfaz local desde el mundo exterior
$IPTABLES -A INPUT -d 127.0.0.0/8 -j REJECT

#No permitir que máquinas de la red interna se conecten al smtp de otros
#servirores en internet, deshabilitar si ud usa smtp remoto
#$IPTABLES -A FORWARD -s $INTERNALNET -p tcp --dport 25 -j DROP

#No permitir que esta MAC pueda navegar
#poner tantas lineas como mac se quieran bloquear
#$IPTABLES -A FORWARD -i $INTERNALIF -m mac --mac-source 00:14:51:27:c5:64 -j
DROP
```

```
#Permitir trafico ilimitado de la red interna que usan direcciones validas
$IPTABLES -A INPUT -i $INTERNALIF -s $INTERNALNET -j ACCEPT

#Bloquear todo tráfico  de la red externa que dice ser de la red interna
#$IPTABLES -A INPUT -i $EXTERNALIF -s $INTERNALNET -j REJECT

#No reenviar trafico SMB
$IPTABLES -A FORWARD -o $EXTERNALIF -p tcp --dport 137 -j REJECT
$IPTABLES -A FORWARD -o $EXTERNALIF -p tcp --dport 138 -j REJECT
$IPTABLES -A FORWARD -o $EXTERNALIF -p tcp --dport 139 -j REJECT
$IPTABLES -A FORWARD -o $EXTERNALIF -p udp --dport 137 -j REJECT
$IPTABLES -A FORWARD -o $EXTERNALIF -p udp --dport 138 -j REJECT
$IPTABLES -A FORWARD -o $EXTERNALIF -p udp --dport 139 -j REJECT
$IPTABLES -A INPUT -i $EXTERNALIF -p udp --dport 137 -j REJECT



#Permitir el resto del tráfico salir
$IPTABLES -A FORWARD -o $EXTERNALIF -i $INTERNALIF -j ACCEPT

#Permitir las respuestas entrar
$IPTABLES -A OUTPUT -m state --state NEW -o $EXTERNALIF -j ACCEPT
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A FORWARD -m state --state NEW -o $EXTERNALIF -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

#Permitir a esta maquina ser un servidor DHCP para su red interna
#$IPTABLES -A INPUT -i $INTERNALIF -p tcp --sport 68 --dport 67 -j ACCEPT
#$IPTABLES -A INPUT -i $INTERNALIF -p udp --sport 68 --dport 67 -j ACCEPT

#Activar en caso de implementar openvpn, interfaces tun/tap
#y puerto 1194 para openvpn
$IPTABLES -A INPUT -i tun+ -j ACCEPT
$IPTABLES -A FORWARD -i tun+ -j ACCEPT
```

```
$IPTABLES -A INPUT -i tap+ -j ACCEPT
$IPTABLES -A FORWARD -i tap+ -j ACCEPT
$IPTABLES -A INPUT -p udp --dport 1194 -j ACCEPT

# DNS
#$IPTABLES -A INPUT -p tcp --dport 53 -j ACCEPT
#$IPTABLES -A INPUT -p udp --dport 53 -j ACCEPT

#icmp
#$IPTABLES -A INPUT -s 190.180.69.189 -i $EXTERNALIF -p icmp -j LOG
$IPTABLES -A INPUT -p icmp -j ACCEPT

# ssh
$IPTABLES -A INPUT -p tcp --dport 1983 -j LOG
$IPTABLES -A INPUT -p tcp --dport 1983 -j ACCEPT
#$IPTABLES -A INPUT -p tcp --dport 1983 -j REJECT



# ftp-data
#$IPTABLES -A INPUT -p tcp  --dport 22 -j ACCEPT

# ftp
#$IPTABLES -A INPUT -p tcp  --dport 21 -j ACCEPT

# http
$IPTABLES -A INPUT -p tcp --dport 80 -j ACCEPT

# POP-3
$IPTABLES -A INPUT -p tcp --dport 110 -j ACCEPT

#SMTP
$IPTABLES -A INPUT -p tcp --dport 587 -j LOG
$IPTABLES -A INPUT -p tcp --dport 587 -j ACCEPT
```

```
#$IPTABLES -A INPUT -p tcp --dport 25 -j LOG
#$IPTABLES -A INPUT -p tcp --dport 25 -j ACCEPT

#imap
$IPTABLES -A INPUT -p tcp --dport 143 -j ACCEPT

# smtp  Una conexion por segundo
$IPTABLES -A INPUT -p tcp --dport 25 --syn -m limit --limit 2/s \
      --limit-burst 10 -j ACCEPT
$IPTABLES -A INPUT -p tcp --dport 25 --syn -j DROP
$IPTABLES -A INPUT -p tcp --dport 25 -j ACCEPT



##DNAT

#Enviar peticiones web a una maquina interna (192.168.3.202 ?)
#$IPTABLES -A PREROUTING -t nat -i $EXTERNALIF -p tcp -d $MYADDR --dport 80 \
#                -j DNAT --to 192.168.3.218:80
#$IPTABLES -A FORWARD -i $EXTERNALIF -p tcp -d 192.168.3.218 --dport 80 -j AC-
CEPT



#Smtp a un servidor interno

#$IPTABLES -A PREROUTING -t nat -i $EXTERNALIF -p tcp -d $MYADDR --dport 25 \
#                -j DNAT --to 192.168.3.219:25
#$IPTABLES -A FORWARD -i $EXTERNALIF -p tcp -d 192.168.3.219 --dport 25 -j AC-
CEPT

#$IPTABLES -A PREROUTING -t nat -i $EXTERNALIF -p tcp -d $MYADDR --dport 587
\
#                -j DNAT --to 192.168.3.219:587
#$IPTABLES -A FORWARD -i $EXTERNALIF -p tcp -d 192.168.3.219 --dport 587 -j AC-
```

```
CEPT

#$IPTABLES -A PREROUTING -t nat -i $EXTERNALIF -p tcp -d $MYADDR --dport 110
\
#                -j DNAT --to 192.168.3.219:110
#$IPTABLES -A FORWARD -i $EXTERNALIF -p tcp -d 192.168.3.219 --dport 110 -j AC-
CEPT

#$IPTABLES -A PREROUTING -t nat -i $EXTERNALIF -p tcp -d $MYADDR --dport 143
\
#                -j DNAT --to 192.168.3.202:143
#$IPTABLES -A FORWARD -i $EXTERNALIF -p tcp -d 192.168.3.202 --dport 143 -j AC-
CEPT

#ftp a un servidor interno
#$IPTABLES -A PREROUTING -t nat -i $EXTERNALIF -p tcp -d $MYADDR --dport
20:21 \
#                -j DNAT --to 192.168.3.10:25
#$IPTABLES -A FORWARD -i $EXTERNALIF -p tcp -d 192.168.0.10 --dport 20:21 -j
ACCEPT



##Puertos que deben ser denegados y guardados
$IPTABLES -A INPUT -p tcp --dport 1433 -m limit -j LOG \
                --log-prefix "Firewalled packet: MSSQL "

$IPTABLES -A INPUT -p tcp --dport 1433 -j DROP
$IPTABLES -A INPUT -p tcp --dport 6670 -m limit -j LOG \
                --log-prefix "Firewalled packet: Deepthrt "
$IPTABLES -A INPUT -p tcp --dport 6670 -j DROP
$IPTABLES -A INPUT -p tcp --dport 6711 -m limit -j LOG \
                --log-prefix "Firewalled packet: Sub7 "
$IPTABLES -A INPUT -p tcp --dport 6711 -j DROP
```

```
$IPTABLES -A INPUT -p tcp --dport 6712 -m limit -j LOG \
                --log-prefix "Firewalled packet: Sub7 "
$IPTABLES -A INPUT -p tcp --dport 6712 -j DROP
$IPTABLES -A INPUT -p tcp --dport 6713 -m limit -j LOG \
                --log-prefix "Firewalled packet: Sub7 "
$IPTABLES -A INPUT -p tcp --dport 6713 -j DROP

$IPTABLES -A INPUT -p tcp --dport 12345 -m limit -j LOG \
                --log-prefix "Firewalled packet: Netbus "
$IPTABLES -A INPUT -p tcp --dport 12345 -j DROP
$IPTABLES -A INPUT -p tcp --dport 12346 -m limit -j LOG \
                --log-prefix "Firewalled packet: Netbus "
$IPTABLES -A INPUT -p tcp --dport 12346 -j DROP
$IPTABLES -A INPUT -p tcp --dport 20034 -m limit -j LOG \
                --log-prefix "Firewalled packet: Netbus "
$IPTABLES -A INPUT -p tcp --dport 20034 -j DROP
$IPTABLES -A INPUT -p tcp --dport 31337 -m limit -j LOG \
                --log-prefix "Firewalled packet: BO "
$IPTABLES -A INPUT -p tcp --dport 31337 -j DROP
$IPTABLES -A INPUT -p tcp --dport 6000  -m limit -j LOG \
                --log-prefix "Firewalled packet: XWin "
$IPTABLES -A INPUT -p tcp --dport 6000  -j DROP

$IPTABLES -A INPUT -p udp --dport 33434:33523 -j DROP



#No guardar IGMP, muchas personas reciben enorme cantidad de este
$IPTABLES -A INPUT -p igmp -j REJECT



#Reject
$IPTABLES -A INPUT -p tcp -j REJECT --reject-with tcp-reset
$IPTABLES -A INPUT -p all -j DROP
```

```
$IPTABLES -A FORWARD -p tcp -j REJECT --reject-with tcp-reset
$IPTABLES -A FORWARD -p all -j DROP

#Aceptar demas conexiones de salida
$IPTABLES -A OUTPUT -j ACCEPT

#redireccionamiento del puerto 80 y el 443 al 3128
$IPTABLES -t nat -A PREROUTING -i $INTERNALIF -p tcp --dport 80 -j REDIRECT --to-port 3128
#$IPTABLES -t nat -A PREROUTING -i $INTERNALIF -p tcp --dport 443 -j REDIRECT --to-port 3128



#Logueamos y descartamos paquetes de la red local intentando salir
#$IPTABLES -A FORWARD -p tcp --dport 25 -j LOG
#$IPTABLES -A FORWARD -p tcp --dport 25 -j DROP
#$IPTABLES -A OUTPUT -p tcp --dport 25 -j DROP

#Enmascarar conexiones internar yendo hacia fuera.
$IPTABLES -A POSTROUTING -t nat -o $EXTERNALIF -j MASQUERADE

exit 0
```

ANEXO 2 ARCHIVO DE CONFIGURACIÓN DE SQUID

```
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.3.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443                 # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210                 # wais
acl Safe_ports port 1025-65535      # unregistered ports
acl Safe_ports port 280                 # http-mgmt
acl Safe_ports port 488                 # gss-http
acl Safe_ports port 591                 # filemaker
acl Safe_ports port 777                 # multiling http
acl CONNECT method CONNECT
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
acl sin_restriccion src "/etc/squid/reglas/sin_restriccion"
acl contabilidad src "/etc/squid/reglas/contabilidad"
acl visitas src "/etc/squid/reglas/visitas"
acl msn port            6891-6900
acl msn port 6901
acl msn port 1457
acl msn port 1461
acl msn port 1447
```

```
acl msn port 1507
acl msn_port port 1863
acl msn_url url_regex -i gateway.dll
acl msn_url url_regex -i ADSAdClient31.dll
acl msnmessenger req_mime_type ^application/x-msn-messenger$
acl msn-gat url_regex gateway.dll?
acl msn_method method POST
acl MSN_Messenger browser ^Mozilla.compatible;.MSN Messenger.
acl hotmail src 64.4.13.0/24
acl hotmail src 65.54.183.0/24
acl hotmail src 65.54.239.0/24
acl hotmail src 65.54.165.138
acl msn-dirs url_regex -i "/etc/squid/reglas/msn-dirs"
acl permitidos url_regex -i "/etc/squid/reglas/permitidos"
acl prohibidos url_regex -i "/etc/squid/reglas/prohibidos"
http_access allow sin_restriccion
http_access allow visitas
http_access deny prohibidos !permitidos
http_access deny contabilidad MSN_Messenger
http_access deny contabilidad msnmessenger
http_access deny contabilidad msn_method msn_url msn-gat
http_access deny contabilidad hotmail
http_access deny contabilidad CONNECT msn_port
http_access deny contabilidad msn
http_access allow contabilidad
http_access allow localhost
http_access deny all
icp_access allow all
http_port 3128 transparent
hierarchy_stoplist cgi-bin ?
cache_mem 8 MB
cache_dir ufs /var/spool/squid 2048 16 256
maximum_object_size 4096 KB
```

```
cache_swap_low 90
cache_swap_high 95
access_log /var/log/squid/access.log squid
cache_log /var/log/squid/cache.log
acl QUERY urlpath_regex cgi-bin \?
cache deny QUERY
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern .               0       20%     4320
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
visible_hostname Proteco_Coasin_S.A.
coredump_dir /var/spool/squid
```

ANEXO 3 LISTA DE CONTROL DE ACCESO "SIN_RESTRICCION"

```
#TECNOLOGIA 2-10#
192.168.3.2
192.168.3.3
192.168.3.4
192.168.3.5
192.168.3.6
192.168.3.7

#METROTEK 8-20
192.168.3.8
192.168.3.9
192.168.3.10
192.168.3.11
192.168.3.12
192.168.3.13
192.168.3.14
192.168.3.15
192.168.3.16
192.168.3.17
192.168.3.18
192.168.3.19
192.168.3.20

#CONTABILIDAD 21 - 40
#192.168.3.21
#192.168.3.22
#192.168.3.23
#192.168.3.24
#192.168.3.25
#192.168.3.26
```

```
#192.168.3.27
#192.168.3.28
#192.168.3.29
#192.168.3.30
#192.168.3.31
#192.168.3.32
#192.168.3.33
#192.168.3.34
#192.168.3.35
#192.168.3.36
#192.168.3.37
#192.168.3.38
#192.168.3.39
#192.168.3.40

#GERENCIA  41 - 49
192.168.3.41
192.168.3.42
192.168.3.43
192.168.3.44
192.168.3.45
192.168.3.46
192.168.3.47
192.168.3.48
192.168.3.49

#VENTAS IMPORTACIONES OPERACIONES 50 - 65
192.168.3.50
192.168.3.51
192.168.3.52
192.168.3.53
192.168.3.54
192.168.3.57
```

192.168.3.58
192.168.3.59
192.168.3.60
192.168.3.61
192.168.3.62
192.168.3.63
192.168.3.64
192.168.3.65

#EQUIPOS DE RED

192.168.3.201
192.168.3.205
192.168.3.206
192.168.3.217
192.168.3.218
192.168.3.219

ANEXO 4 LISTA DE CONTROL DE ACCESO “CONTABILIDAD”

```
#CONTABILIDAD 21 - 40
192.168.3.21
192.168.3.22
192.168.3.23
192.168.3.24
192.168.3.25
192.168.3.26
192.168.3.27
192.168.3.28
192.168.3.29
192.168.3.30
192.168.3.31
192.168.3.32
192.168.3.33
192.168.3.34
192.168.3.35
192.168.3.36
192.168.3.37
192.168.3.38
192.168.3.39
192.168.3.40
```

ANEXO 5 LISTA DE CONTROL DE ACCESO “VISITAS”

192.168.3.100
192.168.3.101
192.168.3.102
192.168.3.103
192.168.3.104
192.168.3.105
192.168.3.106
192.168.3.107
192.168.3.108
192.168.3.109
192.168.3.110
192.168.3.111
192.168.3.112
192.168.3.113
192.168.3.114
192.168.3.115
192.168.3.116
192.168.3.117
192.168.3.118
192.168.3.119
192.168.3.120
192.168.3.121
192.168.3.122
192.168.3.123
192.168.3.124
192.168.3.125
192.168.3.126
192.168.3.127
192.168.3.128
192.168.3.129

ANEXO 6 ARCHIVO DE CONFIGURACIÓN DEL CLIENTE DE OPENVPN

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
```

```
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 190.108.69.190 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody
```

```
# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca "C:\\Program Files (x86)\\OpenVPN\\config\\ca.crt"
cert "C:\\Program Files (x86)\\OpenVPN\\config\\guillermo.crt"
key "C:\\Program Files (x86)\\OpenVPN\\config\\guillermo.key"



#cert "C:\\Archivos de programa (x86)\\OpenVPN\\config\\gleon.crt"
#key "C:\\Archivos de programa (x86)\\OpenVPN\\config\\gleon.key"

# Verify server certificate by checking
```

```
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

ANEXO 7 ARCHIVO DE CONFIGURACIÓN DEL SERVIDOR DHCP

```
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style interim;
ignore client-updates;
authoritaive;
shared-network miredlocal {
        subnet 192.168.3.0 netmask 255.255.255.0 {
        option routers 192.168.3.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.3.255;
        option domain-name "proteco-coasin.com";
        option domain-name-servers 192.168.3.206 192.168.3.1;
        option netbios-name-servers 192.168.3.1;
        #option ntp-servers 200.23.51.205, 132.248.81.29, 148.234.7.30;
        range 192.168.3.130 192.168.3.140;
        default-lease-time 21600;
        max-lease-time 43200;
        }

host m2  {  option host-name "Proteco_tec_07"; hardware ethernet  00:23:45:63:d8:94; fixed-address  192.168.3.2;}

host m3  {  option host-name "Proteco_tec_07"; hardware ethernet  00:56:10:94:7e:a4; fixed-address  192.168.3.3;}

host m4  {  option host-name "pro_tec_04"; hardware ethernet  60:eb:df:dd:5e:27; fixed-address  192.168.3.4;}

host m5  {  option host-name "pro_tec_gleonb"; hardware ethernet  00:56:c7:fb:77:d6; fixed-
```

```
address  192.168.3.5;}

host m6  {  option host-name "pro_tec_gleonb"; hardware ethernet  f0:4d:98:65:96:8f; fixed-address  192.168.3.6;}

host m7  {  option host-name "DAVID_SANT10"; hardware ethernet  2c:41:78:0e:1e:b7; fixed-address  192.168.3.7;}

host m8  {  option host-name "sonyvgnc250n"; hardware ethernet  00:19:d2:6a:b5:47; fixed-address  192.168.3.8;}

host m9  {  option host-name "pro_tec_as"; hardware ethernet  e0:2a:82:e0:78:be; fixed-address  192.168.3.9;}

}
```

ANEXO 8 ARCHIVO DE CONFIGURACIÓN SERVIDOR DNS

```
options {
directory "/var/named";
#dump-file "/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
#allow-recursion { 192.168.3.0/24; 127.0.0.1; };
#allow-query { 192.168.3.0/24; 127.0.0.1; 10.8.0.0/24; };
#forwarders { 190.108.65.3; 190.108.64.2; };
#forward first;
};

zone "." IN {
type hint;
file "named.ca";
};

zone "localdomain." IN {
type master;
file "localdomain.zone";
allow-update { none; };
};

zone "localhost." IN {
type master;
file "localhost.zone";
allow-update { none; };
};

zone "0.0.127.in-addr.arpa." IN {
type master;
file "named.local";
```

```
allow-update { none; };
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa." IN {
type master;
file "named.ip6.local";
allow-update { none; };
};

zone "255.in-addr.arpa." IN {
type master;
file "named.broadcast";
allow-update { none; };
};

zone "0.in-addr.arpa." IN {
type master;
file "named.zero";
allow-update { none; };
};

# configuracion para coasin.com.ec
zone "proteco-coasin.com" {
        type master;
        file "proteco-coasin.com.zone";
        allow-update { none; };
};

zone "3.168.192.in-addr.arpa" {
        type master;
        file "3.168.192.in-addr.arpa.zone";
};
include "/etc/rndc.key";
```

ANEXO 9 ARCHIVO DE CONFIGURACIÓN DE SENDMAIL

```
divert(-1)dnl
dnl #
dnl # This is the sendmail macro config file for m4. If you make changes to
dnl # /etc/mail/sendmail.mc, you will need to regenerate the
dnl # /etc/mail/sendmail.cf file by confirming that the sendmail-cf package is
dnl # installed and then performing a
dnl #
dnl #     make -C /etc/mail
dnl #
include(`/usr/share/sendmail-cf/m4/cf.m4')dnl
VERSIONID(`setup for linux')dnl
OSTYPE(`linux')dnl
dnl #
dnl # Do not advertize sendmail version.
dnl #
dnl define(`confSMTP_LOGIN_MSG', `$j Sendmail; $b')dnl
dnl #
dnl # default logging level is 9, you might want to set it higher to
dnl # debug the configuration
dnl #
dnl define(`confLOG_LEVEL', `9')dnl
dnl #
dnl # Uncomment and edit the following line if your outgoing mail needs to
dnl # be sent out through an external mail server:
dnl #
dnl define(`SMART_HOST', `smtp.your.provider')dnl
dnl #
define(`confDEF_USER_ID', ``8:12'')dnl
dnl define(`confAUTO_REBUILD')dnl
define(`confTO_CONNECT', `1m')dnl
```

```
define(`confTRY_NULL_MX_LIST', `True')dnl
define(`confDONT_PROBE_INTERFACES', `True')dnl
define(`PROCMAIL_MAILER_PATH', `/usr/bin/procmail')dnl
define(`ALIAS_FILE', `/etc/aliases')dnl
define(`STATUS_FILE', `/var/log/mail/statistics')dnl
define(`UUCP_MAILER_MAX', `2000000')dnl
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dnl
define(`confPRIVACY_FLAGS', `authwarnings,novrfy,noexpn,restrictqrun')dnl
define(`confAUTH_OPTIONS', `A')dnl
dnl #
dnl # The following allows relaying if the user authenticates, and disallows
dnl # plaintext authentication (PLAIN/LOGIN) on non-TLS links
dnl #
dnl define(`confAUTH_OPTIONS', `A p')dnl
dnl #
dnl # PLAIN is the preferred plaintext authentication method and used by
dnl # Mozilla Mail and Evolution, though Outlook Express and other MUAs do
dnl # use LOGIN. Other mechanisms should be used if the connection is not
dnl # guaranteed secure.
dnl # Please remember that saslauthd needs to be running for AUTH.
dnl #
dnl TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl #
dnl # Rudimentary information on creating certificates for sendmail TLS:
dnl #     cd /etc/pki/tls/certs; make sendmail.pem
dnl # Complete usage:
dnl #     make -C /etc/pki/tls/certs usage
dnl #
dnl define(`confCACERT_PATH', `/etc/pki/tls/certs')dnl
dnl define(`confCACERT', `/etc/pki/tls/certs/ca-bundle.crt')dnl
```

```
dnl define(`confSERVER_CERT', `/etc/pki/tls/certs/sendmail.pem')dnl
dnl define(`confSERVER_KEY', `/etc/pki/tls/certs/sendmail.pem')dnl
dnl #
dnl # This allows sendmail to use a keyfile that is shared with OpenLDAP's
dnl # slapd, which requires the file to be readble by group ldap
dnl #
dnl define(`confDONT_BLAME_SENDMAIL', `groupreadablekeyfile')dnl
dnl #
dnl define(`confTO_QUEUEWARN', `4h')dnl
dnl define(`confTO_QUEUERETURN', `5d')dnl
dnl define(`confQUEUE_LA', `12')dnl
dnl define(`confREFUSE_LA', `18')dnl
define(`confTO_IDENT', `0')dnl
dnl FEATURE(delay_checks)dnl
FEATURE(`no_default_msa', `dnl')dnl
FEATURE(`smrsh', `/usr/sbin/smrsh')dnl
FEATURE(`mailertable', `hash -o /etc/mail/mailertable.db')dnl
FEATURE(`virtusertable', `hash -o /etc/mail/virtusertable.db')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
dnl #
dnl # The following limits the number of processes sendmail can fork to accept
dnl # incoming messages or process its message queues to 20.) sendmail refuses
dnl # to accept connections once it has reached its quota of child processes.
dnl #
dnl define(`confMAX_DAEMON_CHILDREN', `20')dnl
dnl #
dnl # Limits the number of new connections per second. This caps the overhead
dnl # incurred due to forking new sendmail processes. May be useful against
dnl # DoS attacks or barrages of spam. (As mentioned below, a per-IP address
dnl # limit would be useful but is not available as an option at this writing.)
```

```
dnl #
dnl define(`confCONNECTION_RATE_THROTTLE', `3')dnl
dnl #
dnl # The -t option will retry delivery if e.g. the user runs over his quota.
dnl #
FEATURE(local_procmail, `', `procmail -t -Y -a $h -d $u')dnl
FEATURE(`access_db', `hash -T<TMPF> -o /etc/mail/access.db')dnl
FEATURE(`blacklist_recipients')dnl
FEATURE(`relay_entire_domain')dnl
FEATURE(`relay_mail_from')dnl
EXPOSED_USER(`root')dnl
dnl #
dnl # For using Cyrus-IMAPd as POP3/IMAP server through LMTP delivery uncomment
dnl # the following 2 definitions and activate below in the MAILER section the
dnl # cyrusv2 mailer.
dnl #
dnl define(`confLOCAL_MAILER', `cyrusv2')dnl
dnl define(`CYRUSV2_MAILER_ARGS', `FILE /var/lib/imap/socket/lmtp')dnl
dnl #
dnl # The following causes sendmail to only listen on the IPv4 loopback address
dnl # 127.0.0.1 and not on any other network devices. Remove the loopback
dnl # address restriction to accept email from the internet or intranet.
dnl #
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 587 for
dnl # mail from MUAs that authenticate. Roaming users who can't reach their
dnl # preferred sendmail daemon due to port 25 being blocked or redirected find
dnl # this useful.
dnl #
dnl DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 465, but
```

```
dnl # starting immediately in TLS mode upon connecting. Port 25 or 587 followed
dnl # by STARTTLS is preferred, but roaming clients using Outlook Express can't
dnl # do STARTTLS on ports other than 25. Mozilla Mail can ONLY use STARTTLS
dnl # and doesn't support the deprecated smtps; Evolution <1.1.1 uses smtps
dnl # when SSL is enabled-- STARTTLS support is available in version 1.1.1.
dnl #
dnl # For this to work your OpenSSL certificates must be configured.
dnl #
dnl DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl
dnl #
dnl # The following causes sendmail to additionally listen on the IPv6 loopback
dnl # device. Remove the loopback address restriction listen to the network.
dnl #
dnl DAEMON_OPTIONS(`port=smtp,Addr=::1, Name=MTA-v6, Family=inet6')dnl
dnl #
dnl # enable both ipv6 and ipv4 in sendmail:
dnl #
dnl DAEMON_OPTIONS(`Name=MTA-v4, Family=inet, Name=MTA-v6, Family=inet6')
dnl #
dnl # We strongly recommend not accepting unresolvable domains if you want to
dnl # protect yourself from spam. However, the laptop and users on computers
dnl # that do not have 24x7 DNS do need this.
dnl #
FEATURE(`accept_unresolvable_domains')dnl
dnl #
dnl FEATURE(`relay_based_on_MX')dnl
dnl #
dnl # Also accept email sent to "localhost.localdomain" as local email.
dnl #
LOCAL_DOMAIN(`localhost.localdomain')dnl
dnl #
dnl # The following example makes mail from this host and any additional
dnl # specified domains appear to be sent from mydomain.com
```

```
dnl #
dnl MASQUERADE_AS(`mydomain.com')dnl
dnl #
dnl # masquerade not just the headers, but the envelope as well
dnl #
dnl FEATURE(masquerade_envelope)dnl
dnl #
dnl # masquerade not just @mydomainalias.com, but @*.mydomainalias.com as well
dnl #
dnl FEATURE(masquerade_entire_domain)dnl
dnl #
dnl MASQUERADE_DOMAIN(localhost)dnl
dnl MASQUERADE_DOMAIN(localhost.localdomain)dnl
dnl MASQUERADE_DOMAIN(mydomainalias.com)dnl
dnl MASQUERADE_DOMAIN(mydomain.lan)dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
dnl MAILER(cyrusv2)dnl
DAEMON_OPTIONS(`Name=MTA')
DAEMON_OPTIONS(`Name=MSA,Port=587')
```

ANEXO 10 ARCHIVO DE CONFIGURACIÓN DE LDAP.CONF

```
host 192.168.3.206
base dc=proteco,dc=local
uri ldap://dcp.proteco.local/
binddn cn=linux,ou=TECNOLOGIA,dc=proteco,dc=local
bindpw password
timelimit 120
bind_timelimit 120
idle_timelimit 3600

nss_base_passwd dc=proteco,dc=local?sub
nss_base_shadow dc=proteco,dc=local?sub
nss_base_group dc=proteco,dc=local?sub

nss_map_objectclass posixAccount User
nss_map_objectclass shadowAccount User
nss_map_objectclass posixGroup Group
nss_map_attribute uid sAMAccountName
nss_map_attribute uidNumber uidNumber
nss_map_attribute gidNumber gidNumber
nss_map_attribute loginShell loginShell
nss_map_attribute uniqueMember member
nss_map_attribute homeDirectory unixHomeDirectory

nss_initgroups_ignoreusers
root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mailman,nscd,gdm

pam_login_attribute msSFU30Name
pam_filter objectclass=User
ssl no
pam_password md5
```

ANEXO 11 ARCHIVO DE CONFIGURACIÓN DE NSSWITCH.COF

```
passwd:     files winbind
shadow:     files
group:      files winbind

hosts:      files dns

bootparams: nisplus [NOTFOUND=return] files

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files

netgroup:   nisplus

publickey:  nisplus

automount:  files nisplus
aliases:    files nisplus
```

ANEXO 12 ARCHIVO DE CONFIGURACIÓN DE SYSTEM-AUTH-AC

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.

auth sufficient /lib/security/$ISA/pam_winbind.so
auth sufficient /lib/security/$ISA/pam_unix.so nullok_secure use_first_pass
auth required   /lib/security/$ISA/pam_deny.so

account sufficient /lib/security/$ISA/pam_winbind.so
account required   /lib/security/$ISA/pam_unix.so

password requisite  /lib/security/$ISA/pam_cracklib.so retry=3
password sufficient /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
password required   /lib/security/$ISA/pam_deny.so

session  required   /lib/security/$ISA/pam_mkhomedir.so skel=/etc/skel umask=0077
session  required   /lib/security/$ISA/pam_limits.so
session  required   /lib/security/$ISA/pam_unix.so
```

ANEXO 13 ARCHIVO DE CONFIGURACIÓN DE KRB5.CONF

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = PROTECO.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 PROTECO.LOCAL = {
  kdc = dcp.proteco.local
  admin_server = dcp.proteco.local:749
  default_domain = proteco.local }

[domain_realm]
 .proteco.local = PROTECO.LOCAL
 proteco.local = PROTECO.LOCAL

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false  }
```

ANEXO 14 ARCHIVO DE CONFIGURACIÓN DE SMB.CONF

```
[global]
workgroup = PROTECO
realm = PROTECO.LOCAL
netbios name = server1
server string =
security = ads
use kerberos keytab = true
hosts allow = 192.168. 127. 10.
load printers = no
log file = /var/log/samba/%m.log
client use spnego = yes
max log size = 50
log level = 1
password server = DCP.PROTECO.LOCAL
idmap uid = 10000 - 20000
idmap gid = 10000 - 20000
winbind enum users = yes
winbind enum groups = yes
winbind cache time = 10
winbind nested groups = yes
;winbind nss info = template sfu
winbind use default domain = no
#wins server = 192.168.1.15 192.168.1.16
template homedir = /home/%U
template shell = /bin/bash
;idmap backend = idmap_ad
dns proxy = no
domain master = no
preferred master = no
[Departamento1]
```

```
        comment     = departamento1
        path        = /var/tecnologia
        valid users = proteco\gleon
        public      = no
        writable    = yes
        printable   = no

[Departamento2]
        comment = departamento2
        path = /var/helpdesk
        valid users = proteco\gleon
        writable = no
        #write list = proteco\gleon

[Departamento3]
        comment = departmanet3
        path = /var/proyectos
        valid users = proteco\abolanos,
        write list = proteco\abolanos,
        writable = yes
```

ANEXO 15 ARCHIVO DE CONFIGURACIÓN DE SERVIDOR FTP

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_file=/var/log/xferlog
xferlog_std_format=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
listen=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
```

ANEXO 16 ARCHIVO DE COFIGURACIOÓN BACKUPPC /etc/backuppc/config.pl

```
$ENV{'PATH'} = '/bin:/usr/bin';
delete @ENV{'IFS', 'CDPATH', 'ENV', 'BASH_ENV'};
$Conf{ServerHost} = 'backup-server';
chomp($Conf{ServerHost});
$Conf{ServerPort} = '-1';
$Conf{ServerMesgSecret} = '';
$Conf{MyPath} = '/bin';
$Conf{UmaskMode} = '23';
$Conf{WakeupSchedule} = [
  '1',
  '2',
  '3',
  '4',
  '5',
  '6',
  '7',
  '8',
  '9',
  '10',
  '11',
  '12',
  '13',
  '14',
  '15',
  '16',
  '17',
  '18',
  '19',
  '20',
  '21',
  '22',
```

```
  '23'
];
$Conf{MaxBackups} = '4';
$Conf{MaxUserBackups} = '4';
$Conf{MaxPendingCmds} = '15';
$Conf{CmdQueueNice} = '10';
$Conf{MaxBackupPCNightlyJobs} = '2';
$Conf{BackupPCNightlyPeriod} = '1';
$Conf{MaxOldLogFiles} = '14';
$Conf{DfPath} = '/bin/df';
$Conf{DfCmd} = '$dfPath $topDir';
$Conf{SplitPath} = '/usr/bin/split';
$Conf{ParPath} = undef;
$Conf{CatPath} = '/bin/cat';
$Conf{GzipPath} = '/bin/gzip';
$Conf{Bzip2Path} = '/bin/bzip2';
$Conf{DfMaxUsagePct} = '95';
$Conf{TrashCleanSleepSec} = '300';
$Conf{DHCPAddressRanges} = [];
$Conf{BackupPCUser} = 'backuppc';
$Conf{TopDir} = '/var/lib/backuppc';
$Conf{ConfDir} = '/etc/backuppc';
$Conf{LogDir} = '/var/lib/backuppc/log';
$Conf{InstallDir} = '/usr/share/backuppc';
$Conf{CgiDir} = '/usr/share/backuppc/cgi-bin';
$Conf{BackupPCUserVerify} = '1';
$Conf{HardLinkMax} = '31999';
$Conf{PerlModuleLoad} = undef;
$Conf{ServerInitdPath} = undef;
$Conf{ServerInitdStartCmd} = '';
$Conf{FullPeriod} = '6.97';
$Conf{IncrPeriod} = '0.97';
$Conf{FullKeepCnt} = [
```

```
  '1'
];
$Conf{FullKeepCntMin} = '1';
$Conf{FullAgeMax} = '90';
$Conf{IncrKeepCnt} = '6';
$Conf{IncrKeepCntMin} = '1';
$Conf{IncrAgeMax} = '30';
$Conf{IncrLevels} = [
  '1'
];
$Conf{BackupsDisable} = '0';
$Conf{PartialAgeMax} = '3';
$Conf{IncrFill} = '0';
$Conf{RestoreInfoKeepCnt} = '10';
$Conf{ArchiveInfoKeepCnt} = '10';
$Conf{BackupFilesOnly} = {};
$Conf{BackupFilesExclude} = {};
$Conf{BlackoutBadPingLimit} = '3';
$Conf{BlackoutGoodCnt} = '7';
$Conf{BlackoutPeriods} = [
  {
    'hourEnd' => '19.5',
    'weekDays' => [
      '1',
      '2',
      '3',
      '4',
      '5'
    ],
    'hourBegin' => '7'
  }
];
$Conf{BackupZeroFilesIsFatal} = '1';
```

```
$Conf{XferMethod} = 'smb';
$Conf{XferLogLevel} = '1';
$Conf{ClientCharset} = '';
$Conf{ClientCharsetLegacy} = 'iso-8859-1';
$Conf{SmbShareName} = [
  'C$'
];
$Conf{SmbShareUserName} = '';
$Conf{SmbSharePasswd} = '';
$Conf{SmbClientPath} = '/usr/bin/smbclient';
$Conf{SmbClientFullCmd} = '$smbClientPath \\\\$host\\$shareName $I_option -U
$userName -E -d 1 -c tarmode\\ full -Tc$X_option - $fileList';
$Conf{SmbClientIncrCmd} = '$smbClientPath \\\\$host\\$shareName $I_option -U
$userName -E -d 1 -c tarmode\\ full -TcN$X_option $timeStampFile - $fileList';
$Conf{SmbClientRestoreCmd} = '$smbClientPath \\\\$host\\$shareName $I_option -U
$userName -E -d 1 -c tarmode\\ full -Tx -';
$Conf{TarShareName} = [
  '/'
];
$Conf{TarClientCmd} = '$sshPath -q -x -n -l root $host env LC_ALL=C $tarPath -c -v -f - -
C $shareName+ --totals';
$Conf{TarFullArgs} = '$fileList+';
$Conf{TarIncrArgs} = '--newer=$incrDate+ $fileList+';
$Conf{TarClientRestoreCmd} = '$sshPath -q -x -l root $host env LC_ALL=C $tarPath -x -p
--numeric-owner --same-owner -v -f - -C $shareName+';
$Conf{TarClientPath} = '/bin/tar';
$Conf{RsyncClientPath} = '/usr/bin/rsync';
$Conf{RsyncClientCmd} = '$sshPath -q -x -l root $host $rsyncPath $argList+';
$Conf{RsyncClientRestoreCmd} = '$sshPath -q -x -l root $host $rsyncPath $argList+';
$Conf{RsyncShareName} = [
  '/'
];
$Conf{RsyncdClientPort} = '873';
```

```
$Conf{RsyncdUserName} = '';
$Conf{RsyncdPasswd} = '';
$Conf{RsyncdAuthRequired} = '1';
$Conf{RsyncCsumCacheVerifyProb} = '0.01';
$Conf{RsyncArgs} = [
  '--numeric-ids',
  '--perms',
  '--owner',
  '--group',
  '-D',
  '--links',
  '--hard-links',
  '--times',
  '--block-size=2048',
  '--recursive'
];
$Conf{RsyncArgsExtra} = [];
$Conf{RsyncRestoreArgs} = [
  '--numeric-ids',
  '--perms',
  '--owner',
  '--group',
  '-D',
  '--links',
  '--hard-links',
  '--times',
  '--block-size=2048',
  '--relative',
  '--ignore-times',
  '--recursive'
];
$Conf{FtpShareName} = [
  ''
```

```
];
$Conf{FtpUserName} = '';
$Conf{FtpPasswd} = '';
$Conf{FtpPassive} = '1';
$Conf{FtpBlockSize} = '10240';
$Conf{FtpPort} = '21';
$Conf{FtpTimeout} = '120';
$Conf{FtpFollowSymlinks} = '0';
$Conf{ArchiveDest} = '/tmp';
$Conf{ArchiveComp} = 'gzip';
$Conf{ArchivePar} = '0';
$Conf{ArchiveSplit} = '0';
$Conf{ArchiveClientCmd} = '$Installdir/bin/BackupPC_archiveHost $tarCreatePath $split-
path $parpath $host $backupnumber $compression $compext $splitsize $archiveloc $parfile
*';
$Conf{SshPath} = '/usr/bin/ssh';
$Conf{NmbLookupPath} = '/usr/bin/nmblookup';
$Conf{NmbLookupCmd} = '$nmbLookupPath -A $host';
$Conf{NmbLookupFindHostCmd} = '$nmbLookupPath $host';
$Conf{FixedIPNetBiosNameCheck} = '0';
$Conf{PingPath} = '/bin/ping';
$Conf{Ping6Path} = undef;
$Conf{PingCmd} = '$pingPath -c 1 $host';
$Conf{PingMaxMsec} = '20';
$Conf{CompressLevel} = '3';
$Conf{ClientTimeout} = '72000';
$Conf{MaxOldPerPCLogFiles} = '12';
$Conf{DumpPreUserCmd} = undef;
$Conf{DumpPostUserCmd} = undef;
$Conf{DumpPreShareCmd} = undef;
$Conf{DumpPostShareCmd} = undef;
$Conf{RestorePreUserCmd} = undef;
$Conf{RestorePostUserCmd} = undef;
```

```
$Conf{ArchivePreUserCmd} = undef;
$Conf{ArchivePostUserCmd} = undef;
$Conf{UserCmdCheckStatus} = '0';
$Conf{ClientNameAlias} = undef;
$Conf{SendmailPath} = '/usr/sbin/sendmail';
$Conf{EMailNotifyMinDays} = '2.5';
$Conf{EMailFromUserName} = 'backuppc';
$Conf{EMailAdminUserName} = 'backuppc';
$Conf{EMailUserDestDomain} = '';
$Conf{EMailNoBackupEverSubj} = undef;
$Conf{EMailNoBackupEverMesg} = undef;
$Conf{EMailNotifyOldBackupDays} = '7';
$Conf{EMailNoBackupRecentSubj} = undef;
$Conf{EMailNoBackupRecentMesg} = undef;
$Conf{EMailNotifyOldOutlookDays} = '5';
$Conf{EMailOutlookBackupSubj} = undef;
$Conf{EMailOutlookBackupMesg} = undef;
$Conf{EMailHeaders} = 'MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
';
$Conf{CgiAdminUserGroup} = 'backuppc';
$Conf{CgiAdminUsers} = 'backuppc';
$Conf{CgiURL} = 'http://backup-server/backuppc/index.cgi';
$Conf{Language} = 'es';
$Conf{CgiUserHomePageCheck} = '';
$Conf{CgiUserUrlCreate} = 'mailto:%s';
$Conf{CgiDateFormatMMDD} = '1';
$Conf{CgiNavBarAdminAllHosts} = '1';
$Conf{CgiSearchBoxEnable} = '1';
$Conf{CgiNavBarLinks} = [
  {
    'link' => '?action=view&type=docs',
    'lname' => 'Documentation',
```

```
    'name' => undef
  },
  {
    'link' => 'http://backuppc.wiki.sourceforge.net',
    'lname' => undef,
    'name' => 'Wiki'
  },
  {
    'link' => 'http://backuppc.sourceforge.net',
    'lname' => undef,
    'name' => 'SourceForge'
  }
];
$Conf{CgiStatusHilightColor} = {
  'Reason_backup_failed' => '#ffcccc',
  'Reason_backup_done' => '#ccffcc',
  'Reason_backup_canceled_by_user' => '#ff9900',
  'Reason_no_ping' => '#ffff99',
  'Disabled_OnlyManualBackups' => '#d1d1d1',
  'Status_backup_in_progress' => '#66cc99',
  'Disabled_AllBackupsDisabled' => '#d1d1d1'
};
$Conf{CgiHeaders} = '<meta http-equiv="pragma" content="no-cache">';
$Conf{CgiImageDir} = '/usr/share/backuppc/image';
$Conf{CgiExt2ContentType} = {};
$Conf{CgiImageDirURL} = '/backuppc/image';
$Conf{CgiCSSFile} = 'BackupPC_stnd.css';
$Conf{CgiUserConfigEditEnable} = '1';
$Conf{CgiUserConfigEdit} = {
  'EMailOutlookBackupSubj' => '1',
  'ClientCharset' => '1',
  'TarFullArgs' => '1',
  'RsyncdPasswd' => '1',
```

```
'FtpBlockSize' => '1',
'IncrKeepCnt' => '1',
'PartialAgeMax' => '1',
'FixedIPNetBiosNameCheck' => '1',
'SmbShareUserName' => '1',
'EMailFromUserName' => '1',
'ArchivePreUserCmd' => '0',
'PingCmd' => '0',
'FullAgeMax' => '1',
'FtpUserName' => '1',
'PingMaxMsec' => '1',
'CompressLevel' => '1',
'DumpPreShareCmd' => '0',
'BackupFilesOnly' => '1',
'EMailNotifyOldBackupDays' => '1',
'EMailAdminUserName' => '1',
'RsyncCsumCacheVerifyProb' => '1',
'BlackoutPeriods' => '1',
'NmbLookupFindHostCmd' => '0',
'MaxOldPerPCLogFiles' => '1',
'TarClientCmd' => '0',
'EMailNotifyOldOutlookDays' => '1',
'SmbSharePasswd' => '1',
'SmbClientIncrCmd' => '0',
'FullKeepCntMin' => '1',
'RsyncArgs' => '1',
'FtpFollowSymlinks' => '1',
'ArchiveComp' => '1',
'TarIncrArgs' => '1',
'EMailUserDestDomain' => '1',
'TarClientPath' => '0',
'RsyncClientCmd' => '0',
'IncrFill' => '1',
```

```
'RestoreInfoKeepCnt' => '1',
'UserCmdCheckStatus' => '0',
'RsyncdClientPort' => '1',
'IncrAgeMax' => '1',
'RsyncdUserName' => '1',
'RsyncRestoreArgs' => '1',
'ClientCharsetLegacy' => '1',
'SmbClientFullCmd' => '0',
'ArchiveInfoKeepCnt' => '1',
'FtpShareName' => '1',
'BackupZeroFilesIsFatal' => '1',
'EMailNoBackupRecentMesg' => '1',
'FtpPort' => '1',
'FullKeepCnt' => '1',
'TarShareName' => '1',
'EMailNoBackupEverSubj' => '1',
'TarClientRestoreCmd' => '0',
'EMailNoBackupRecentSubj' => '1',
'ArchivePar' => '1',
'XferLogLevel' => '1',
'ArchiveDest' => '1',
'RsyncdAuthRequired' => '1',
'ClientTimeout' => '1',
'EMailNotifyMinDays' => '1',
'SmbClientRestoreCmd' => '0',
'ClientNameAlias' => '1',
'DumpPostShareCmd' => '0',
'IncrLevels' => '1',
'EMailOutlookBackupMesg' => '1',
'BlackoutBadPingLimit' => '1',
'BackupFilesExclude' => '1',
'FullPeriod' => '1',
'RsyncClientRestoreCmd' => '0',
```

```
  'ArchivePostUserCmd' => '0',
  'IncrPeriod' => '1',
  'RsyncShareName' => '1',
  'FtpTimeout' => '1',
  'RestorePostUserCmd' => '0',
  'BlackoutGoodCnt' => '1',
  'ArchiveClientCmd' => '0',
  'ArchiveSplit' => '1',
  'FtpRestoreEnabled' => '1',
  'XferMethod' => '1',
  'NmbLookupCmd' => '0',
  'BackupsDisable' => '1',
  'SmbShareName' => '1',
  'FtpPasswd' => '1',
  'RestorePreUserCmd' => '0',
  'RsyncArgsExtra' => '1',
  'IncrKeepCntMin' => '1',
  'EMailNoBackupEverMesg' => '1',
  'EMailHeaders' => '1',
  'DumpPreUserCmd' => '0',
  'RsyncClientPath' => '0',
  'DumpPostUserCmd' => '0'
};
```