ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UN SISTEMA DE SEGURIDAD OPERACIONAL PARA MEJORAR LA PROTECCIÓN EN LAS REDES LAN Y WAN DE PETROINDUSTRIAL

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

MARCELO DAVID PALLO BARONA
david_pallo@hotmail.com

DIRECTOR: DR. LUIS CORRALES PhD
luisco5049@yahoo.com

Quito, Octubre de 2009

DECLARACIÓN

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

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

Marcelo David Pallo Barona

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Marcelo David Pallo Barona, bajo mi supervisión.

Dr. Luis Corrales

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Al culminar este proyecto de titulación, debo dar infinitas gracias a Dios por darme la dicha de existir e iluminar siempre mi camino, brindándome una hermosa familia y buenos amigos.

A mis padres por su apoyo incondicional, por brindarme la oportunidad de estudiar para poder enfrentar de una mejor manera mi futuro.

A mis amigos por compartir momentos inolvidables de mi vida, por brindarme su amistad desinteresada, que me motivaron a luchar por mis objetivos.

Al Dr. Luis Corrales por aceptar ser mi tutor, quien estuvo siempre dispuesto a compartir sus valiosos conocimientos para poder culminar satisfactoriamente el presente proyecto de titulación.

A la Escuela Politécnica Nacional, a todos mis maestros que me brindaron sus vastas enseñanzas a cada instante de mi carrera.

A Petroindustrial por su apertura y colaboración durante el desarrollo de este proyecto.

David Pallo Barona.

DEDICATORIA

Con profundo cariño dedico este trabajo, a los seres más importantes en mi vida; mis padres, que siempre me brindaron su amor y comprensión, por ser quienes me inculcaron buenos valores morales, me enseñaron lo importante de la honestidad, trabajo y humildad, a ellos que con sus consejos y total apoyo supieron darme el ejemplo de constancia y superación, sobre todo me enseñaron que las cosas que perduran en la vida se consiguen con esfuerzo y sacrificio, que Dios los bendiga y les cuide siempre.

David Pallo Barona.

CONTENIDO

ÍNDICE GENERAL

CAPÍTULO 2

ANÁLISIS DE LAS TECNOLOGÍAS DE SEGURIDAD PARA REDES

CAPÍTULO 3

DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

CAPÍTULO 4

DETERMINACIÓN DE COSTOS REFERENCIALES DEL SISTEMA DE SEGURIDAD

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE FIGURAS

CAPITULO 1
ESTUDIO DEL SISTEMA DE SEGURIDAD ACTUAL Y DE COMUNICACIÓN DE PETROINDUSTRIAL

CAPÍTULO 2
ANÁLISIS DE LAS TECNOLOGÍAS DE SEGURIDAD PARA REDES

CAPÍTULO 3

DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

ÍNDICE DE TABLAS

CAPITULO 1

ESTUDIO DEL SISTEMA DE SEGURIDAD ACTUAL Y DE COMUNICACIÓN DE PETROINDUSTRIAL

CAPÍTULO 3

DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

CAPITULO 4

DETERMINACIÓN DE COSTOS REFERENCIALES DEL SISTEMA DE SEGURIDAD

RESUMEN

Petroindustrial como filial de Petroecuador, tiene a su cargo tres Distritos a nivel nacional los cuales son: Refinería Estatal Esmeraldas, Refinería La Libertad y Complejo Industrial Shushufindi, cada uno de estos aportan considerablemente al desarrollo económico del país y son presa fácil de las amenazas que se suscitan diariamente en Internet ya que cada uno de estos posee un enlace directo con diferentes proveedores del servicio. El objetivo de este trabajo fue diseñar un sistema de seguridad operacional para mejorar la protección en las redes LAN y WAN de Petroindustrial.

Para cumplir con este objetivo se realizó el estudio de tecnologías de seguridad como firewall, IPS, IDS, Proxy, controlador de ancho de banda, sistemas de monitoreo. Además se investigó sobre la administración unificada de amenazas (UTM, Unified Threat Management), la cual fue utilizada para este diseño, ya que permite desarrollar en forma integral múltiples medidas de seguridad en una sola plataforma y además cuenta con muchas aplicaciones para este fin.

Se compararon dos alternativas importantes de equipos como son: Juniper y Linserver UCNC (Universal Corporate Network Center), de acuerdo a los requerimientos actuales de la empresa, para elegir la mejor opción de dispositivo UTM que garantice la seguridad de la información.

Para solucionar el problema de la falta de seguridad en la red de Petroindustrial, se diseña la seguridad alrededor del equipo Linserver UCNC, el cual se basa en la plataforma Open Source, específicamente Enterprise Linux Red Hat Advanced Server 4.4. Esta plataforma dentro de los Enterprise Linux a nivel mundial es una de las más reconocidas por su confiabilidad dentro de los sistemas de misión crítica como Bases de Datos DB2 y Oracle, SQL, servidores de comunicaciones corporativos, servidores de procesamiento de datos especiales. Esta plataforma permitirá obtener servicios de alto manejo de tráfico como Mail, DNS, Web, Webmail, AntiSpam, Antivirus de Gateway, Proxy, VPN, IDS, IPS y Firewall, que se requiera en el futuro, de manera fácil y sencilla.

PRESENTACIÓN

En la actualidad millones de personas en el mundo ingresan a Internet para realizar un sin número de tareas como: envío de correo electrónico, navegación en la World Wide Web e incluso hacer transacciones bancarias, compras etc, por lo que se debe estar conscientes que este es un entorno potencialmente vulnerable. Por esta razón las empresas están expuestas a la alteración de registros o base de datos, copia de información privada, obtención de contraseñas, denegación de servicios, caída de servidores y otros factores más. Por tal motivo en el presente proyecto de titulación se pretende contribuir a la protección de la información e infraestructura de Petroindustrial, con el diseño de un sistema de seguridad operacional para proteger las redes LAN y WAN.

Con este objetivo, el trabajo ha sido dividido en cinco capítulos que cubren lo siguiente:

En el primer capítulo se estudia la red actual de Petroindustrial, para tener un conocimiento claro de los riesgos y vulnerabilidades a la que está expuesta esta empresa en relación a la seguridad de la información, para de esta manera presentar una solución acorde a sus necesidades. También se definen los lineamientos de la planeación y el diseño de un modelo de seguridad con el objetivo de establecer una cultura de seguridad en la organización.

En el segundo capítulo se describen los conceptos más importantes referentes a Seguridad de Redes, como son: amenazas, ataques, riesgos y vulnerabilidades que puede sufrir la empresa durante la transmisión de información. También se realiza el estudio de las principales tecnologías de seguridad, como firewall, IPS, IDS, controlador de ancho de banda, con los cuales se puede brindar una administración segura de las redes LAN y WAN de la empresa.

Por otra parte, en el tercer capítulo se realiza el diseño del sistema de seguridad operacional para la protección de las redes LAN y WAN de Petroindustrial, para lo

cual se efectúa una comparación de equipos y tecnologías que cumplan los requerimientos establecidos por la empresa.

Luego, en el cuarto capítulo se da a conocer los costos referenciales del hardware y software de las dos propuestas tentativas, también costos adicionales de una futura implementación del presente diseño.

Por último, en el quinto capítulo, se extraen conclusiones y recomendaciones obtenidas luego de haber desarrollado el presente proyecto de titulación.

CAPÍTULO 1

ESTUDIO DEL SISTEMA DE SEGURIDAD ACTUAL Y DE COMUNICACIÓN DE PETROINDUSTRIAL

Hoy en día es de primordial importancia salvaguardar la información digital de una empresa, para proteger la infraestructura y los activos de la misma, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos; y las responsabilidades que debe asumir cada uno de los empleados de la organización para apoyar este objetivo.

Con este objetivo, en este trabajo se diseña un sistema de seguridad informática, donde se definirán los lineamientos de un modelo de seguridad con el fin de establecer esta cultura en la organización. Asimismo, buscará guiarla a redactar sus propios procedimientos de seguridad, los cuales deberán estar enmarcados en las políticas que conforman este plan.

1.1 INFORMACIÓN GENERAL DE PETROINDUSTRIAL [12]

1.1.1 PETROINDUSTRIAL COMO FILIAL DE PETROECUADOR

La Empresa Estatal Petróleos del Ecuador, Petroecuador, tiene por objeto el desarrollo de actividades en todas las fases de la industria petrolera en el país.

Petroecuador es la matriz ejecutiva de un grupo formado por tres empresas filiales, especializadas en las siguientes actividades hidrocarburíferas:

- Exploración y explotación: PETROPRODUCCION
- Industrialización: PETROINDUSTRIAL
- Comercialización y transporte: PETROCOMERCIAL

En el ejercicio de sus actividades, Petroecuador y sus empresas filiales preservan el equilibrio ecológico, previniendo y controlando la contaminación ambiental, así como evitando que sus actividades afecten negativamente a la organización económica y social de las poblaciones asentadas en las zonas donde éstas se realizan.

Por ende Petroindustrial es la filial de Petroecuador encargada de transformar los hidrocarburos mediante procesos de refinación para producir derivados que satisfagan la demanda interna del país.

1.1.2 DESCRIPCIÓN HISTÓRICA DE PETROINDUSTRIAL

La Empresa Estatal de Industrialización de Petróleos del Ecuador: Petroindustrial fue creada el 26 de diciembre de 1989, como parte del proceso de transformación empresarial de CEPE (Corporación Estatal Petrolera Ecuatoriana), con el siguiente objetivo: "Óptima utilización de los hidrocarburos, que pertenecen al patrimonio inalienable e intangible del Estado, para el desarrollo económico y social del país, de acuerdo con la política nacional de hidrocarburos establecida por el Presidente de la República, incluyendo la investigación científica y la generación y transferencia de tecnología".

1.1.3 ORGANIZACIÓN FUNCIONAL DE PETROINDUSTRIAL

Petroindustrial está estructurada por: el Consejo de Administración, la Vicepresidencia, la Subgerencia de Operaciones, la Subgerencia de Proyectos y dependencias técnico administrativas de gestión empresarial.

El Consejo de Administración de Petroecuador es el órgano superior de dirección, encargado de formular las políticas y de controlar su cumplimiento.

El Vicepresidente de Petroindustrial es el representante legal de la empresa y el responsable directo de la gestión técnica, financiera y administrativa de la filial.

En la Figura 1.1 se muestra el diagrama de la estructura organizacional de la Matriz de Petroindustrial.

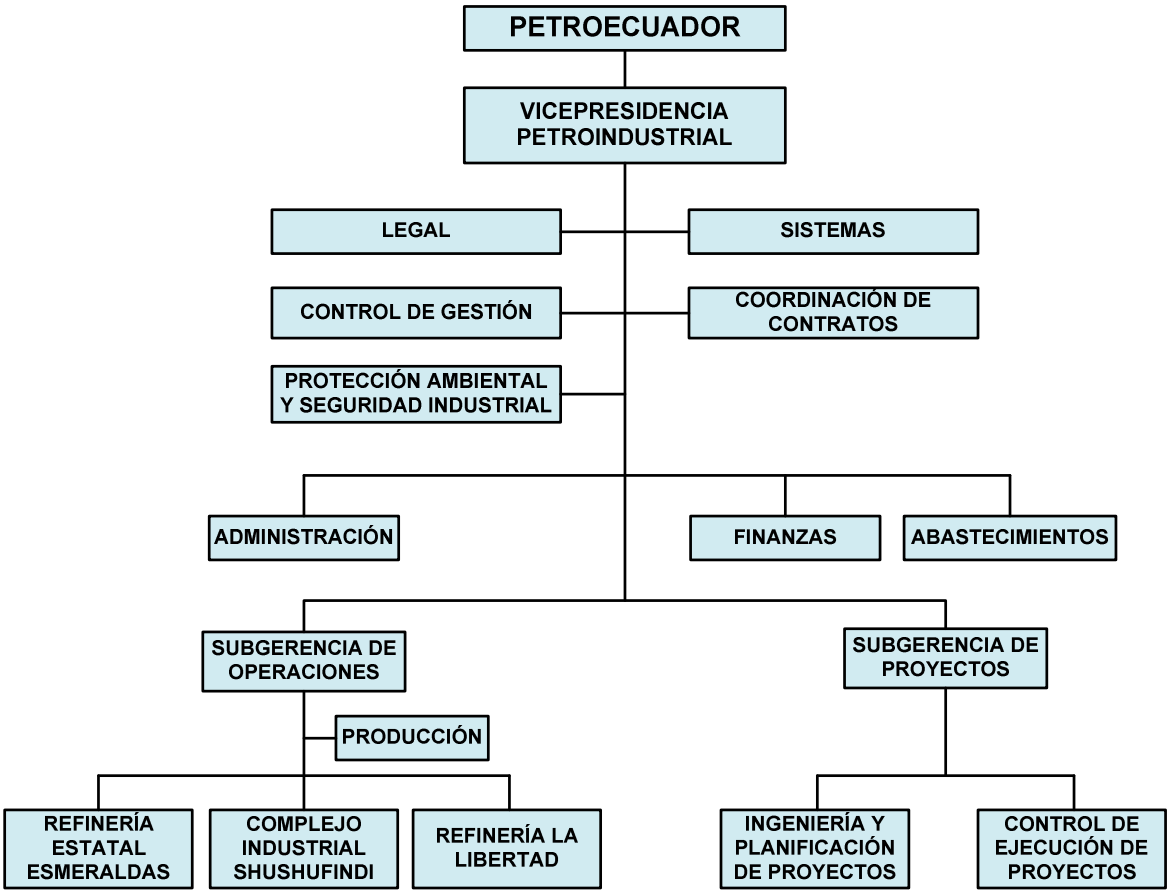


Figura 1.1 Estructura Organizacional de la Matriz de Petroindustrial [12]

1.1.3.1 Misión de Petroindustrial

Producir combustibles y otros derivados del petróleo con estándares de calidad mundial, preservando estrictamente el medio ambiente y contribuyendo al desarrollo productivo del Ecuador.

1.1.3.2 Visión de Petroindustrial

Empresa de industrialización de petróleo, de propiedad del Estado Ecuatoriano, con capacidad estratégica, flexibilidad organizacional y cultura empresarial competitiva a nivel mundial, que opera con estándares internacionales de eficiencia y mantiene armonía con los recursos socio-ambientales.

1.1.3.3 Objetivo Global de la Empresa

Industrializar hidrocarburos en el país, para producir derivados a través de una eficiente gestión empresarial, preservando el equilibrio ecológico, previniendo y controlando la contaminación ambiental.

1.1.3.4 Políticas a largo plazo

Incrementar la producción nacional de derivados del petróleo para abastecer la demanda interna del país y convertir al Ecuador en exportador de derivados, con el consecuente beneficio económico para la economía nacional.

1.1.4 PETROINDUSTRIAL Y SUS REFINERÍAS A NIVEL NACIONAL

Petroindustrial filial de Petroecuador tiene a cargo la administración de tres Refinerías a nivel nacional, las mismas que cumplen un papel muy importante en la industrialización del crudo, para el desarrollo del país y son: Refinería Estatal de Esmeraldas (REE), Refinería La Libertad (RLL) y Complejo Industrial Shushufindi (CIS).

1.1.4.1 Refinería Estatal de Esmeraldas (REE)

La REE está situada en la provincia de Esmeraldas en el sector noroccidental del país. Fue diseñada y construida entre 1975 y 1977 para procesar 55.600BPD[1]. En 1987 se amplío a 90.000BPD.

Luego de 20 años en 1997 amplió sus instalaciones para procesar 110.000BPD, adaptándose para procesar crudos más pesados, incorporando nuevas unidades para mejorar la calidad de los combustibles y minimizar el impacto ambiental. Se encuentra a una distancia de 7 Km de la ciudad de Esmeraldas, en la vía hacia Atacames.

Está a 300m en línea recta al Río Teaone, 3Km al Río Esmeraldas y 3,8Km al Océano Pacífico.

En la Figura 1.2 se muestran fotos de la Refinería Estatal de Esmeraldas.

Figura 1.2 Refinería Estatal de Esmeraldas [12]

En la Figura 1.3 se muestra el diagrama de la estructura organizacional de la Refinería Estatal de Esmeraldas.

[1] **BPD**: Barriles de petróleo diarios.

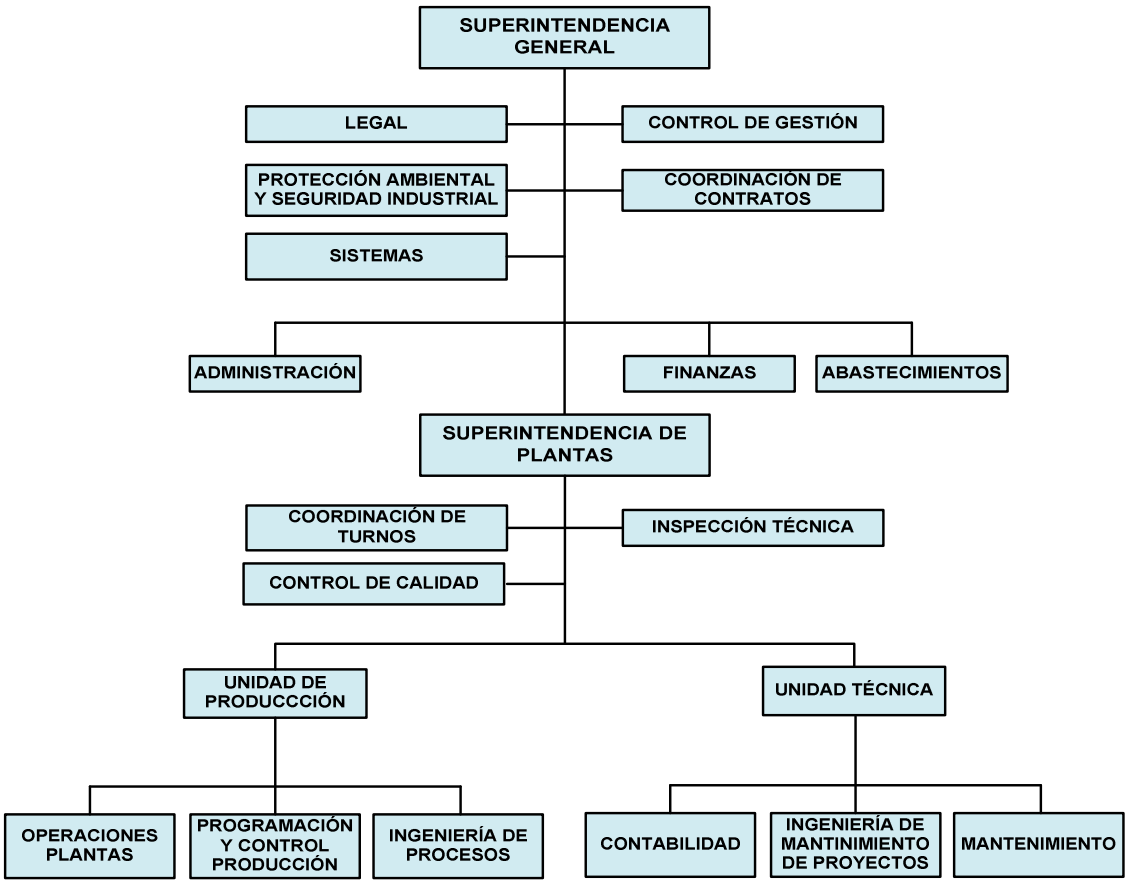


Figura 1.3 Estructura Organizacional de la Refinería Estatal de Esmeraldas [12]

1.1.4.2 Refinería La Libertad (RLL)

Está situada en la Provincia de Santa Elena Cantón La Libertad. En el mes de noviembre de 1989, se revertieron al Estado Ecuatoriano las instalaciones de la Refinería Anglo Ecuadorian Oil Fields Ltda. y en el año 1990 la refinería Repetrol (ex Gulf), al concluir los contratos de operación con éstas compañías. Estas instalaciones están ubicadas en la Península de Santa Elena.

La RLL está diseñada para procesar 45.000BPD de petróleo crudo extraído del Oriente Ecuatoriano y produce los siguientes derivados: GLP[1], Gasolina, Diesel Número 1, Diesel Número 2, Jet Fuel, Fuel Oil Número 6, Solvente Número 1, Solvente Número 2 (Rubber Solvent), Spray Oil y Mineral Turpentine.

[1] **GLP:** Gas Licuado del Petróleo, es la mezcla de gases condensables presentes en el gas natural o disueltos en el petróleo. Los componentes del GLP, aunque a temperatura y presión ambientales son gases, son fáciles de condensar, de ahí su nombre. En la práctica se puede decir que los GLP son una mezcla de propano y butano.

La RLL con 60 años de operación en la península de Santa Elena es el centro refinador más antiguo del Ecuador, y ahora el segundo por su capacidad de producción.

En la Figura 1.4 se muestran fotos de la Refinería La Libertad.

Figura 1.4 Refinería La Libertad [12]

En la Figura 1.5 se muestra el diagrama de la estructura organizacional de la Refinería La Libertad.

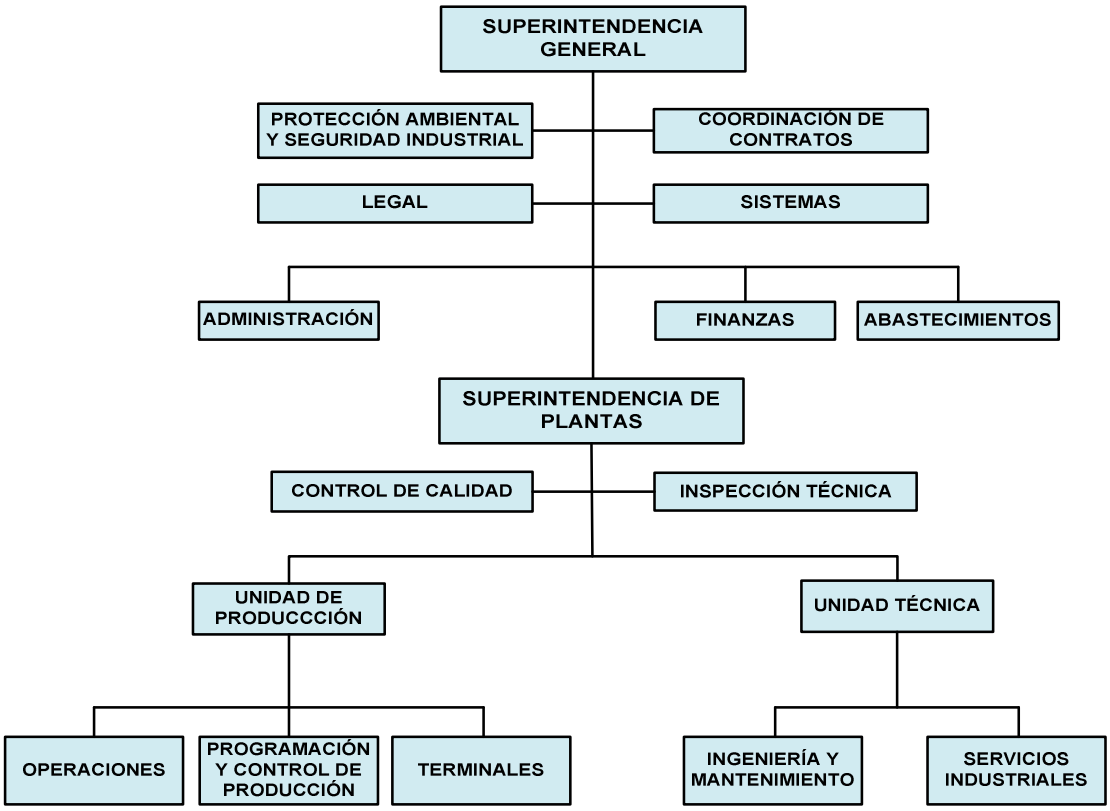


Figura 1.5 Estructura Organizacional de la Refinería La Libertad [12]

1.1.4.3 Complejo Industrial Shushufindi (CIS)

Está ubicado en la Provincia de Sucumbíos en la región Oriental del País. Está formado por:

- Refinería Amazonas.
- Planta de gas de Shushufindi.

La Refinería Amazonas arrancó en 1987 con una capacidad de 10.000BPD, en 1995 se duplicó su capacidad a 20.000BPD. Está formada por dos Unidades gemelas de destilación atmosférica.

La Planta de gas de Shushufindi inicio sus operaciones en 1981, se diseñó para aprovechar el gas natural asociado al Crudo extraído en los campos y producir GLP y gasolina natural. Su máxima carga es de 25 millones de pies cúbicos estándar de gas asociado. Tiene capacidad para producir hasta 500 Tm/día de GLP y 2.800BPD de gasolina.

En la Figura 1.6 se muestran fotos del Complejo Industrial Shushufindi.

Figura 1.6 Complejo Industrial Shushufindi [12]

En la Figura 1.7 se muestra el diagrama de la estructura organizacional del Complejo Industrial Shushufindi.

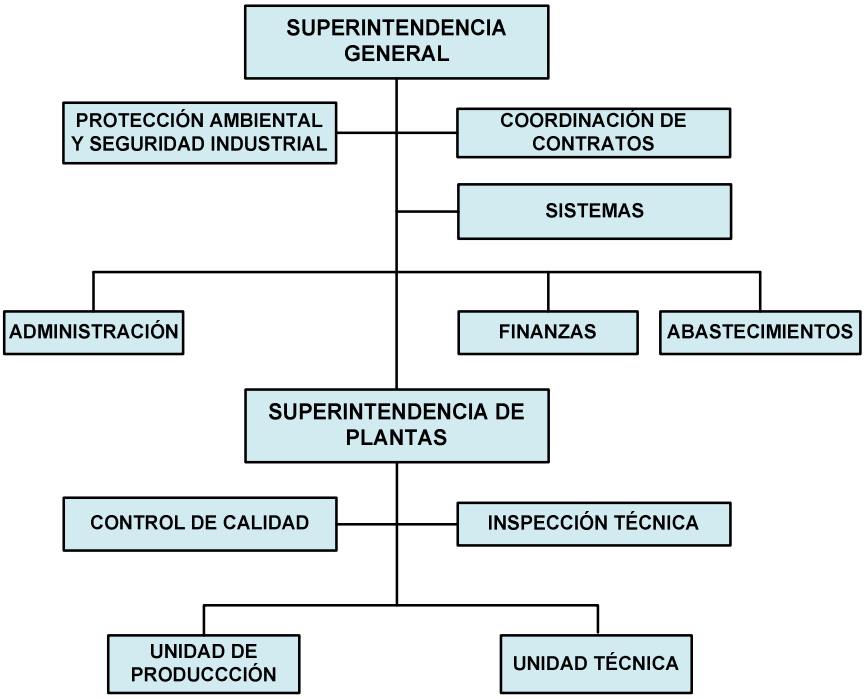


Figura 1.7 Estructura Organizacional del Complejo Industrial Shushufindi [12]

1.2 INFRAESTRUCTURA DE LA RED DE COMUNICACIÓN DE PETROINDUSTRIAL

1.2.1 TOPOLOGÍA DE LA RED LAN Y WAN DE PETROINDUSTRIAL

La red LAN y WAN de Petroindustrial tiene una composición estructural con un elevado grado de complejidad, ya que ésta, como toda red actual, no está exenta de crecimiento y constantes nuevos requerimientos para satisfacer las necesidades de los usuarios y las nuevas exigencias tecnológicas que sobre la red va imponiendo cada proyecto de innovación que se desarrolla dentro de esta filial de Petroecuador.

La red de Petroindustrial consta de cuatro redes LAN para la matriz y para los tres distritos. Estas se encuentran diseñadas para garantizar un buen servicio a todos y cada uno de los trabajadores de la empresa. En la Figura 1.8 se puede observar el diagrama de la red LAN y WAN de Petroindustrial. Estas redes se comunican entre ellas a través de una nube Frame Relay de Petrocomercial.

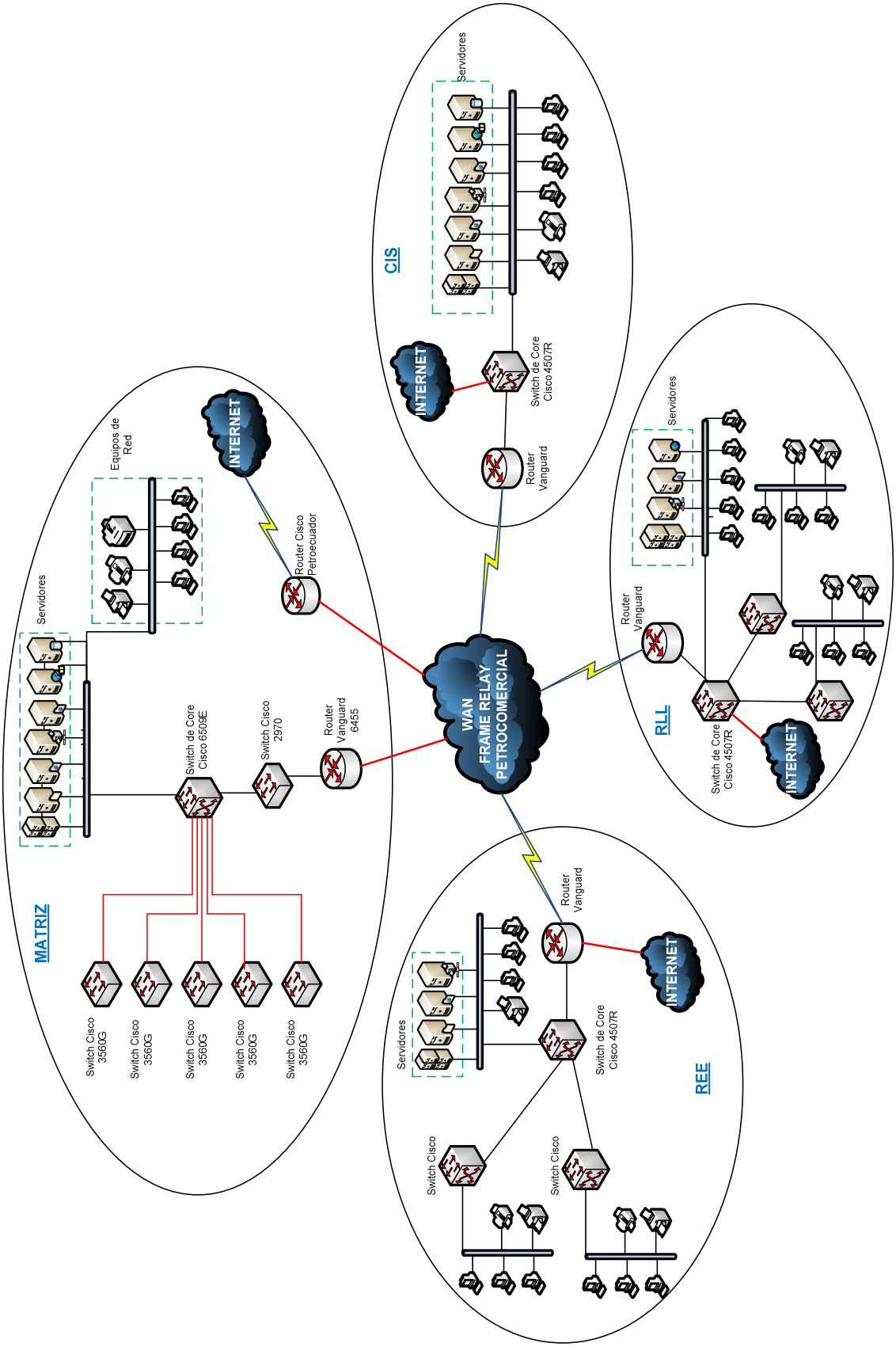


Figura 1.8 Diagrama de la red LAN y WAN de Petroindustrial

1.2.1.1 Topología de la Red LAN de Petroindustrial-Matriz

La Matriz de Petroindustrial se encuentra en la ciudad de Quito en las calles Alpallana E8-30 y Diego de Almagro.

Actualmente la estructura de la red LAN de Petroindustrial en su nivel físico tiene la siguiente composición:

Como equipo activo de red principal o switch de core (núcleo) posee un Switch-Route de capa 3, marca Cisco System, modelo Catalyst de la serie 6509E; el mismo que tiene instalado 2 tarjetas supervisor que funcionan con un sistema de alta disponibilidad con redundancia, 5 módulos de 48 puertos gigabit ethernet y un módulo adicional de 32 puertos GBIC para conexiones up-link de fibra óptica.

Figura 1.9 Switch Cisco Catalyst 6509E [13]

Dentro del backbone vertical de fibra óptica tiene 5 switches de marca Cisco, modelo Catalyst de la serie 3500 con 48 puertos Giga bit Ethernet más 4 puertos up-link de fibra óptica que complementan su estructura.

Como equipo principal de enrutamiento tanto para la red LAN como WAN tiene un Router Vanguard 6455 de marca Motorola, el mismo que cumple con la función de enlace entre las redes de las refinerías, a través del sistema de telecomunicaciones y la red de la Matriz de Petroindustrial. De la misma manera permite la conexión con la red de sistemas de Petroecuador, que es el área

encargada de brindar el acceso a la red de Internet para toda la red LAN de Petroindustrial-Matriz.

La Matriz de Petroindustrial opera en un edificio de 12 pisos, por lo que el backbone de la red LAN se constituye de un Switch Cisco Catalyst 3560G cada dos pisos, de esta manera logra abastecer a los usuarios que trabajan en este lugar.

El cuarto de Servidores se encuentra en el octavo piso en el área de Sistemas, el mismo que esta adecuadamente equipado, para garantizar la seguridad física y operativa de los equipos que posee esta empresa.

En la Tabla 1.1 se detalla los servidores que se encuentran operando en ésta área:

N°	MARCA	MODELO	PROCESADOR	CAPACIDAD DE ALMACENAMIENTO	MEMORIA RAM	SISTEMA OPERATIVO	SERVICIO QUE SE EJECUTA
1	IBM	X series 220	PENTIUM III	50 GB	1 GB	WINDOWS 2000 Server	SQL Server 2000
2	DELL	POWEREDGE	PENTIUM Xeon	144 GB	1 GB	WINDOWS 2000 Server	Servidor de impresora, aplicaciones de terceros: Legal, Autocad, Bibliotecas de usuarios
3	COMPAQ	ML570	PENTIUM Xeon	210 GB	1 GB	WINDOWS 2000 Server	Administración Electrónica de Documentos, sistema Stellent
4	IBM	X series 235	PENTIUM Xeon	144 GB	5 GB	WINDOWS 2000 Server	Controlador de Dominio, Secundario, Administración de Antivirus, Web Security, MySQL
5	HP	Blade Quad_core	PENTIUM Xeon X5355	68 GB	4 GB	WINDOWS 2003 Server	Controlador de Dominio Principal de la red local de Matriz
6	HP	Blade Quad_core	PENTIUM Xeon X5355	68 GB	4 GB	WINDOWS 2003 Server	Exchange Server
7	HP	Blade Quad_core	PENTIUM Xeon X5355	68 GB	4 GB	WINDOWS 2003 Server	Servidor Aplicaciones Web, Intranet PIN
8	HP	Blade Quad_core	PENTIUM Xeon X5355	68 GB	4 GB	WINDOWS 2003 Server	Servidor Cisco Work
9	HP	Blade Quad_core	PENTIUM Xeon X5355	68 GB	4 GB	WINDOWS 2003 Server	No Utilizado
10	HP	DC 5100 MT	PENTIUM	80 GB	1 GB	LINUX	Servidor SMTP Filtering
11	IBM	AS/400 9406-810	POWER5 2465	105,4 GB	1,2 GB	OS400	CG/IFS, Uniclass, Maint Tracker, Recursos Humanos, Contratos
12	IBM	AS/400 9406 M	POWER5 2465	105,4 GB	720 MB	OS400	Programas Producto IBM, Participación de Desarrollo para la Matriz PIN

Tabla 1.1 Detalle de los Servidores que operan en Petroindustrial-Matriz

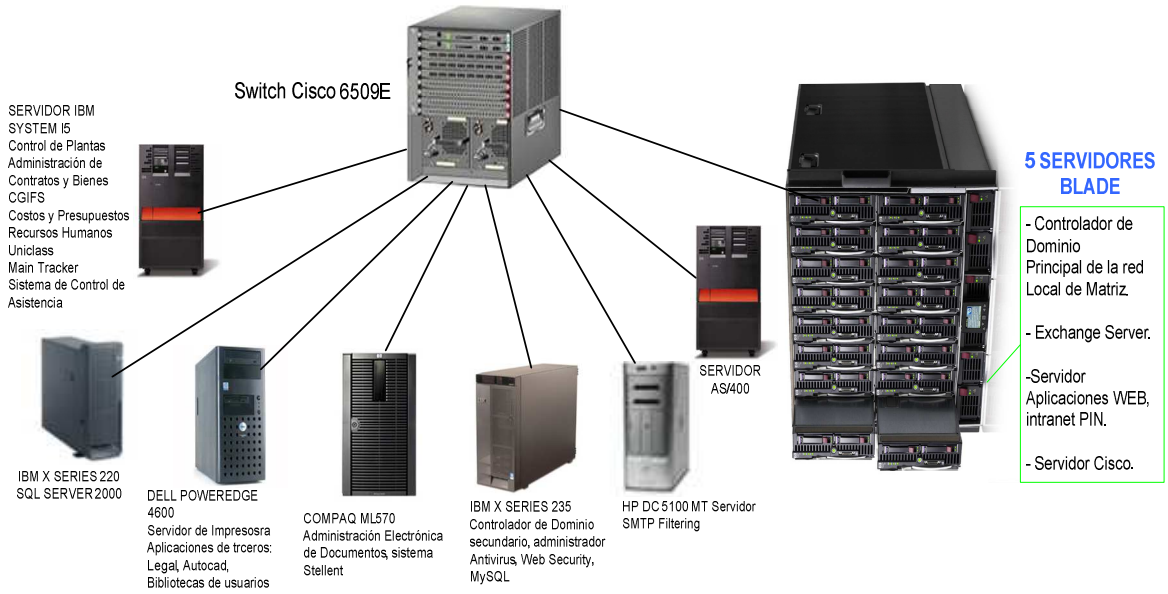


Figura 1.10 Servidores que operan en Petroindustrial-Matriz

La estructura de la red LAN de Petroindustrial en su nivel lógico y de configuración tiene la siguiente composición:

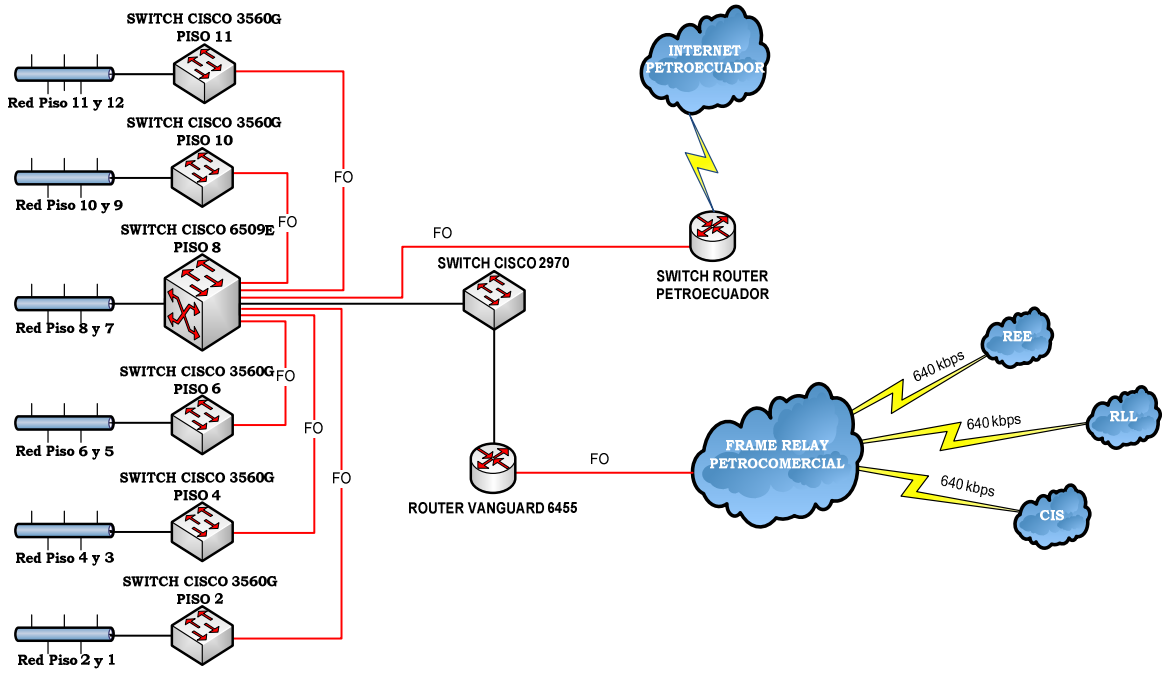


Figura 1.11 Topología de la Red LAN de Petroindustrial-Matriz

1.2.1.2 Topología de la Red LAN de Petroindustrial-REE

Es la refinería más grande que posee Petroindustrial, se encuentra constituida por varias unidades operativas, en cada una de ellas se encuentra un switch para proporcionar las debidas facilidades de conectividad, para abastecer a todos los usuarios en esta red. Como equipo principal de enrutamiento tanto para la red LAN como WAN tiene un Router Vanguard 6455 de marca Motorola.

En la infraestructura de la red posee un Switch Catalyst 4507R como equipo de Core, el mismo que cuenta con 2 fuentes de poder redundantes, 1 módulo supervisor, 1 módulo de 6 puertos SFP[1]-Giga bit Ethernet, 1 módulo de 24 puertos Giga bit Ethernet y 3 módulos de 48 puertos Giga bit Ethernet.

Los otros Switches instalados son modelo Catalyst 2960 de 24 Giga bit Ethernet y 4 puertos dual SFP-Ethernet.

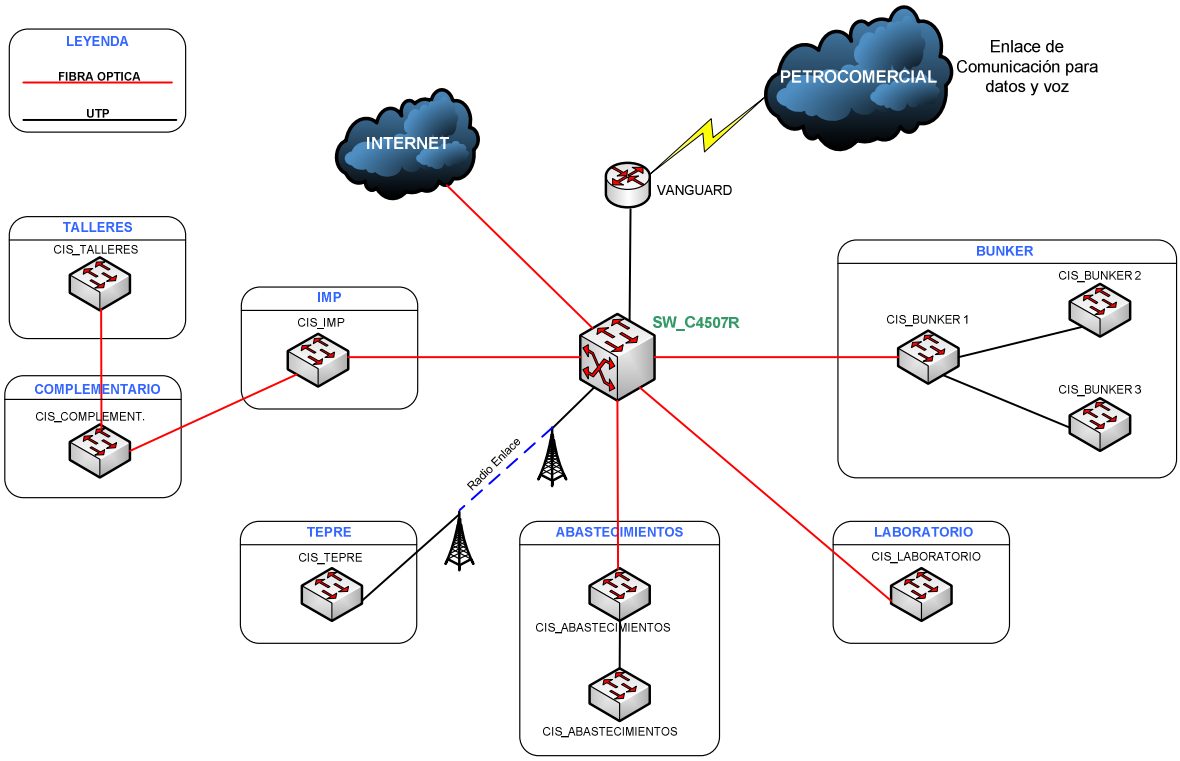


Figura 1.12 Topología de la Red LAN de Petroindustrial-REE

[1] **SFP:** Small Factor Pluggable, conector utilizado en aplicaciones de telecomunicaciones y comunicación de datos, comúnmente se utiliza con fibra óptica y cable UTP.

1.2.1.3 Topología de la Red LAN de Petroindustrial-CIS

De igual forma está constituido por un equipo de enrutamiento Router Vanguard 6455 de marca Motorola.

En la infraestructura de la red posee un Switch Catalyst 4507R como equipo de Core, el mismo que cuenta con 2 fuentes de poder redundantes, 1 módulo supervisor, 1 módulo de 6 puertos SFP-Giga bit Ethernet, 1 módulo de 24 puertos Giga bit Ethernet y 3 módulos de 48 puertos Giga bit Ethernet.

Los otros dispositivos de red que posee esta Refinería son Switches Catalyst 2960 de 24 puertos Giga bit Ethernet y 4 puertos dual SFP-Ethernet.

Todos estos equipos están conectados mediante una fibra óptica multimodo para una mejor transmisión de datos, y de esta forma brindar la mejor eficiencia en el tráfico de información.

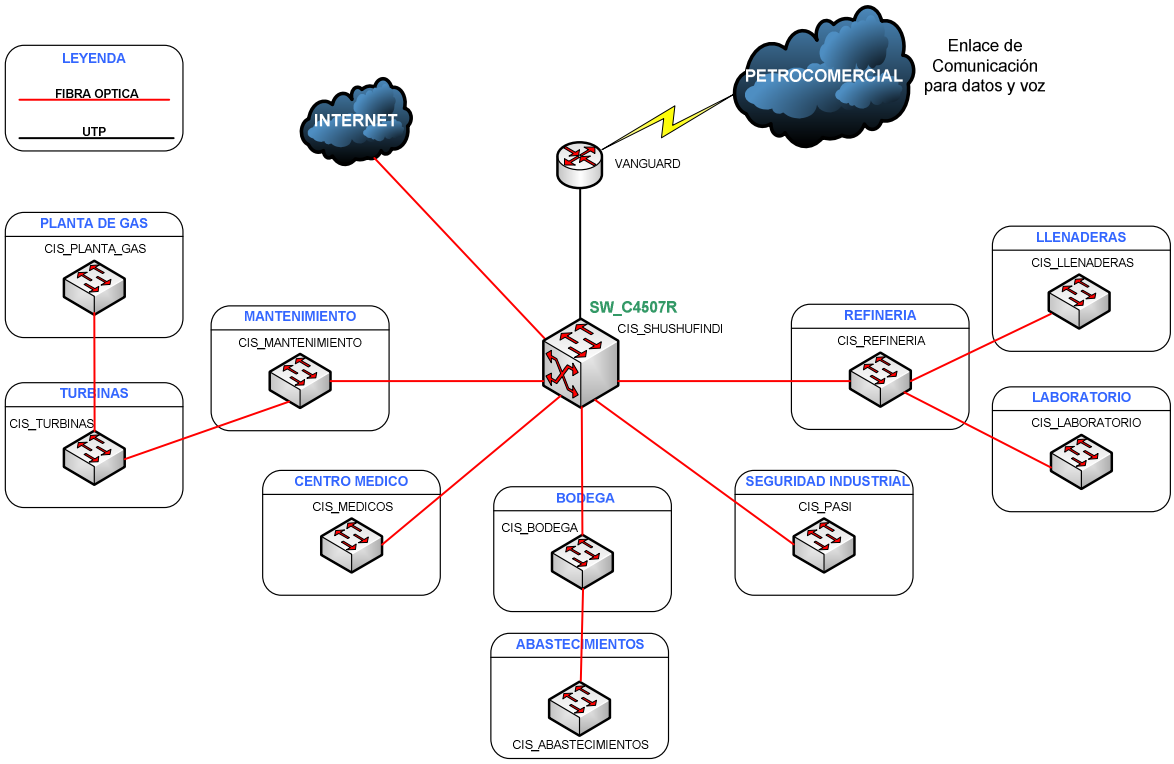


Figura 1.13 Topología de la Red LAN de Petroindustrial-CIS

1.2.1.4 Topología de la Red LAN de Petroindustrial-RLL

Este distrito cuenta con un equipo de enrutamiento Router Vanguard 6455 de marca Motorola.

También se encuentra equipado de un cuarto de servidores, en donde se ubica como equipo de core, un Switch Catalyst 4507R con 2 fuentes de poder redundantes, 1 módulo supervisor, 1 módulo de puertos SFP-Gigabit Ethernet, 1 módulo de 24 puertos Giga bit Ethernet y 1 módulo de 48 puertos Giga bit Ethernet.

Este distrito cuenta también con un Switch Catalyst 4503R con 2 fuentes de poder redundantes. 1 modulo supervisor. 1 modulo de 6 puertos SFP-Giga bit Ethernet, 1 modulo de 24 puertos Giga bit Ethernet y 1 módulo de 48 puertos Giga bit Ethernet, además 6 Switches Catalyst 3560 de 28 puertos Giga bit Ethernet, 4 puertos dual SFP-Ethernet y con 7 Switches Catalyst 2960 de 24 puertos Giga bit Ethernet, 4 puertos dual SFP-Ethernet.

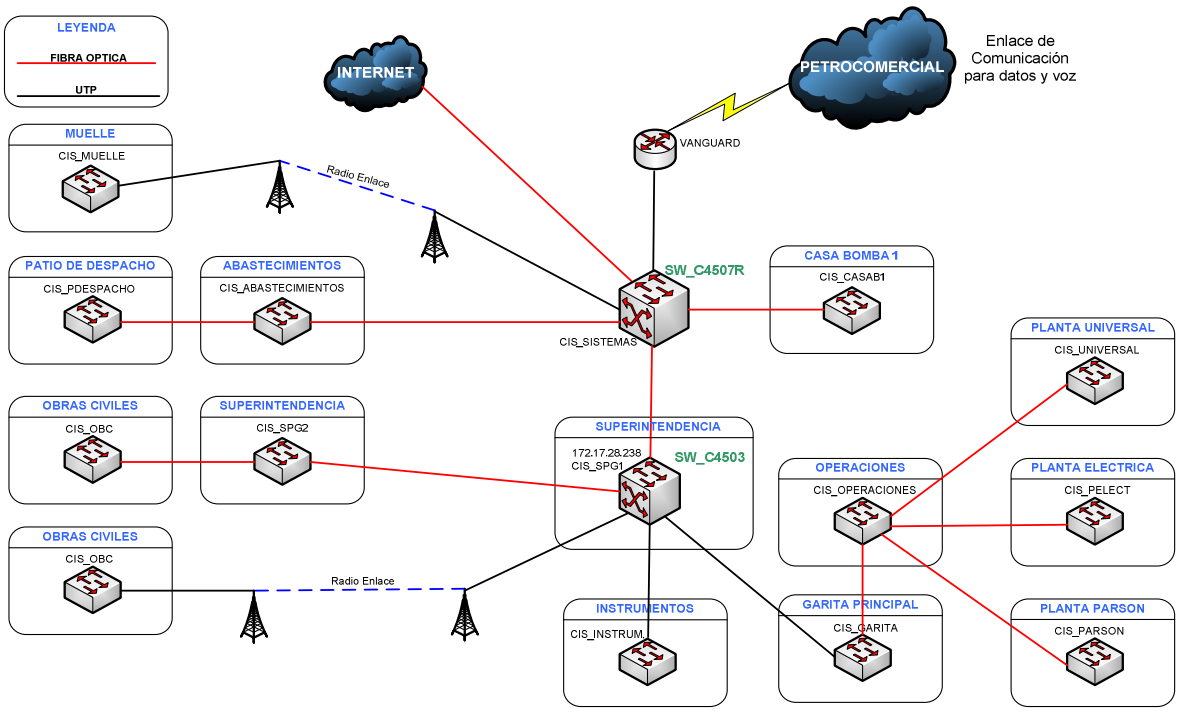


Figura 1.14 Topología de la Red LAN de Petroindustrial-RLL

1.2.2 DIRECCIONAMIENTO DE PETROINDUSTRIAL

La estructura de la red LAN de Petroindustrial en su nivel lógico, está diseñada de la siguiente manera:

Se ha asignado una red privada tipo B (172.30.0.0) para el direccionamiento de Petroindustrial, la misma que está dividida en subredes para abastecer a la Matriz y a los diferentes distritos. Cada distrito tiene un rango específico de redes, asignadas para su adecuada administración, según las necesidades de cada área productiva. A continuación se indica el direccionamiento por cada distrito como también de la Matriz de Petroindustrial.

1.2.2.1 Direccionamiento de Petroindustrial-Matriz

Como se comentó anteriormente, se tiene la dirección tipo B 172.30.0.0 para Petroindustrial, la misma que se encuentra dividida en subredes de las cuales se utilizan las siguientes: 172.30.16.0, 172.30.17.0, 172.30.18.0 y 172.30.116.0. Estas redes a su vez se encuentran subneteadas, para una mejor administración de la red local.

En el equipo Switch Cisco Catalyst 6509E se tiene configurado un número de 11 VLANs, con el objetivo de reunir a los usuarios y hosts en grupos de red administrables y más manejables; reduciendo así el broadcast. La distribución de las VLANs se ha realizado ubicando la agrupación de acuerdo a la unidad de trabajo y oficinas que funcionan en cada uno de los pisos del edificio de la empresa.

De las 11 VLANs configuradas, la VLAN número 2, 9, 10 y 18 tienen una máscara de 24 bits lo que proporciona un número de 254 direcciones IP asignables. La VLAN 2 esta asignada exclusivamente para la red de servidores e impresoras con puertos Ethernet. La VLAN 9 se ha designado para la red de telefonía IP. Por último la VLAN 10 se ha asignado como la VLAN de Seguridad que es donde se

ingresan los PC's que por algún motivo están generado tráfico dentro de la red para su revisión y corrección del problema, por último la VLAN 18 es utilizada para la conexión con Petroecuador para el Internet.

El resto de Subredes ó VLAN de este esquema actual de direccionamiento tiene un rango de 64 direcciones IP, siendo asignables un total de 62 direcciones para los host. A parte de toda la configuración de VLANs dentro del equipo Switch Cisco, también se ha incorporado una tabla de rutas para que el tráfico sea correctamente direccionado hacia el próximo salto a donde pertenece. Aquí están incluidas las rutas que dirigen el tráfico tanto para cada una de las redes de las refinerías, así como también el tráfico que va hacia la red de sistemas de Petroecuador para la salida a Internet.

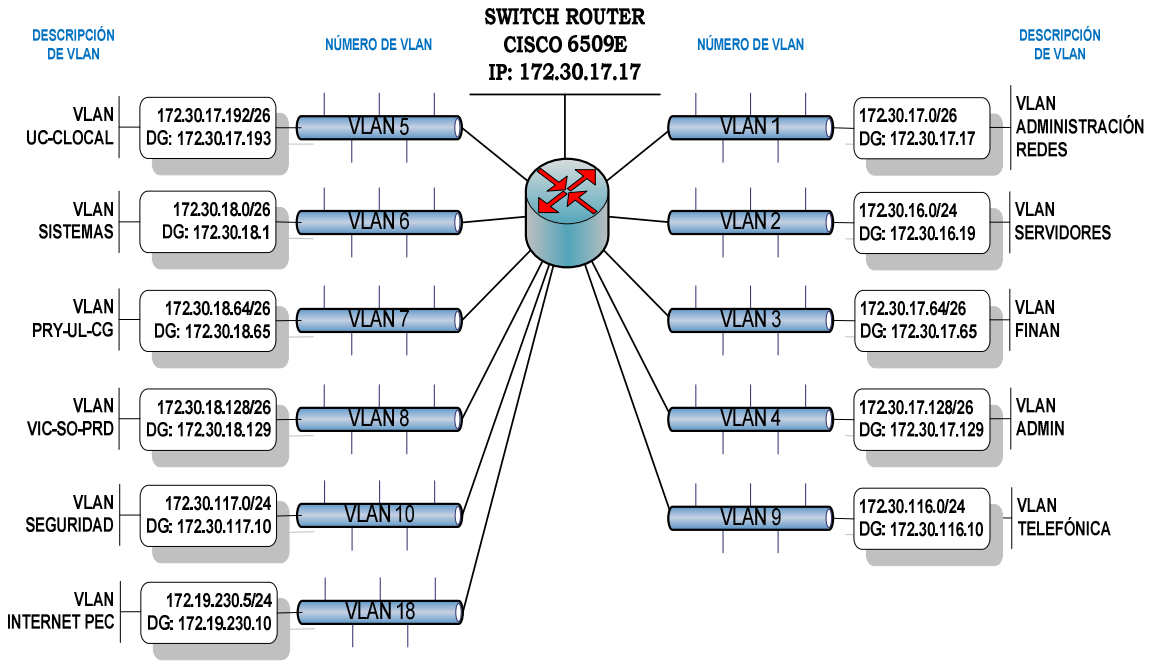


Figura 1.15 Distribución de VLANs de Petroindustrial-Matriz

1.2.2.2 Direccionamiento de Petroindustrial-REE

Para la Refinería Estatal de Esmeraldas se han asignado el rango de las siguientes redes: 172.30.20.0, 172.30.21.0, 172.30.22.0 y 172.30.23.0. De igual

manera estas direcciones de red se encuentran subneteadas para una mejor administración local.

En el switch de core de esta refinería, que es un Cisco Catalyst 4507R se encuentran configuradas 12 VLANs, de las cuales la 1 y 12 tienen una máscara de 24 bits lo que proporciona un número de 254 direcciones IP asignables. Las VLANs 2 y 3 tienen una máscara de 25 bits lo que da 126 direcciones IP asignables. Las VLANs restantes poseen una máscara de 27 bits; es decir, 30 direcciones IP asignables.

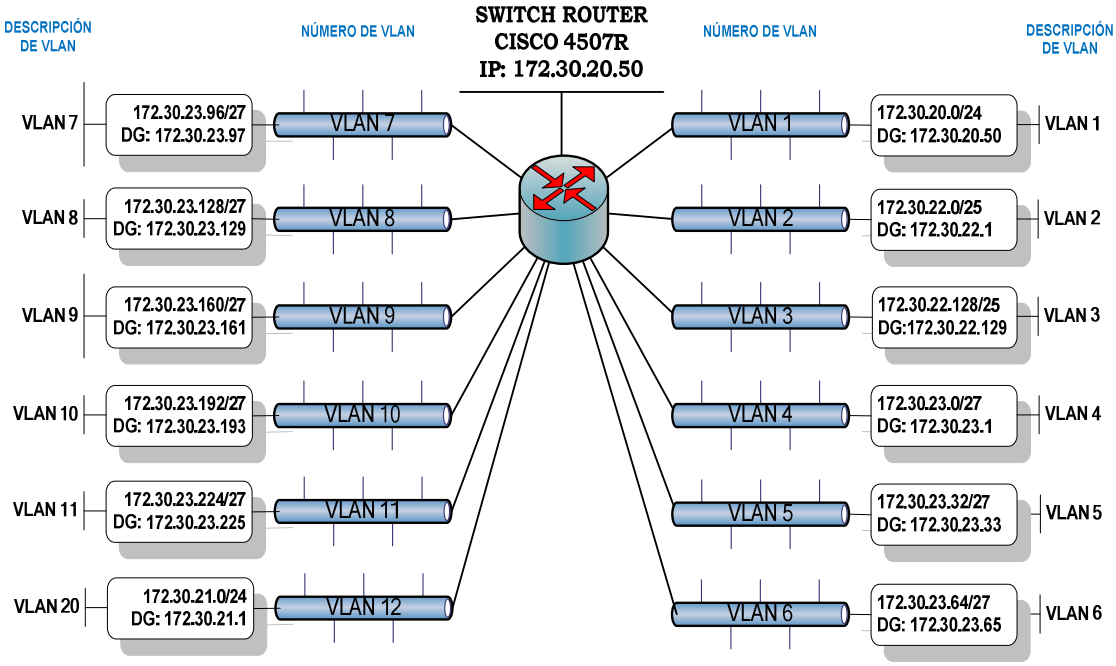


Figura 1.16 Distribución de VLANs de Petroindustrial-REE

1.2.2.3 Direccionamiento de Petroindustrial-CIS

Para el Complejo Industrial Shushufindi se han asignado el rango de las siguientes redes: 172.30.24.0, 172.30.25.0, 172.30.26.0 y 172.30.27.0. De la misma forma estas direcciones de red se encuentran subneteadas para una mejor administración local.

En el switch de core de esta refinería que es un Cisco Catalyst 4507R se encuentran configuradas 13 VLANs, de las cuales la 1 tiene una máscara de 24 bits lo que proporciona un número de 254 direcciones IP asignables. La VLAN 13 tiene una máscara de 26 bits lo que da 62 direcciones IP asignables. Las VLANs 10 y 11 tienen una máscara de 27 bits por lo que se tiene 30 direcciones IP asignables y las VLANs restantes poseen una máscara de 28 bits; es decir, 14 direcciones IP asignables.

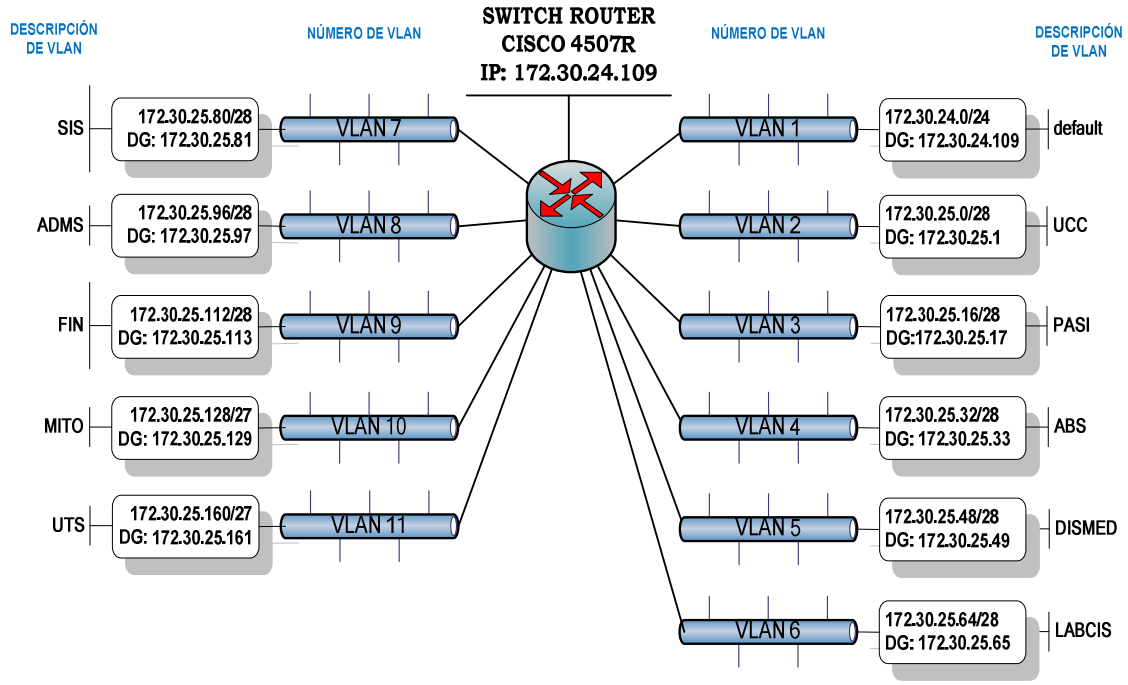


Figura 1.17 Distribución de VLANs de Petroindustrial-CIS

1.2.2.4 Direccionamiento de Petroindustrial-RLL

Para la Refinería La Libertad se han asignado el rango de las siguientes redes: 172.30.28.0, 172.30.29.0, 172.30.30.0 y 172.30.31.0. De la misma forma, estas direcciones de red se encuentran subneteadas para una mejor administración local.

En el switch de core de esta refinería, que es un Cisco Catalyst 4507R, se encuentran configuradas 12 VLANs, de las cuales la Vlan 1 tiene una máscara de

24 bits lo que proporciona un número de 254 direcciones IP asignables. Las VLANs restantes poseen una máscara de 26 bits; es decir, 62 direcciones IP asignables.

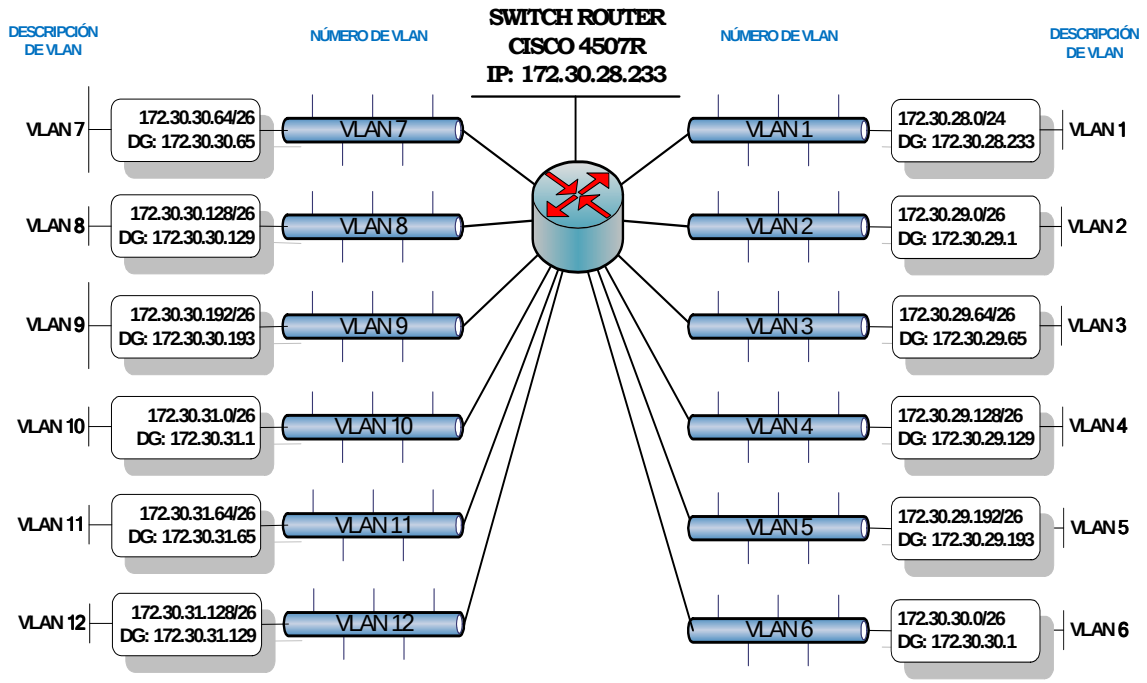


Figura 1.18 Distribución de VLANs de Petroindustrial-RLL

1.3 SISTEMA DE SEGURIDAD ACTUAL DE PETROINDUSTRIAL

1.3.1 SEGURIDAD PERIMETRAL

Actualmente Petroindustrial no cuenta con una seguridad a nivel perimetral. Lo único que controla el tráfico hacia la red LAN desde Internet es un Firewall que posee Petroecuador, ya que es un servicio que brinda a Petroindustrial-Matriz, y los distritos, al tener un proveedor distinto de Internet no cuentan con seguridad para sus respectivas redes LAN.

1.3.2 SEGURIDAD INTERNA

Para la seguridad interna maneja una tecnología llamada Symantec$_{TM}$[1] Web Security la cual realiza el filtrado de contenidos y la protección contra virus de alto rendimiento para el Gateway HTTP/FTP.

Symantec Web Security protege el Gateway HTTP/FTP de una organización contra virus y otras amenazas para brindar un acceso a Internet seguro y productivo. Symantec Web Security, utilizando las tecnologías escalables e integradas de filtrado de contenidos y protección antivirus que Symantec desarrolla y soporta, realiza también análisis simultáneos de virus y contenidos de Web inapropiados. Esta eficaz solución para múltiples protocolos mejora la productividad de los empleados, incrementa el aprendizaje en los entornos educativos y reduce la exposición de los activos analizando y administrando el uso de Internet. Es una solución que ahorra el ancho de banda y mejora la seguridad de la red administrando las descargas de archivos, reduciendo la navegación inadecuada en la Web y fortaleciendo la defensa contra las amenazas combinadas.

1.3.2.1 Bondades que brinda la Tecnología Symantec$_{TM}$ Web Security [14]

- **La eficacia de una sola exploración de tecnologías integradas**

Symantec$_{TM}$ Web Security utiliza un solo proceso de baja latencia que protege eficazmente contra ataques de códigos maliciosos y explora el contenido de Web sin consumir recursos de red. Es la única solución de un solo proveedor que integra técnicas basadas en listas y herramientas heurísticas de análisis sensibles al contenido para proteger al nivel de gateway contra virus y contenidos inadecuados.

[1] TM: Trade Mark, significa que una empresa tiene ese nombre registrado y lo usa como nombre comercial para la comercialización del producto.

Symantec$_{TM}$ Web Security incluye la protección de varias tecnologías propietarias de Symantec:

Motor de exploración modular NAVEX: detecta las nuevas clases de virus y puede actualizarse sin tener que desinstalar software existente, reimplantar nuevo software o reiniciar el sistema.

Digital Immune System: una tecnología de ciclo cerrado que administra automáticamente el proceso de detección-análisis-cura, incluyendo la puesta en cuarentena de archivos infectados para su envío por líneas seguras a Symantec Security Response.

Symantec Striker: aplica perfiles para identificar y erradicar rápidamente clases completas de códigos maliciosos.

Symantec Bloodhound: puede detectar hasta el 80 por ciento de los nuevos virus de archivo ejecutable, incluyendo los códigos maliciosos móviles.

- **Tecnologías de filtrado de contenidos completo**

La tecnología multilingüe y patentada Dynamic Document Review (DDR) de Symantec proporciona un completo filtrado de contenidos. La tecnología DDR va más allá de la simple búsqueda de palabras clave, ya que analiza relaciones de palabras sensibles al contexto. Funciona en tiempo real determinando al vuelo y con precisión la necesidad de bloquear un contenido de Web inapropiado, incluso si dicho contenido todavía no ha sido incluido en una lista de filtros. La tecnología DDR detecta y bloquea eficazmente nuevos sitios o sitios de acceso reciente, sitios anteriormente aceptados que han modificado su contenido, así como sitios bloqueados que contienen nuevos nombres de dominio.

Además de la tecnología DDR, Symantec$_{TM}$ Web Security ofrece listas de filtros URL personalizables desarrolladas y soportadas por Symantec. De esta manera los administradores pueden filtrar los sitios Web mundiales de acuerdo con las

políticas de la organización en todo el sistema, en grupos, o en forma individual, utilizando 31 categorías predefinidas, como por ejemplo, sexo, juegos de apuesta o intolerancia. Symantec actualiza automáticamente las listas de filtros del software diariamente.

- **Administración centralizada basada en políticas**

Para una instalación, configuración y administración fáciles de toda la empresa, Symantec$_{TM}$ Web Security proporciona una interfaz intuitiva de Web basada en HTML y soporte SSL seguro para directorios externos (incluyendo LDAP, Active Directory y Windows NT® user/group). Los administradores pueden crear, programar e implementar perfiles de navegación personalizados para usuarios individuales, PCs o grupos. Para racionalizar aún más la administración, la nueva administración centralizada de políticas multiservidor permite que los administradores modifiquen automáticamente las políticas de exploración y filtrado para cada uno de los servidores Symantec$_{TM}$ Web Security en su red, desde cualquier servidor que forme parte de la red. Cualquier cambio realizado en la configuración de la exploración de virus o del filtrado de contenidos en cualquier servidor Symantec$_{TM}$ Web Security se propaga automáticamente a todos los otros servidores Symantec$_{TM}$ Web Security de la red.

Los administradores también pueden monitorear y registrar la actividad de Web tanto en los sitios filtrados como en los no filtrados, así como utilizar herramientas de auditoría e informe para evaluar el cumplimiento de las políticas de uso aceptables. Symantec$_{TM}$ Web Security alerta automáticamente a los administradores a través del correo electrónico del incumplimiento de las políticas y la función AutoLock (Auto bloqueo) puede negar el acceso a Internet a las cuentas que intentan ver repetidamente contenidos bloqueados. Genera informes integrados de virus y uso de la Web que pueden utilizarse en programas de hoja de cálculo y otras aplicaciones. Por último, Symantec LiveUpdate ofrece una protección continua y actualizada, incluso en ubicaciones a distancia, porque recupera, de forma manual o programada, las definiciones de virus del sitio Web de Symantec.

Symantec$_{TM}$ Web Security suministra la primera línea de defensa contra los virus procedentes de la Web, así como una herramienta para crear informes y administrar el uso de Internet de los empleados. Los administradores de TI pueden definir políticas para usuarios, grupos, equipos o toda la organización, mientras que procesan en paralelo bases de datos estándar y servicios de directorio, tales como LDAP, Active Directory y Windows NT® users/groups.

- **Administración centralizada basada en políticas**

Para una instalación, configuración y administración fáciles de toda la empresa, Symantec$_{TM}$ Web Security proporciona una interfaz intuitiva de Web basada en HTML y soporte SSL seguro para directorios externos (incluyendo LDAP, Active Directory y Windows NT® user/group). Los administradores pueden crear, programar e implementar perfiles de navegación personalizados para usuarios individuales, PCs o grupos. Para racionalizar aún más la administración, la nueva administración centralizada de políticas multiservidor permite que los administradores modifiquen automáticamente las políticas de exploración y filtrado para cada uno de los servidores Symantec Web Security en su red, desde cualquier servidor que forme parte de la red. Cualquier cambio realizado en la configuración de la exploración de virus o del filtrado de contenidos en cualquier servidor Symantec Web Security se propaga automáticamente a todos los otros servidores Symantec Web Security de la red.

Los administradores también pueden monitorear y registrar la actividad de Web tanto en los sitios filtrados como en los no filtrados, así como utilizar herramientas de auditoría e informe para evaluar el cumplimiento de las políticas de uso aceptables. Symantec Web Security alerta automáticamente a los administradores a través del correo electrónico del incumplimiento de las políticas y la función AutoLock (Auto bloqueo) puede negar el acceso a Internet a las cuentas que intentan ver repetidamente contenidos bloqueados. Genera informes integrados de virus y uso de la Web que pueden utilizarse en programas de hoja de cálculo y otras aplicaciones. Por último, Symantec LiveUpdate ofrece una protección

continua y actualizada, incluso en ubicaciones a distancia, porque recupera, de forma manual o programada, las definiciones de virus del sitio Web de Symantec.

- **Rendimiento Mejorado de la Red**

Para mejorar el rendimiento de la red, Symantec$_{TM}$ Web Security analiza sólo el tráfico sospechoso de Web y administra eficazmente las descargas de archivo grandes. Los administradores de TI pueden controlar el acceso a Internet según la hora del día y el día de la semana, proporcionando así una mayor capacidad de ancho de banda a aquellos que más necesiten utilizar Internet en los períodos pico.

- **Respaldo por Symantec Security Response**

Symantec Security Response, la organización líder mundial en investigación y soporte de seguridad en Internet, dedica el equipo de expertos más grande del mercado a la identificación y neutralización de los virus las 24 horas del día en todo el mundo. Symantec Security Response proporciona respuestas globales y rápidas contra ataques generalizados de virus, investigación proactiva para restringir futuras amenazas y una formación permanente.

1.4 SISTEMA DE COMUNICACIÓN DE PETROINDUSTRIAL

Petroindustrial para la comunicación con sus distritos utiliza los enlaces de microonda de Petrocomercial.

1.4.1 INFRAESTRUCTURA DEL SISTEMA DE COMUNICACIONES

A nivel de equipos de enrutamiento o Routers, y con el fin de proporcionar un ancho de banda adecuado para mantener la comunicación estable con sus tres refinerías, Petroindustrial tiene instalado a nivel nacional equipos ruteadores Motorola- Vanguard modelo 6455, en los cuales tiene habilitada la tecnología de

encapsulamiento Frame Relay. Estos equipos además tienen el soporte para encapsulamiento de voz a través de tarjetas FXS y FXO, lo que proporciona conectividad tanto a nivel de datos como de voz con las refinerías.
Un detalle más que es importante recalcar de estos equipos de enrutamiento Vanguard es la disponibilidad de una tarjeta con soporte para enlaces E1 a 2048Kbps, la misma que está prestando servicio y operando en condiciones normales y permitiendo enviar por este medio hasta 30 canales de voz al mismo tiempo.

Petroindustrial dispone de una central telefónica marca NEC modelo IP NEAX 2000, la cual integra 3 tarjetas E1 para comunicaciones, de las cuales solamente 1 de las tarjetas se encuentra habilitada y sincronizada con el equipo principal de enrutamiento Router Vanguard 6455, por medio de la cual se está enviando un total de 14 extensiones telefónicas distribuidas a los tres campos de refinamiento a nivel nacional.

Figura 1.19 Central Telefónica Marca NEC modelo IP NEAX [15]

1.4.2 COMUNICACIONES A TRAVES DE ENLACES DE MICROONDAS

Los puntos principales de enlace que permiten el tránsito de las señales de voz y datos se indican a continuación:

- **Ruta Quito-Esmeraldas**

Pichincha

Guajaló

Atacazo

- **Ruta Quito-La Libertad**

Pilisurco

Capadia

Cerro Azul

Cerro González

- **Ruta Quito-Shushufindi**

Guamaní

Condijua

Tres Cruces

El Reventador

Lumbaquí

Panamiño (en el Coca)

1.4.3 EQUIPAMIENTO

Todo este proceso de comunicación se realiza con equipos modulares transmisores los cuales forman parte de toda la infraestructura de telecomunicaciones de Petroecuador.

Petroindustrial se suma a esta cadena por medio de sus propios equipos con características similares permitiendo compatibilidad con todo el sistema integrado, sus especificaciones se presentan a continuación:

Equipo Matriz

- Radio: Harris Farinon MDS 960 DS, sus características son:

  - Equipo de alta capacidad, E1
  - Capacidad 30 canales.
  - Control de Alarmas.
  - Antena de 2 pies
  - Kit de montaje.
- Multiplexor: Marconi Kilomux.
- Baterías: supply, cargador / rectificador.

Equipos Refinería Estatal de Esmeraldas y Refinería La Libertad.

- Radio Marca Microwave MDS 960 DS, sus características son:
  - Transmisor de 927,6125 MHz
  - Receptor de 951,6125 MHz
  - Amplificador parlante LAC Modelo A19-681
  - Velocidad de 384 Kbps
- Multiplexor RAD Kilomux 2000
- Baterías: un cargador.

Complejo Industrial Shushufindi

- Radio Marca BAYLY, sus características son:
  - Transmisor de 1874,5 MHz
  - Receptor de 1755,5 MHz
  - Velocidad de 2048 Mbps por 2 E1
- Baterías: cargador / rectificador.

CAPÍTULO 2

ANÁLISIS DE LAS TECNOLOGÍAS DE SEGURIDAD PARA REDES

En este capítulo se describe los conceptos más importantes referentes a Seguridad de Redes, así como las principales amenazas, ataques, riesgos y vulnerabilidades que puede sufrir la empresa durante la transmisión de información.

Se revisa la importancia que cumple unas adecuadas Políticas de Seguridad, mediante las cuales se brinda un esquema para garantizar la adecuada transferencia de información.

Además se realiza el estudio de las principales tecnologías de seguridad, como firewall, IPS, IDS, controlador de ancho de banda, entre los principales con los cuales se puede brindar una administración segura de las redes LAN y WAN de las empresas.

2.1 INTRODUCCIÓN

La seguridad de las redes electrónicas y de los sistemas de información suscita cada vez más preocupación, en paralelo al rápido aumento del número de

usuarios y del valor de sus transacciones. La seguridad ha cobrado ahora una importancia crítica, hasta el punto de que constituye un requisito previo para el crecimiento del comercio electrónico y el funcionamiento de la economía en su conjunto. La combinación de varios factores explica que la seguridad de la información y de las comunicaciones se encuentre en la actualidad a la cabeza de las prioridades políticas principalmente en los países europeos.

Las administraciones públicas se han dado cuenta de hasta qué punto la economía y los ciudadanos dependen del funcionamiento eficaz de las redes de comunicación y varias de ellas han comenzado a revisar sus disposiciones en materia de seguridad.

Internet ha creado una conectividad mundial que pone en contacto millones de redes, grandes y pequeñas, y cientos de millones de ordenadores individuales y, cada vez más, otros aparatos como los teléfonos móviles. Ello ha llevado consigo una reducción considerable del costo del acceso ilegal; por lo tanto, un peligro al paso a valiosa información económica.

Es bien conocida la difusión a través de Internet de virus que han causado importantes daños por destrucción de información o denegación de acceso a la red. Tales problemas de seguridad no se limitan a un país concreto, sino que se extienden rápidamente a través de la red.

La seguridad se ha convertido en uno de los principales desafíos a que se enfrentan los responsables políticos y el estudio de una respuesta adecuada a este problema constituye una tarea cada vez más compleja. Hace tan solo unos años, la seguridad de la red era fundamentalmente un problema para los monopolios de Países que ofrecían servicios especializados basados en redes públicas, fundamentalmente la red telefónica. La seguridad de los sistemas informáticos se limitaba a las grandes organizaciones y a los controles de acceso.

La elaboración de una política de seguridad constituía una tarea relativamente fácil. La situación ha cambiado radicalmente debido a una serie de

transformaciones producidas en el mercado mundial, entre las que cabe citar la liberalización, la convergencia y la mundialización.

En la actualidad predomina la propiedad y gestión privadas de las redes. Los servicios de comunicación están abiertos a la competencia y la seguridad forma parte de la oferta de mercado. No obstante, muchos clientes ignoran la amplitud de los riesgos en materia de seguridad a la hora de conectarse a la red y toman su decisión sin estar perfectamente informados.

Las redes y los sistemas de información están en un proceso de convergencia. Cada vez están más interconectados, ofrecen el mismo tipo de servicio sin discontinuidad y personalizado y comparten en cierta medida la misma infraestructura. Los equipos terminales (PC, teléfonos móviles, etc.) se han convertido en un elemento activo de la arquitectura de la red y pueden conectarse a distintas redes.

Las redes son internacionales. Una parte significativa de la comunicación actual se transfronteriza y transita por terceros países (a veces sin que el usuario final sea consciente de ello), por lo que cualquier solución a los problemas de seguridad habrá de tener en cuenta este factor. La mayoría de las redes están formadas por productos comerciales procedentes de proveedores internacionales. Los productos de seguridad deberán ser compatibles con las normas internacionales.

2.2 SEGURIDAD INFORMÁTICA [1] [5] [10]

2.2.1 CONCEPTO

Es una característica de un sistema que le proporciona un grado de confiabilidad[1]; es decir, permite a sus elementos (en este caso software, hardware y datos)

[1] **Confiabilidad:** Significa que a los objetos de un sistema van a tener acceso únicamente los elementos autorizados, sin proporcionar disponibilidad de estos datos a otras entidades.

mantener las características importantes que son: confiabilidad, integridad[1], disponibilidad[2], consistencia[3], control[4] y auditoria[5].

Se puede decir también que la seguridad de las redes y de la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confiabilidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Es preciso tener en cuenta todos los factores que pueden amenazar la seguridad, y no únicamente los de carácter malintencionado. Desde el punto de vista de los usuarios, los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques malintencionados. En conclusión, se puede decir que la seguridad informática es un conjunto de soluciones técnicas dadas a problemas ocasionados en computadores por distintos tipos de amenazas.

2.3 AMENAZAS DE REDES [4][8][11]

2.3.1 RIESGOS DE INTRUSIONES EN LA RED Y TIPOS DE AMENAZA

Sin importar si están conectadas por cable o de manera inalámbrica, las redes de computadoras cada vez se tornan más esenciales para las actividades diarias. Tanto las personas como las organizaciones dependen de sus computadores y de

---

[1] **Integridad:** Indica que los objetos pueden ser modificados de una manera controlada solamente por elementos autorizados.
[2] **Disponibilidad:** Dice que los objetos del sistema siempre deben estar accesibles para los elementos autorizados.
[3] **Consistencia:** Asegura que el sistema se comporte como lo esperan los usuarios.
[4] **Control:** Reglamenta el acceso al sistema, solo a entidades autorizadas.
[5] **Auditoria:** Registra los sucesos que pasan en el sistema identificando las acciones realizadas y los realizadores de éstas, sean éstos autorizados o no.

las redes para funciones como correo electrónico, contabilidad, organización y administración de archivos. Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red y pérdidas de trabajo. Los ataques a una red pueden ser devastadores y pueden causar pérdida de tiempo y de dinero debido a los daños o robos de información o de activos importantes.

Los intrusos pueden obtener acceso a la red a través de vulnerabilidades del software, ataques al hardware o incluso a través de métodos menos tecnológicos, como el de adivinar el nombre de usuario y la contraseña de una persona. Por lo general, a los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se los denomina piratas informáticos.

Una vez que el pirata informático obtiene acceso a la red, pueden surgir cuatro tipos de amenazas:

- Robo de información
- Robo de identidad
- Pérdida/manipulación de datos
- Interrupción del servicio

2.3.1.1 Robo de Información

Es el ingreso no autorizado en una computadora para obtener información confidencial. La información puede utilizarse o venderse con diferentes fines. Ejemplo: robo de la información propietaria de una organización, como la información de investigación y desarrollo.

2.3.1.2 Pérdida y Manipulación de Datos

Es el ingreso en una computadora para destruir o alterar registros de datos. Ejemplo de pérdida de datos: envío de un virus que formatea el disco duro de la computadora. Ejemplo de manipulación de datos: ingreso no autorizado en un sistema de registros para modificar información, como el precio de un artículo.

2.3.1.3 Robo de Identidad

Es una forma en la que se roba información personal con el fin de usurpar la identidad de otra persona. Al utilizar esta información un individuo puede obtener documentos legales, solicitar créditos y hacer compras en línea no autorizadas. El robo de identidad es un problema creciente que cuesta miles de millones de dólares al año.

2.3.1.4 Interrupción del Servicio

Es el método en el cual se impide que los usuarios legítimos puedan acceder a servicios que deberían poder utilizar.

Figura 2.1 Tipos de Amenazas [11]

2.3.2 ORIGENES DE LAS INTRUSIONES EN LA RED

Las amenazas de seguridad causadas por intrusos en la red pueden originarse tanto en forma interna como externa.

2.3.2.1 Amenazas Externas

Las amenazas externas provienen de personas que trabajan fuera de una organización. Estas personas no tienen autorización para acceder al sistema o a la red de la computadora. Los atacantes externos logran ingresar a la red principalmente desde Internet, enlaces inalámbricos o servidores de acceso dial-up.

2.3.2.2 Amenazas Internas

Las amenazas internas se originan cuando una persona cuenta con acceso autorizado a la red a través de una cuenta de usuario o tiene acceso físico al equipo de la red. Un atacante interno conoce la política interna y las personas. Por lo general, conocen información valiosa y vulnerable y saben cómo acceder a ésta.

Sin embargo, no todos los ataques internos son intencionales. En algunos casos la amenaza interna puede provenir de un empleado confiable que capta un virus o una amenaza de seguridad mientras se encuentra fuera de la compañía y, sin saberlo, lo lleva a la red interna.

La mayor parte de las compañías invierte recursos considerables para defenderse contra los ataques externos; sin embargo, la mayor parte de las amenazas son de origen interno. De acuerdo con el FBI[1] el acceso interno y la mala utilización de los sistemas de computación representan aproximadamente el 70% de los incidentes de violación de seguridad notificados.

[1] **FBI:** Federal Bureau of Investigation (Oficina Federal de Investigación)

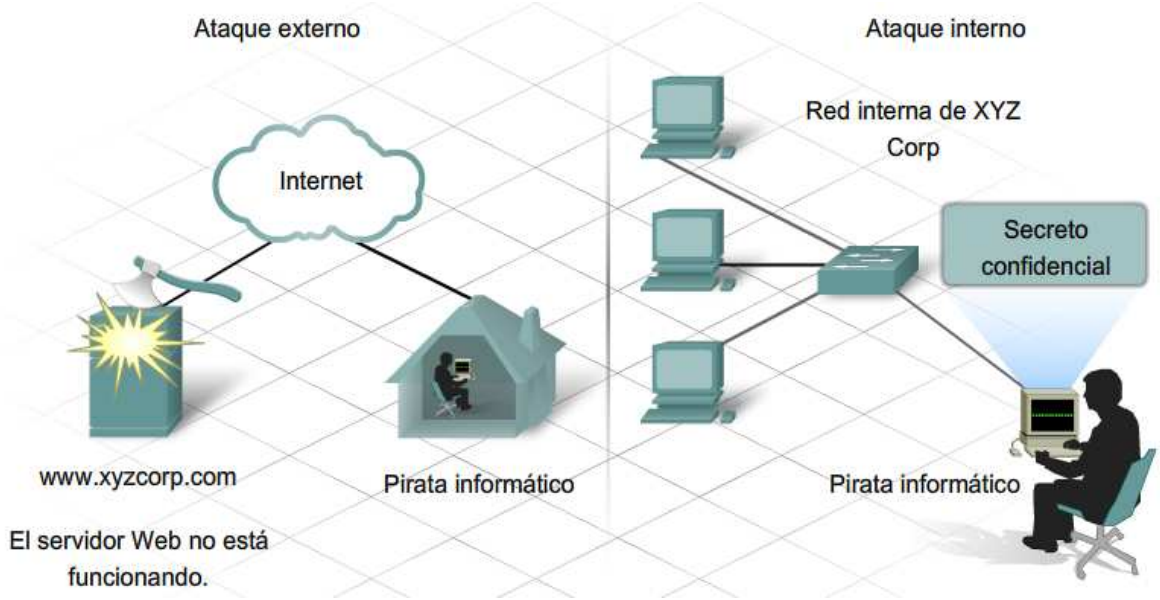


Figura 2.2 Tipos de Ataque [11]

2.3.3 INGENIERÍA SOCIAL Y SUPLANTACIÓN DE IDENTIDAD [1][3]

Para un intruso, una de las formas más fáciles de obtener acceso, ya sea interno o externo, es el aprovechamiento de las conductas humanas. Uno de los métodos más comunes de explotación de las debilidades humanas se denomina ingeniería social.

2.3.3.1 Ingeniería Social

Ingeniería social es un término que hace referencia a la capacidad de algo o alguien para influenciar la conducta de un grupo de personas. En el contexto de la seguridad de computadores y redes, la ingeniería social hace referencia a una serie de técnicas utilizadas para engañar a los usuarios internos a fin de que realicen acciones específicas o revelen información confidencial.

A través de estas técnicas, el atacante se aprovecha de usuarios legítimos desprevenidos para obtener acceso a los recursos internos y a información privada, como números de cuentas bancarias o contraseñas.

Los ataques de ingeniería social aprovechan el hecho de que a los usuarios generalmente se los considera uno de los enlaces más débiles en lo que se refiere a la seguridad. Los ingenieros sociales pueden ser internos o externos a la organización; sin embargo, por lo general no conocen a sus víctimas cara a cara.

El pretexto es una forma de ingeniería social en la que se utiliza una situación inventada para que una víctima divulgue información o lleve a cabo una acción. Generalmente, el contacto con el objetivo se establece telefónicamente. Para que el pretexto sea efectivo el atacante deberá establecer la legitimidad con la víctima o el objetivo deseado. Esto requiere, por lo general, que el atacante cuente con conocimientos o investigaciones previas. Por ejemplo: si el atacante conoce el número de seguro social del objetivo, puede utilizar esta información para ganar la confianza de su objetivo. De esta manera es más probable que el objetivo divulgue información. En la Figura 2.3 se puede observar un ejemplo de Ingeniería social.

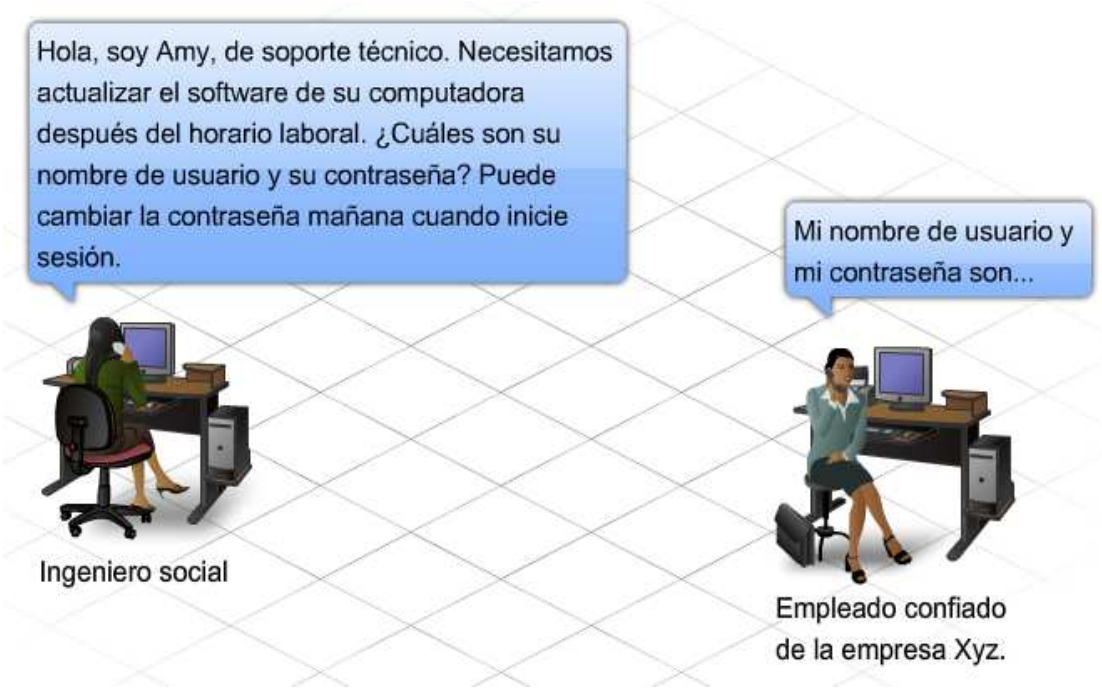


Figura 2.3 Ejemplo de Ingeniería Social [11]

2.3.3.2 Suplantación de Identidad

La suplantación de identidad es una forma de ingeniería social en la que el estafador pretende representar a una organización externa legítima. Generalmente se pone en contacto con el objetivo (el estafado) mediante correo electrónico.

El vishing o suplantación de identidad telefónica es una nueva forma de ingeniería social que utiliza el sistema de voz sobre IP (VOIP). Con el vishing, un usuario desprevenido recibe un correo de voz donde se le solicita que llame a un número telefónico que parece ser un servicio de banca telefónica legítimo. A continuación, la llamada es interceptada por un ladrón. De esta forma se roban los números de cuentas bancarias o las contraseñas introducidas telefónicamente para verificación. En la Figura 2.4 se puede observar un ejemplo de Suplantación de Identidad.

Figura 2.4 Ejemplo de Suplantación de Identidad [11]

2.4 ATAQUES DE REDES [1] [11]

2.4.1 VIRUS, GUSANOS Y CABALLOS DE TROYA

La ingeniería social es una amenaza de seguridad común que se basa en la debilidad humana para obtener los resultados deseados.

Además de la ingeniería social, existen otros tipos de ataques que explotan las vulnerabilidades del software de computadoras. Algunos ejemplos de técnicas de ataque son: virus, gusanos y caballos de Troya Todos estos son tipos de software maliciosos que se introducen en un host. Pueden dañar un sistema, destruir datos y también denegar el acceso a redes, sistemas o servicios. También pueden enviar datos y detalles personales de usuarios de PC desprevenidos a delincuentes. En muchos casos, pueden replicarse y propagarse a otros hosts conectados a la red.

En algunas ocasiones estas técnicas se utilizan en combinación con la ingeniería social para engañar a un usuario desprevenido a fin de llevar a cabo el ataque.

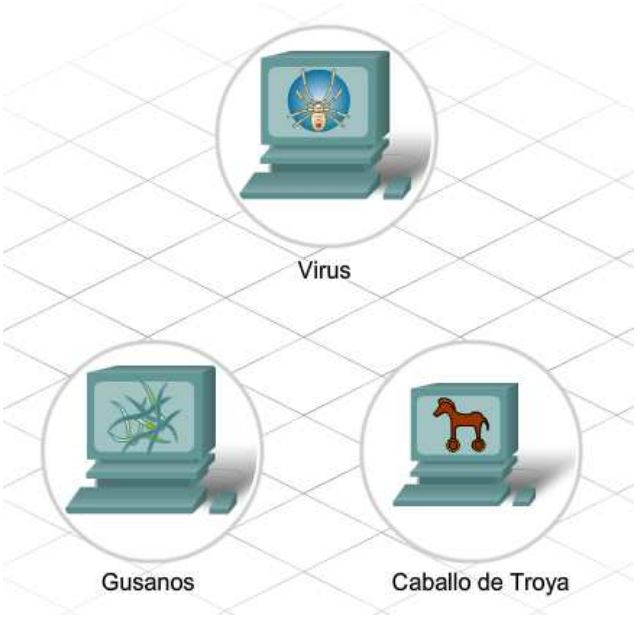


Figura 2.5 Métodos de Ataque [11]

2.4.1.1 Virus

Un virus es un programa que se ejecuta y se propaga al modificar otros programas o archivos. Un virus no puede iniciarse por sí mismo, sino que debe ser activado. Una vez que está activado, un virus no puede hacer más que replicarse y propagarse. A pesar de ser simple, hasta este tipo de virus es peligroso, ya que puede utilizar rápidamente toda la memoria disponible e interrumpir completamente el sistema. Un virus más peligroso puede estar programado para borrar o dañar archivos específicos antes de propagarse. Los virus pueden transmitirse mediante documentos adjuntos a correos electrónicos, archivos descargados, mensajes instantáneos, disquetes, CD o dispositivos USB.

2.4.1.2 Gusanos

Un gusano es similar a un virus pero, a diferencia de éste, no necesita adjuntarse a un programa existente. Un gusano utiliza la red para enviar copias de sí mismo a cualquier host conectado. Un gusano puede ejecutarse independientemente y propagarse rápidamente. No requieren necesariamente activación o intervención humana. Los gusanos que se propagan por sí mismos por la red pueden tener un impacto mucho mayor que un simple virus y pueden infectar rápidamente grandes partes de Internet.

2.4.1.3 Caballos de Troya

Un caballo de Troya es un programa que no se replica por sí mismo y que se escribe para asemejarse a un programa legítimo, cuando en realidad se trata de una herramienta de ataque. Un caballo de Troya se basa en su apariencia legítima para engañar a una víctima a fin de que inicie el programa. Puede ser relativamente inofensivo o contener códigos que pueden dañar el contenido del disco duro de la computadora. Los troyanos también pueden crear una puerta trasera en un sistema para permitir que los piratas informáticos obtengan acceso.

2.4.2 DENEGACIÓN DE SERVICIO Y ATAQUES DE FUERZA BRUTA

Por lo general, el objetivo de un atacante es interrumpir el funcionamiento normal de una red. Este tipo de ataque a menudo se lleva a cabo con el fin de interrumpir el funcionamiento de una organización.

2.4.2.1 Denegación de Servicio (DoS)

Los ataques DoS son ataques agresivos sobre una computadora personal o un grupo de computadoras con el fin de denegar el servicio a los usuarios a quienes está dirigido. Los ataques DoS tienen como objetivo sistemas de usuarios finales, servidores, routers y enlaces de red.

En general, los ataques DoS tienen como fin:

- Inundar un sistema o una red con tráfico a fin de evitar que el tráfico de red legítimo fluya.
- Interrumpir las conexiones entre un cliente y un servidor para evitar el acceso al servicio.

Existen varios tipos de ataques DoS. Los administradores de redes deben estar al tanto de los tipos de ataques DoS que se pueden producir a fin de asegurarse de que sus redes estén protegidas. Dos tipos comunes de ataques DoS son:

Flooding SYN (sincrónica): Se envía una gran cantidad de paquetes a un servidor, para solicitar una conexión de cliente. Los paquetes contienen direcciones IP de origen no válidas. El servidor se ocupa de responder a estas solicitudes falsas y, por lo tanto, no puede responder a las solicitudes legítimas.

Ping of death: Se envía a un dispositivo un paquete con un tamaño mayor que el máximo permitido por IP (65 535 bytes). Esto puede hacer que el sistema receptor colapse.

En las Figuras 2.6 (a, b, c y d) se puede observar la secuencia del proceso de Denegación de Servicio.

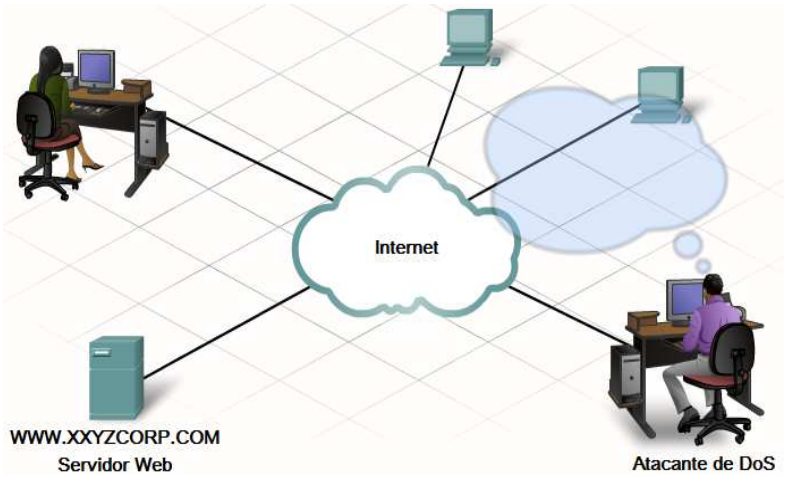


Figura 2.6 (a) Inicio de Ataque de DoS

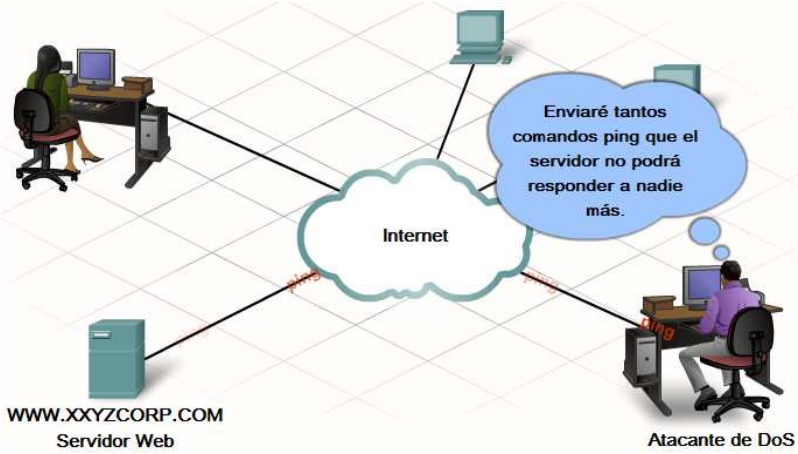


Figura 2.6 (b) Forma de Ataque a través de comandos ping

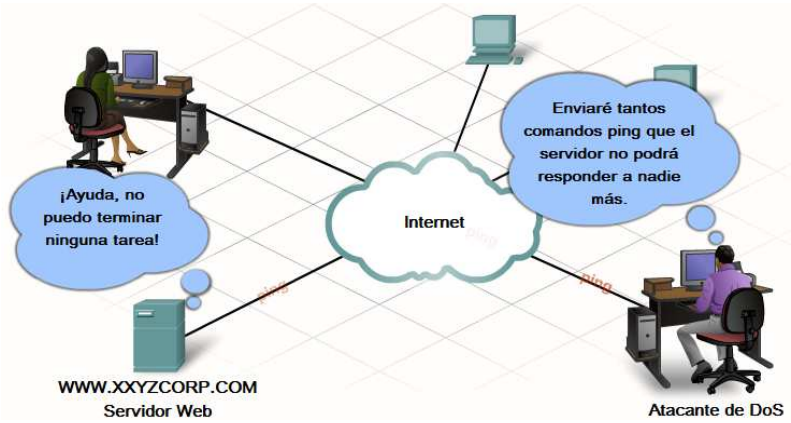


Figura 2.6 (c) Saturación del Servidor

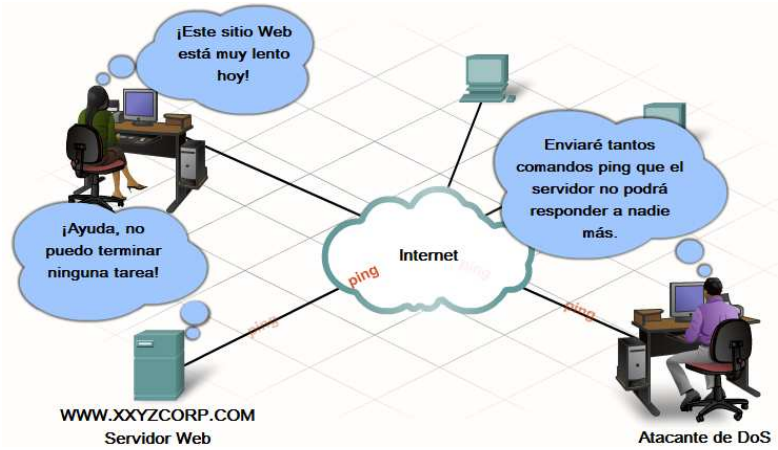


Figura 2.6 (d) Resultado del Ataque (Servicio lento)

Figura 2.6 Ejemplo de Denegación de Servicio [11]

2.4.2.2 Denegación de Servicio Distribuida (DDoS)

La DDoS es una forma de ataque DoS más sofisticada y potencialmente más perjudicial. Está diseñada para saturar y sobrecargar los enlaces de red con datos inútiles. Los ataques DDoS operan en una escala mucho mayor que los ataques DoS. Generalmente, cientos o miles de puntos de ataque intentan saturar un objetivo al mismo tiempo. Los puntos de ataque pueden ser computadoras inadvertidas que ya hayan sido infectadas por el código DDoS. Cuando son invocados, los sistemas infectados con el código DDoS atacan el sitio del objetivo.

En las Figuras 2.7 (a, b, c y d) se puede observar la secuencia del proceso de Denegación de Servicio Distribuida.

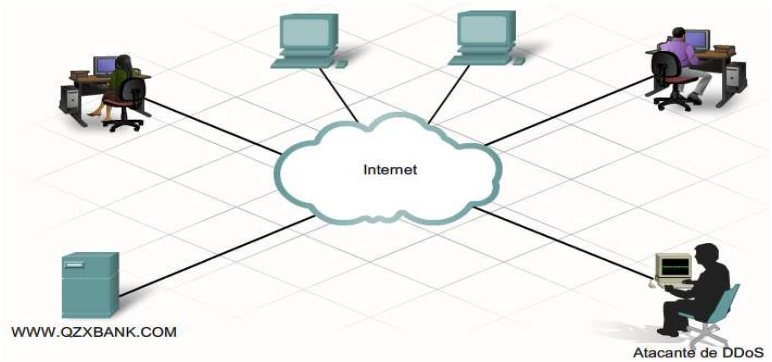


Figura 2.7 (a) Inicio de Ataque DDoS

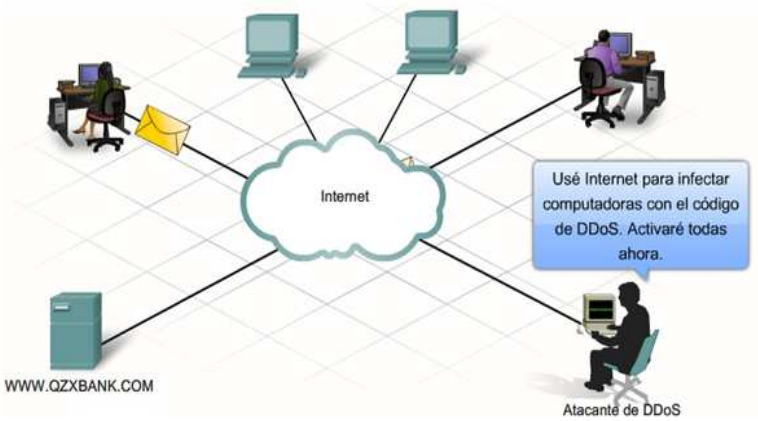


Figura 2.7 (b) Activación del código DDoS a través de Internet

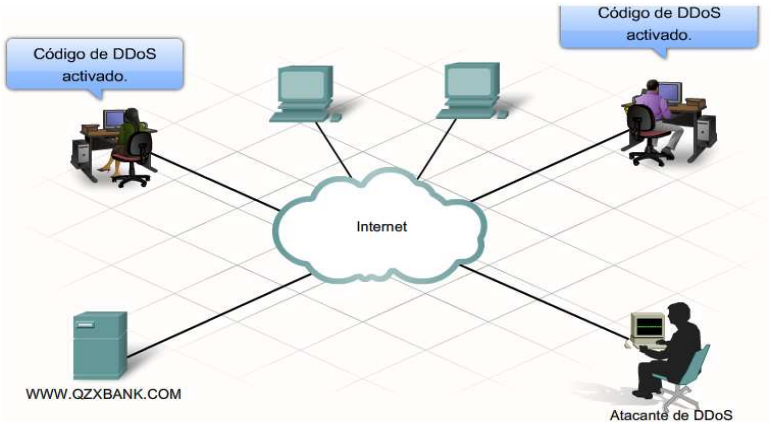


Figura 2.7 (c) Máquinas infectadas con código DDos que contiene tráfico inútil

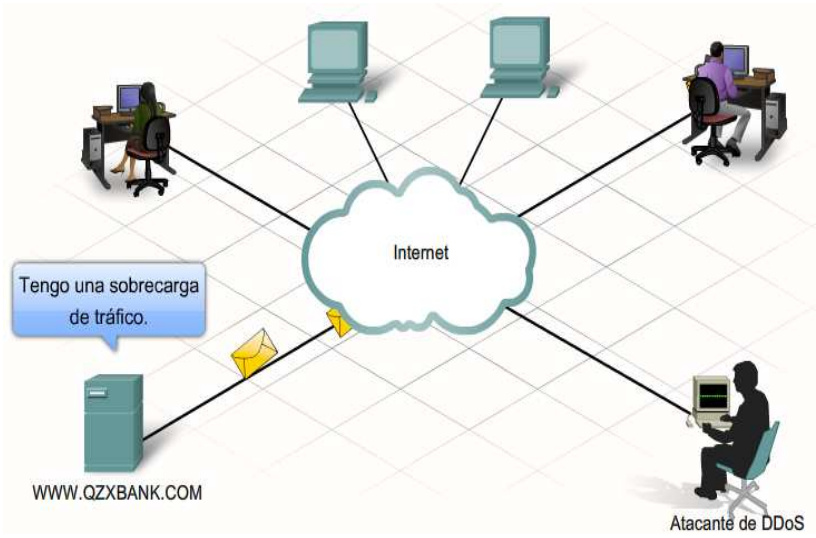


Figura 2.7 (d) Saturación del Servidor

Figura 2.7 Ejemplo de Denegación de Servicio Distribuida [11]

2.4.2.3 Ataques de Fuerza Bruta

No todos los ataques que provocan interrupciones en la red son ataques DoS específicos. Un ataque de fuerza bruta es otro tipo de ataque que puede causar la denegación de servicio.

En los ataques de fuerza bruta se utiliza una computadora veloz para tratar de adivinar contraseñas o para descifrar un código de encriptación[1]. El atacante prueba una gran cantidad de posibilidades de manera rápida y sucesiva para obtener acceso o descifrar el código. Los ataques de fuerza bruta pueden causar una denegación de servicio debido al tráfico excesivo hacia un recurso específico o al bloqueo de las cuentas de usuario.

2.4.3 SPYWARE, COOKIES DE SEGUIMIENTO, ADWARE Y ELEMENTOS EMERGENTES

No todos los ataques causan daños o evitan que los usuarios legítimos tengan acceso a los recursos. Muchas amenazas están diseñadas para recopilar información acerca de los usuarios que, a su vez, puede utilizarse con fines de publicidad, comercialización e investigación. Algunas de estas amenazas son el spyware, las cookies de seguimiento, el Adware y los elementos emergentes. Si bien es posible que éstos no dañen la computadora, sí pueden invadir la privacidad y generar molestias.

2.4.3.1 Spyware

El spyware es cualquier programa que reúne información personal de su computadora sin su permiso o conocimiento. Esta información se envía a los anunciantes u otros usuarios de Internet y puede incluir contraseñas y números de cuentas.

---

[1] **Código de Encriptación:** es el proceso de mezclar el contenido de un archivo o mensaje para hacerlo incomprensible para cualquiera que no posea la clave requerida para descifrar el archivo o mensaje.

Generalmente, el spyware se instala de manera inadvertida al descargar un archivo, instalar otro programa o hacer clic en un elemento emergente. Puede disminuir la velocidad de una computadora y realizar cambios a las configuraciones internas, y también crear más vulnerabilidades para otras amenazas. Además, el spyware puede ser muy difícil de eliminar.

2.4.3.2 Cookies de Seguimiento

Las cookies son un tipo de spyware, pero no siempre son perjudiciales. Se utilizan para registrar información de los usuarios de Internet cuando visitan sitios Web. Las cookies pueden ser útiles o convenientes, ya que permiten la personalización y otras técnicas que ahorran tiempo. Muchos sitios Web requieren que las cookies estén habilitadas para que el usuario pueda conectarse.

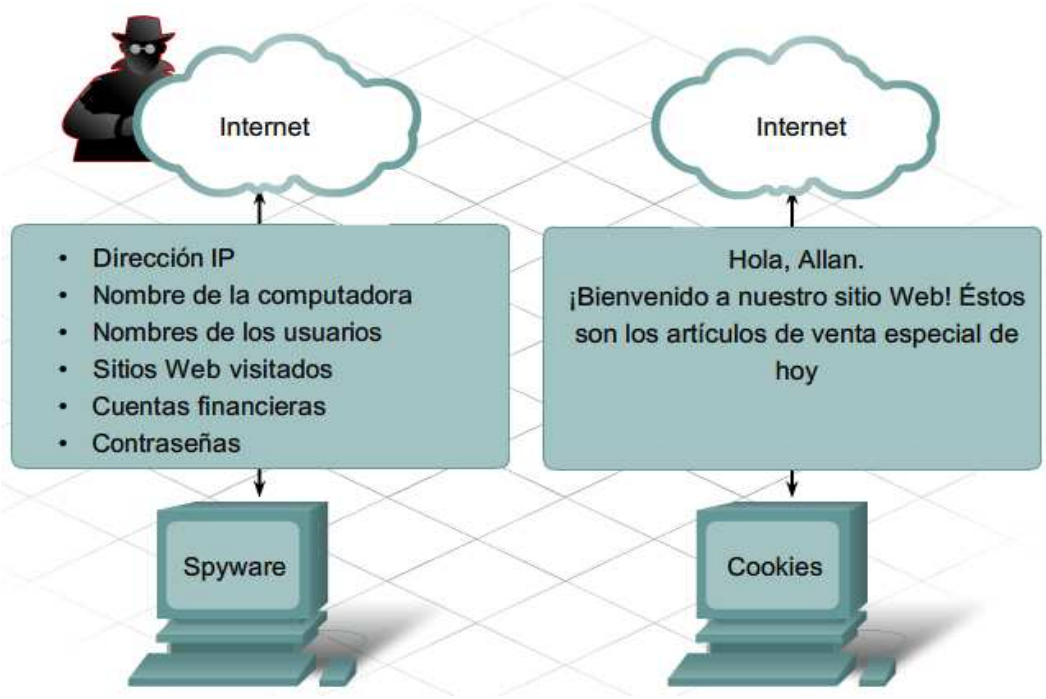


Figura 2.8 Spyware y Cookies de Seguimiento [11]

2.4.3.3 Adware

El Adware es una forma de spyware utilizada para recopilar información acerca de un usuario, de acuerdo con los sitios Web que éste visita. A continuación, esta información se utiliza para publicidad orientada a un usuario en particular. Generalmente, el usuario instala el Adware a cambio de un producto "gratuito". Cuando un usuario abre una ventana del explorador, el Adware puede iniciar nuevas ventanas que intentan publicitar productos o servicios de acuerdo con las prácticas de navegación del usuario. Las ventanas no deseadas del explorador pueden abrirse repetidamente y pueden dificultar mucho la navegación por Internet, en especial en las conexiones de Internet más lentas. El Adware puede ser muy difícil de desinstalar.

2.4.3.4 Elementos Emergentes y Ventanas pop-under

Los elementos emergentes y las ventanas pop-under son ventanas de publicidad adicionales que aparecen cuando se visita un sitio Web. A diferencia del Adware, los elementos emergentes y las ventanas pop-under no están diseñados para recopilar información acerca del usuario y generalmente sólo se asocian con el sitio que se visita.

- Elementos emergentes: Se abren delante de la ventana actual del explorador.
- Ventanas pop-under: Se abren detrás de la ventana actual del explorador.

Pueden ser molestas y, por lo general, publicitan productos o servicios no deseables.

Figura 2.9 Ejemplo de Adware, Elementos Emergentes y Ventanas pop-under [11]

2.4.4 CORREO NO DESEADO

Otro de los molestos productos derivados de nuestra confianza cada vez mayor en las comunicaciones electrónicas es el tráfico de correo electrónico no deseado. En algunas ocasiones, los comerciantes no desean perder tiempo con el marketing orientado. Desean enviar sus publicidades por correo electrónico a tantos usuarios finales como sea posible, con la esperanza de que alguien se interese en su producto o servicio. Este enfoque de marketing de amplia distribución en Internet se conoce como correo no deseado.

El correo no deseado es una amenaza seria para las redes, ya que puede sobrecargar los ISP (Proveedor del Servicio de Internet), los servidores de correo electrónico y los sistemas individuales de usuario final. A la persona u organización responsable de enviar el correo no deseado se la denomina spammer. Para enviar el correo electrónico los spammers utilizan, por lo general, los servidores de correo electrónico que no están protegidos por contraseña. Los spammers pueden utilizar técnicas de pirateo informático, como virus, gusanos y caballos de Troya para tomar control de las computadoras domésticas. A continuación, estas computadoras se utilizan para enviar correo no deseado sin conocimiento del propietario. El correo no deseado puede enviarse por correo

electrónico o, más recientemente, por medio de software de mensajería instantánea.

Se calcula que cada usuario de Internet recibe más de 3000 correos no deseados en un año. El correo no deseado consume grandes cantidades de ancho de banda de Internet y es un problema tan serio que algunos países ya tienen leyes que regulan su uso.

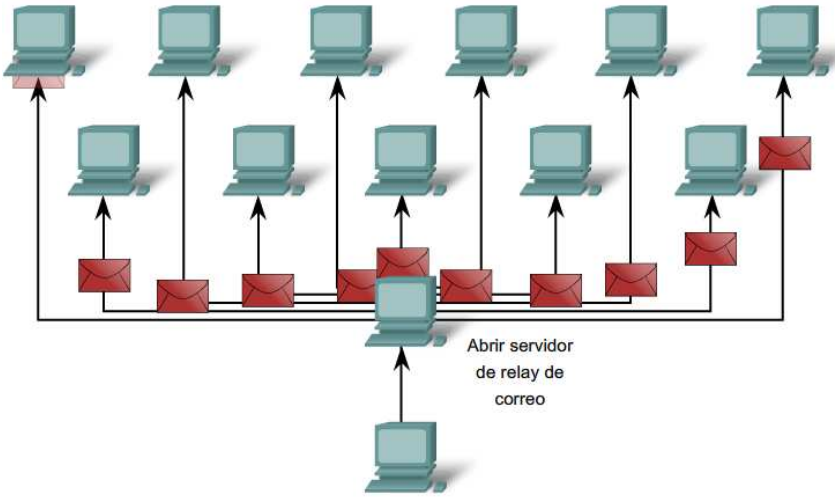


Figura 2.10 Correo no Deseado [11]

2.4.5 RESUMEN DE LAS AMENAZAS EN MATERIA DE SEGURIDAD

Las empresas que utilizan la red para vender sus productos u organizar la entrega de los mismos pueden verse paralizadas por un ataque del tipo "denegación de servicio". La información personal y financiera puede ser interceptada y utilizada con fines fraudulentos. La seguridad nacional puede verse amenazada. Estos ejemplos dan una idea del peligro que supone una seguridad deficiente. Cabe distinguir entre ataques intencionados y alteraciones no intencionadas. El objetivo es especificar el tipo de riesgos para la seguridad con el fin de preparar un marco político para mejorar la seguridad de las redes.

2.5 IDENTIFICACIÓN DE RIESGOS POTENCIALES QUE AFECTAN A LA SEGURIDAD EN LA RED

Un análisis de riesgo debe identificar los riesgos, recursos y datos de la red. El análisis de riesgo es identificar los componentes de la red, evaluar la importancia de cada uno de ellos, y entonces aplicar un nivel apropiado de seguridad. Esto ayuda a mantener un equilibrio laborable entre la seguridad y la accesibilidad a la red.

Se puede mencionar los siguientes pasos para identificar los riesgos potenciales que afectan a la seguridad de la red.

2.5.1 IDENTIFICACIÓN DEL RECURSO

Antes de que la red pueda afianzarse, se debe identificar los componentes individuales que constituyen la red. Se debe crear un inventario de los recursos, de todos los dispositivos de la red, como los ordenadores y servidores. Una vez que el inventario está completo, los componentes pueden priorizarse y pueden evaluarse para las vulnerabilidades.

2.5.2 VALORACIÓN DE VULNERABILIDADES

Una vez que los componentes de la red se han identificado, se pueden evaluar para las vulnerabilidades. Estas podrían ser las debilidades en la tecnología, configuración, o política de seguridad. Cualquier vulnerabilidad que se descubra necesitará ser analizada para descartar cualquier tipo de amenaza que podría aprovecharse de la vulnerabilidad. Las vulnerabilidades pueden ser solucionadas por varios métodos, aplicando parches de software, dispositivos de reconfiguración, u otras medidas como firewalls y software de anti-virus.

2.5.3 IDENTIFICACIÓN DE LA AMENAZA

Una amenaza es un evento que puede aprovecharse de una vulnerabilidad y puede causar un impacto negativo en la red. Las amenazas potenciales a la red

necesitan ser identificadas, y las vulnerabilidades relacionadas necesitan ser direccionadas para minimizar el riesgo de la amenaza.

2.6 POLITICAS DE SEGURIDAD [1] [11]

2.6.1 MEDIDAS COMUNES DE SEGURIDAD

No se pueden eliminar o evitar completamente los riesgos de seguridad. Sin embargo, tanto la administración como la evaluación efectiva de riesgos pueden minimizar significativamente los riesgos de seguridad existentes. Para minimizar los riesgos es importante comprender que no existe un único producto que pueda asegurar una organización. La verdadera seguridad de redes proviene de una combinación de productos y servicios junto con una política de seguridad exhaustiva y un compromiso de respetar esa política.

Una política de seguridad es una declaración formal de las normas que los usuarios deben respetar a fin de acceder a los bienes de tecnología e información. Puede ser tan simple como una política de uso aceptable o contener muchas páginas y detallar cada aspecto de conectividad de los usuarios, así como los procedimientos de uso de redes. La política de seguridad debe ser el punto central acerca de la forma en la que se protege, se supervisa, se evalúa y se mejora una red. Mientras que la mayoría de los usuarios domésticos no tiene una política de seguridad formal por escrito, a medida que una red crece en tamaño y en alcance, la importancia de una política de seguridad definida para todos los usuarios aumenta drásticamente. Algunos de los puntos que deben incluirse en una política de seguridad son: políticas de identificación y autenticación, políticas de contraseñas, políticas de uso aceptable, políticas de acceso remoto y procedimientos para el manejo de incidentes.

Políticas de Identificación y Autenticación: Especifica las personas autorizadas que pueden tener acceso a los recursos de la red y los procedimientos de verificación.

Incluye el acceso físico a los armarios de cableado estructurado y los recursos críticos de la red, por ejemplo switches, routers y puntos de acceso.

Políticas de Contraseña: Garantiza que las contraseñas cumplan con requisitos mínimos y se cambien periódicamente.

Políticas de usos aceptables: Identifican aplicaciones y usos de red que son aceptables.

Políticas de acceso remoto: Identifican cómo los usuarios remotos pueden obtener acceso a la red y qué elementos están disponibles a través de la conectividad remota.

Procedimientos de mantenimientos de red: Especifica los sistemas operativos de los dispositivos de la red y los procedimientos de actualización de las aplicaciones de los usuarios finales.

Procedimientos de administración de incidentes: Describe cómo se administran los incidentes de seguridad. Cuando se desarrolla una política de seguridad es necesario que todos los usuarios de la red la cumplan y la sigan para que sea efectiva.

La política de seguridad debe ser el punto central acerca de la forma en la que se protege, se supervisa, se evalúa y se mejora una red. Los procedimientos de seguridad implementan políticas de seguridad. Los procedimientos definen la configuración, el inicio de sesión, la auditoría y los procesos de mantenimiento de los hosts y dispositivos de red. Incluyen la utilización tanto de medidas preventivas para reducir el riesgo como de medidas activas acerca de la forma de manejar las amenazas de seguridad conocidas. Los procedimientos de seguridad abarcan desde tareas simples y poco costosas, como el mantenimiento de las versiones actualizadas de software, hasta implementaciones complejas de firewalls y sistemas de detección de intrusiones.

Algunas de las herramientas y aplicaciones de seguridad utilizadas en la protección de redes incluyen:

Parches y actualizaciones de software: Software aplicado a un sistema operativo o una aplicación para corregir una vulnerabilidad de seguridad conocida o agregar una funcionalidad.

Protección contra virus: Software instalado en una estación de trabajo de un usuario final o en un servidor para detectar y eliminar virus, gusanos y caballos de Troya de los archivos y los correos electrónicos.

Protección contra spyware: Software instalado en una estación de trabajo de un usuario final para detectar y eliminar spyware y adware.

Bloqueadores de correo no deseado: Software instalado en una estación de trabajo de un usuario final para identificar y eliminar correos electrónicos no deseados.

Bloqueadores de elementos emergentes: Software instalado en una estación de trabajo de un usuario final para evitar que se muestren ventanas de publicidad emergentes y pop-under.

Firewalls: Herramienta de seguridad que controla el tráfico que entra a la red y sale de ella.

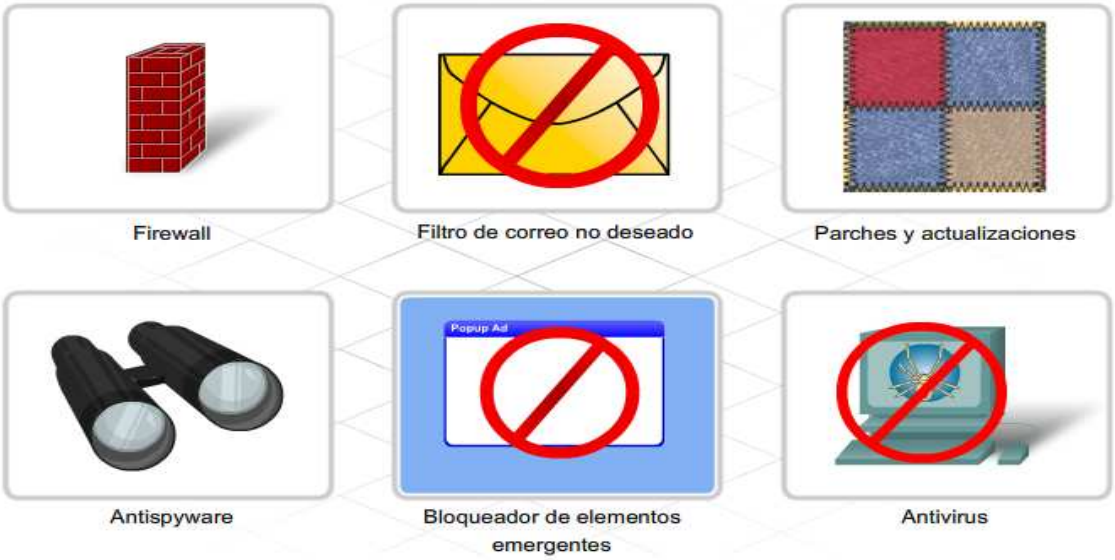


Figura 2.11 Herramientas y Aplicaciones de seguridad utilizadas en protección de redes [11]

2.6.2 PARCHES Y ACTUALIZACIONES

Uno de los métodos más comunes que utiliza un pirata informático para obtener acceso a los hosts y/o a las redes es atacar las vulnerabilidades del software. Es importante mantener las aplicaciones de software actualizadas con los últimos parches y actualizaciones de seguridad a fin de ayudar a evitar las amenazas. Un parche es un pequeño código que corrige un problema específico. Por otro lado, una actualización puede incluir funciones adicionales al paquete de software y también parches para problemas específicos.

Los proveedores de SO (sistemas operativos, como Linux, Windows, etc.) y aplicaciones proporcionan continuamente actualizaciones y parches de seguridad que pueden corregir vulnerabilidades conocidas del software. Además, los proveedores lanzan, por lo general, conjuntos de parches y actualizaciones, conocidos como paquetes de servicios. Afortunadamente, muchos sistemas operativos ofrecen una función de actualización automática que permite que las actualizaciones de SO y las aplicaciones se descarguen e instalen automáticamente en un host.

2.6.3 SOFTWARE ANTIVIRUS

Aun cuando los SO y las aplicaciones tengan todos los parches y actualizaciones, pueden seguir siendo vulnerables a ataques. Todo dispositivo conectado a una red es vulnerable a virus, gusanos y caballos de Troya. Éstos pueden utilizarse para dañar el código del SO, afectar el rendimiento de una computadora, alterar las aplicaciones y destruir los datos.

Éstos son algunos indicadores de la presencia de un virus, gusano o caballo de Troya:

- La computadora comienza a actuar de forma anormal.
- Los programas no responden al mouse y a las combinaciones de teclas.
- Los programas se inician o se apagan por sí solos.

- El programa de correo electrónico comienza a enviar grandes cantidades de correos.
- Se utiliza demasiado la CPU.
- Se ejecuta una gran cantidad de procesos, ya sean conocidos o no identificables.
- La computadora funciona mucho más lentamente o deja de funcionar.

El software antivirus puede utilizarse como herramienta preventiva o reactiva. Previene las infecciones y detecta y elimina virus, gusanos y caballos de Troya. El software antivirus debe estar instalado en todas las computadoras conectadas a la red. Existen muchos programas antivirus disponibles.

El software antivirus depende del conocimiento del virus para poder eliminarlo. Por lo tanto, cuando se identifica, es importante notificar al administrador de red acerca del virus o de cualquier comportamiento que se asemeje a un virus. Generalmente, esto se lleva a cabo al enviar un informe de incidentes de acuerdo con la política de seguridad de redes de la empresa.

Los administradores de red también pueden informar a la agencia de gobierno local encargada de los problemas de seguridad acerca de los nuevos casos de amenazas. Por ejemplo: el sitio Web de una de las agencias de los Estados Unidos es: https://forms.us-cert.gov/report/. Esta agencia se encarga de desarrollar medidas que permitan contrarrestar las nuevas amenazas de virus y también asegurar que estas medidas estén disponibles para los diferentes desarrolladores de software antivirus.

Algunas de las funciones que pueden incluirse en los programas antivirus son:

Verificación de correo electrónico: Escanea los correos electrónicos entrantes y salientes e identifica los archivos adjuntos sospechosos.

Escaneo dinámico de residentes: Verifica los archivos y documentos ejecutables cuando se accede a éstos.

Escaneos programados: Es posible programar escaneos de virus para que se ejecuten a intervalos regulares y verificar controladores específicos o toda la computadora.

Actualizaciones automáticas: Verifican y descargan características y patrones de virus conocidos. Se pueden programar para efectuar una verificación regular de actualizaciones.

Figura 2.12 Ejemplo de Software Antivirus [11]

2.6.4 SOFTWARE CONTRA CORREO NO DESEADO

El correo no deseado no sólo es molesto, sino que también puede sobrecargar los servidores de correo electrónico y potencialmente transportar virus y otras amenazas de seguridad. Así mismo, los spammers toman control de un host al implementar un código en forma de virus o caballo de Troya. Posteriormente, el host se utiliza para enviar correo no deseado sin el conocimiento del usuario. Una computadora infectada de esta forma se conoce como fábrica de correo no deseado.

El software contra correo no deseado protege a los hosts al identificar el correo no deseado y llevar a cabo una acción, como colocarlo en la carpeta de correo no deseado o borrarlo. Puede cargarse localmente en una máquina, pero también

puede cargarse en los servidores de correo electrónico. Además, muchos ISP ofrecen filtros de correo no deseado. El software contra correo no deseado no reconoce todo el correo no deseado, por lo que es importante tener cuidado al abrir los correos electrónicos. También puede identificar accidentalmente correo deseado como correo no deseado y tratarlo de la misma forma.

Además de utilizar bloqueadores de correo no deseado, algunas otras acciones preventivas para evitar la propagación de correo no deseado son:

1. Aplicar actualizaciones de SO y aplicaciones cuando estén disponibles.
2. Ejecutar los programas antivirus regularmente para mantenerlos actualizados.
3. No reenviar correos electrónicos sospechosos.
4. No abrir archivos adjuntos de correos electrónicos, en especial de personas desconocidas.
5. Establecer reglas en el correo electrónico para borrar el correo no deseado que logre ignorar al software contra correo no deseado.
6. Identificar las fuentes de correo no deseado y notificarlas al administrador de red para que puedan bloquearse.
7. Notificar incidentes a la agencia gubernamental que se ocupa del abuso del correo no deseado.

Uno de los tipos más comunes de correo no deseado enviado son las advertencias contra virus. Si bien algunas advertencias contra virus enviadas por correo electrónico son reales, una gran cantidad de ellas no es cierta y no existe realmente. Este tipo de correo no deseado puede ocasionar problemas, ya que las personas le advierten a otras acerca de los probables desastres, y de esta manera inundan el sistema de correos electrónicos. Además, los administradores de redes pueden exagerar y perder tiempo investigando un problema que no existe. Finalmente, muchos de estos correos electrónicos, en realidad, pueden contribuir a la propagación de virus, gusanos y caballos de Troya. Antes de reenviar correos electrónicos sobre advertencia contra virus, verifique en una fuente confiable que el virus sea real.

2.6.5 ANTISPYWARE Y ADWARE

El spyware y el adware también pueden causar síntomas similares a los de los virus. Además de recopilar información no autorizada, pueden utilizar recursos importantes de la computadora y afectar el rendimiento. El software antispyware detecta y elimina las aplicaciones de spyware y también evita las instalaciones futuras. Muchas aplicaciones antispyware también incluyen la detección y la eliminación de cookies y adware. Algunos paquetes antivirus incluyen funciones antispyware.

2.6.6 BLOQUEADORES DE ELEMENTOS EMERGENTES

El software bloqueador de elementos emergentes puede instalarse para evitar los elementos emergentes y las ventanas pop-under. Muchos exploradores Web incluyen, por defecto, una función bloqueadora de elementos emergentes. Tenga en cuenta que algunos programas y páginas Web crean elementos emergentes necesarios y convenientes. La mayoría de los bloqueadores de elementos emergentes ofrece una función de invalidación para este fin.

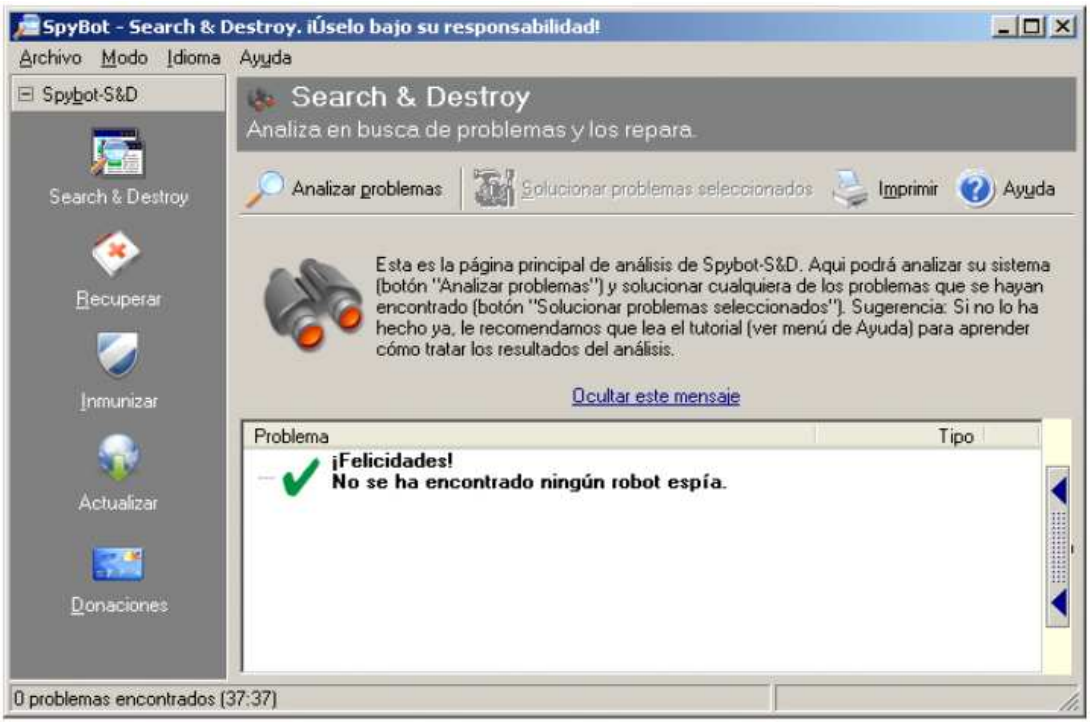


Figura 2.13 Ejemplo de Bloqueadores de Elementos Emergentes [11]

2.6.7 CREACIÓN DE UNA POLÍTICA APROPIADA

Se debe tomar en cuenta que cada organización es diferente, por tanto, cada organización tendrá diferentes políticas. Las plantillas de políticas son útiles para que la organización las examine y aprenda de ellas. Sin embargo, copiar palabra por palabra alguna política de otra organización no es la mejor manera de crear políticas.

2.6.7.1 Definición de lo que es importante

El primer paso en la creación de la política de la organización es definir cuales políticas son importantes. No todas las políticas serán necesarias para toda organización. Por ejemplo, una organización que genera información para internet puede requerir más que un plan de recuperación de desastres que de una política de uso de computadoras. El personal de seguridad de la organización debería poder identificar cuáles políticas son más relevantes e importantes para una organización. De no ser así, una evaluación de riesgos podría proporcionar una guía en esta área.

2.6.7.2 Definición de un comportamiento aceptable

El comportamiento aceptable de un empleado será diferente en relación con la cultura de la organización. Por ejemplo algunas organizaciones pueden permitir a todos los empleados a navegar en Internet sin restricción alguna. En ese caso, la cultura de la organización es confiar en sus empleados para asegurarse de que el trabajo se esté completando. Otras organizaciones pueden imponer restricciones como qué empleados pueden tener acceso a Internet y aun cargar software que restrinja el acceso a ciertos sitios web considerados inaceptables. Las políticas para estas organizaciones pueden diferir de manera significativa. De hecho, en el caso de la primera organización, ésta puede decidir no implementar en absoluto una política para el uso de Internet. Es importante que los profesionales de seguridad recuerden que no todas las políticas se ajustan bien a todas las organizaciones. Antes de que un profesional de seguridad comience a redactar la

política para una organización, debería tomarse algo de tiempo para aprender la cultura de dicha organización y las expectativas que ésta tiene respecto a sus empleados.

2.6.7.3 Identificación de las personas involucradas

Una política creada en el vacío rara vez tiene éxito. Teniendo esto en mente, el profesional de seguridad debe ser apto para manejar el desarrollo de la política con ayuda de otros miembros de la organización. El departamento de seguridad debería buscar el consejo del abogado general de la organización y del departamento de recursos humanos cuando desarrolle cualquier política. Otros grupos que podrían estar incluidos en el proceso pueden ser administradores del sistema, usuarios de sistemas de cómputo y el personal de seguridad física. En términos generales, todos los que serán afectados por la política deberían estar incluidos en el proceso de desarrollo de la misma, de manera que se obtenga un entendimiento de lo que se espera.

2.6.7.4 Definición de los perfiles apropiados

El desarrollo de una política comienza con un buen esquema. Existen muchas fuentes de buenos esquemas de política disponibles. Algunas de estas fuentes se encuentran en libros, y algunas otras están disponibles también en Internet. Por ejemplo, RFC 2196, “The Site Security Handbook”, proporciona varios esquemas para diversas políticas.

2.6.7.5 Desarrollo de la Política

El departamento de seguridad debería manejar el desarrollo de las políticas de seguridad. Esto no significa que el departamento de seguridad debería escribir las políticas sin la intervención de otros departamentos, sino que el departamento de seguridad debería hacerse cargo del proyecto y ver que se realice. Comenzar el proceso con un esquema y un borrador de cada sección de la política. Al mismo tiempo, contactar a las personas involucradas y hablarles del proyecto. Invitarles a

integrarse. Quienes acepten deberían recibir un borrador de la política y ser invitados a una reunión en la que el borrador será examinado y se hagan comentarios sobre él.

2.7 TECNOLOGÍAS DE SEGURIDAD [2] [8][11]

2.7.1 FIREWALL [2][6][11]

Además de proteger las computadoras y servidores individuales conectados a la red, es importante controlar el tráfico de entrada y de salida de la red.

El firewall es una de las herramientas de seguridad más efectivas y disponibles para la protección de los usuarios internos de la red contra las amenazas externas. El firewall reside entre dos o más redes y controla el tráfico entre ellas; de este modo, ayuda a prevenir el acceso sin autorización. Los productos de firewall usan diferentes técnicas para determinar qué acceso permitir y qué acceso denegar en una red.

Filtrado de paquetes: Evita o permite el acceso de acuerdo con las direcciones IP o MAC.

Filtrado de aplicaciones y sitios Web: Evita o permite el acceso de acuerdo con la aplicación. Se puede bloquear un sitio Web al especificar la dirección URL del sitio o algunas palabras clave.

Inspección de paquetes con estado (SPI): Los paquetes entrantes deben ser respuestas legítimas de los hosts internos. Los paquetes no solicitados son bloqueados, a menos que se permitan específicamente. La SPI también puede incluir la capacidad de reconocer y filtrar tipos específicos de ataques, como los ataques DoS.

Los productos de firewall pueden admitir una o más de estas capacidades de filtrado. Además, los firewalls llevan a cabo, por lo general, traducción de direcciones de red (NAT). NAT traduce una dirección interna o un grupo de

direcciones en una dirección pública y externa que se envía a través de la red. Esto permite ocultar las direcciones IP internas de los usuarios externos.

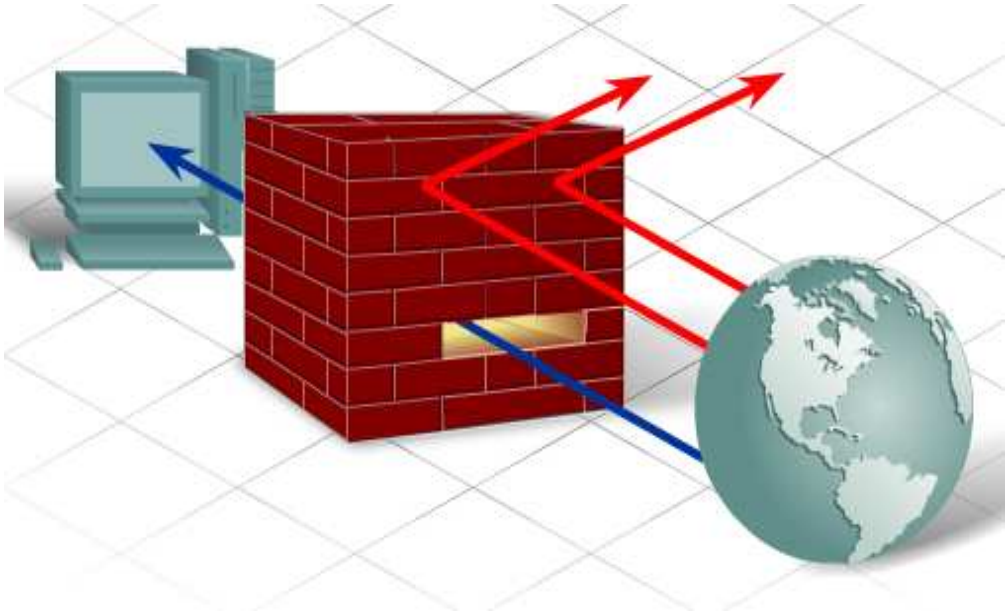


Figura 2.14 Firewall [11]

2.7.1.1 Formas de Suministración de Firewalls

Los productos de firewall se suministran de varias formas:

Firewalls basados en aplicaciones

Un firewall basado en una aplicación es un firewall incorporado en un dispositivo de hardware dedicado, conocido como una aplicación de seguridad. Las aplicaciones de seguridad son dispositivos que se utilizan exclusivamente como firewall con computadoras especializadas que no tienen periféricos ni discos duros. Los firewalls basados en aplicaciones pueden inspeccionar el tráfico con mayor rapidez y son menos propensos a sufrir fallos.

Firewalls basados en servidores

Un firewall basado en servidores consta de una aplicación de firewall que se ejecuta en un sistema operativo de red (NOS), como UNIX, Windows o Novell.

Estos firewalls generalmente proporcionan una solución que combina un firewall SPI y control de acceso basado en direcciones IP o aplicaciones. Los firewalls basados en servidores pueden ser menos seguros que los firewalls basados en dispositivos utilizados exclusivamente para ese fin, debido a la debilidad de seguridad de los sistemas operativos de propósito general.

Firewalls integrados

Se implementa un firewall integrado al añadir funcionalidades de hardware en un dispositivo existente, como un router. La mayoría de los routers integrados domésticos tienen incorporadas capacidades de firewall básicas que admiten el filtrado de paquetes, de aplicaciones y de sitios Web. Los routers más especializados que ejecutan sistemas operativos especiales como el Sistema Operativo de Internetwork de Cisco (IOS) también tienen capacidades de firewall que se pueden configurar.

Firewalls personales

Los firewalls personales residen en las computadoras host y no están diseñados para implementaciones LAN. Pueden estar disponibles por defecto en el SO o pueden ser instalados por un proveedor externo. Estos firewalls normalmente filtran con SPI. EL usuario puede tener que decidir si desea permitir la conexión de ciertas aplicaciones o puede definir una lista de excepciones automáticas. Con frecuencia los firewalls personales se utilizan cuando un dispositivo de host se conecta directamente a un modem ISP. Si no están bien configurados pueden interferir en el acceso a Internet. No se recomienda utilizar más de un firewall personal a la vez porque puede haber conflictos entre ellos.

Figura 2.15 Formas de Suministración de Firewall [11]

2.7.1.2 Utilización de un Firewall

Al colocar el firewall entre la red interna (intranet) e Internet como un dispositivo de frontera, se puede supervisar y controlar todo el tráfico de entrada y salida de Internet. Esto crea una clara línea de defensa entre la red interna y la externa. Sin embargo, existen algunos clientes externos que requieren acceso a los recursos internos. Se puede configurar una zona desmilitarizada (DMZ) para lograr esto.

El término zona desmilitarizada se adquiere de la terminología militar, donde una DMZ es una zona designada entre dos potencias, en la que la actividad militar no está permitida. En el ámbito de las redes de computadoras, una DMZ hace referencia a un área de la red que es accesible tanto para los usuarios internos como para los externos. Es más segura que la red externa, pero no tan segura como la red interna. Se crea a través de uno o más firewalls para separar las redes internas, externas o DMZ. Normalmente, en una DMZ se colocan servidores Web para acceso público.

En las siguientes figuras se puede observar la función que cumple un firewall tanto en la red interna como en la externa.

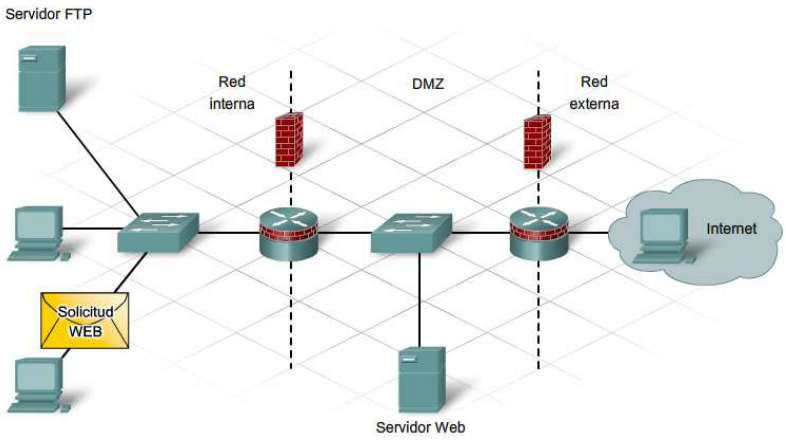


Figura 2.16 (a) Solicitud de un archivo Web desde la red interna

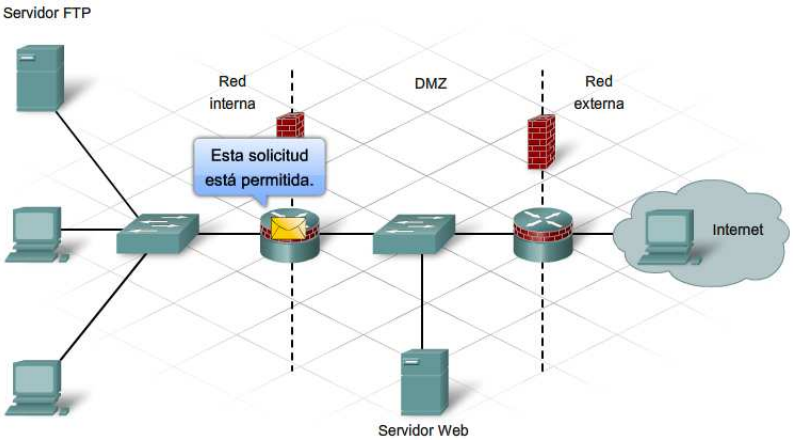


Figura 2.16 (b) Permiso de Solicitud en el Firewall de la red interna

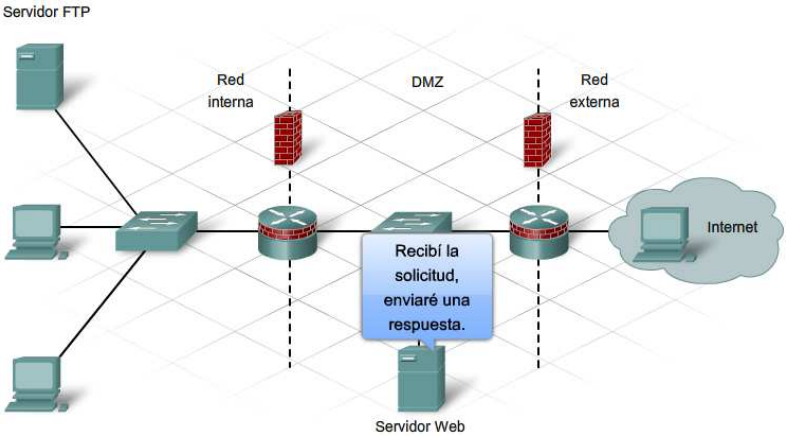


Figura 2.16 (c) Recibo y Envío en el Servidor de Web

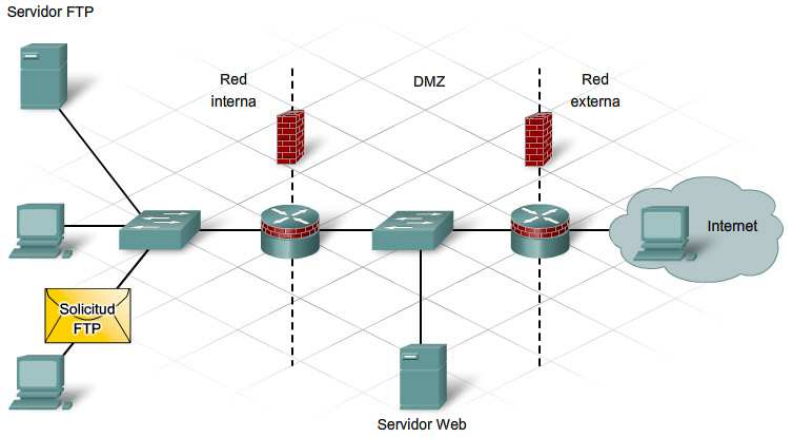


Figura 2.16 (d) Solicitud de un archivo FTP en la red interna

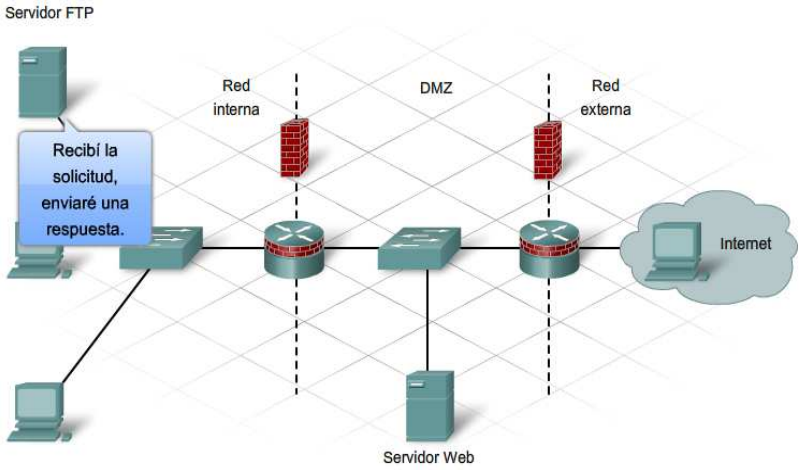


Figura 2.16 (e) Recibo y Envío en el Servidor FTP

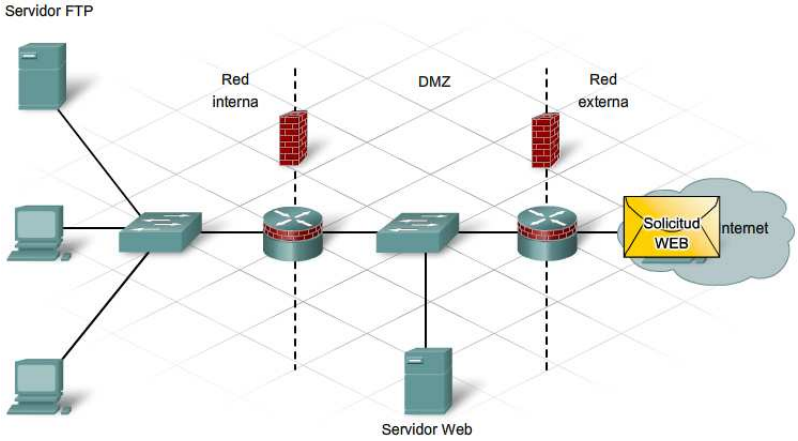


Figura 2.16 (f) Solicitud de archivo Web desde la red externa

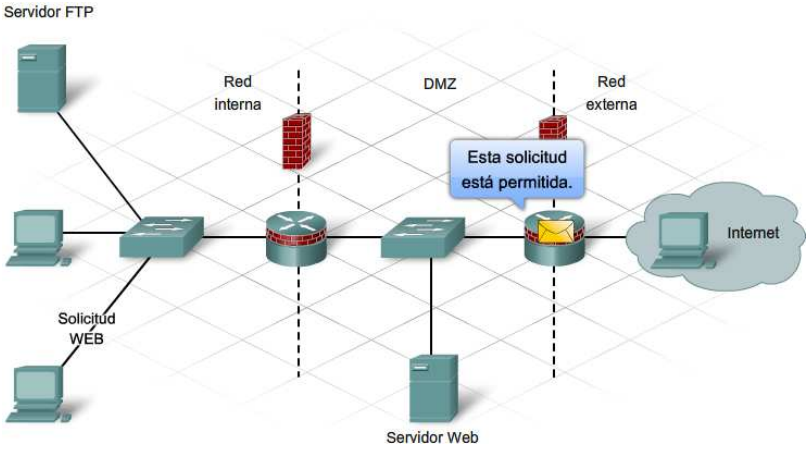


Figura 2.16 (g) Permiso de Solicitud en el Firewall de la red externa

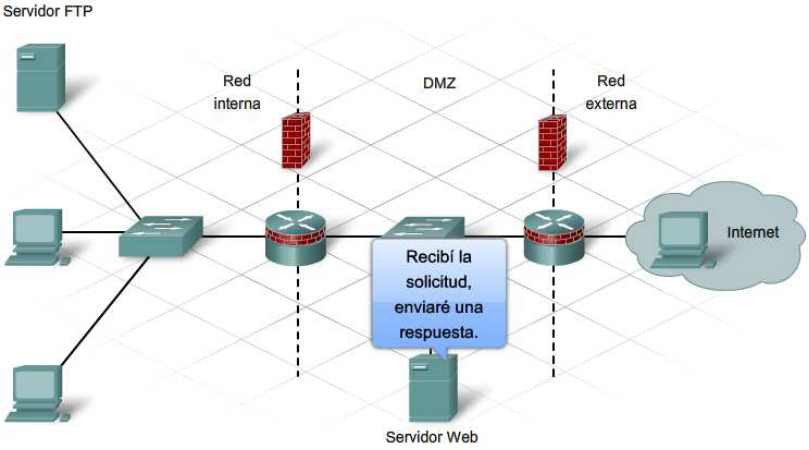


Figura 2.16 (h) Recibo y Envío en el Servidor de Web

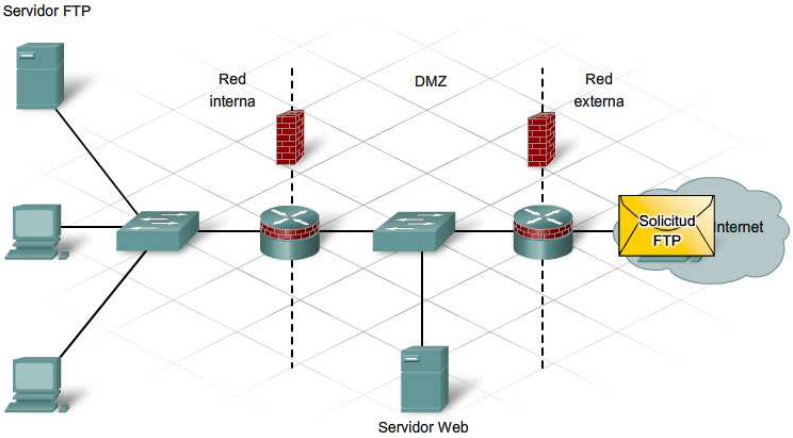


Figura 2.16 (i) Solicitud de un archivo FTP desde la red externa

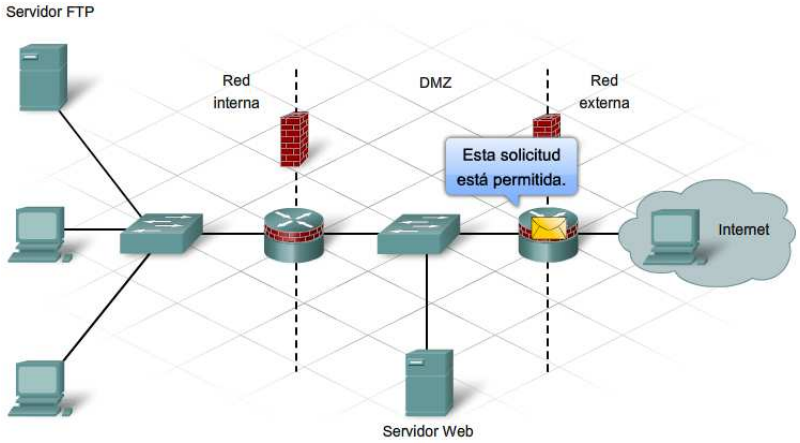


Figura 2.16 (j) Permiso de Solicitud en el Firewall de la red externa

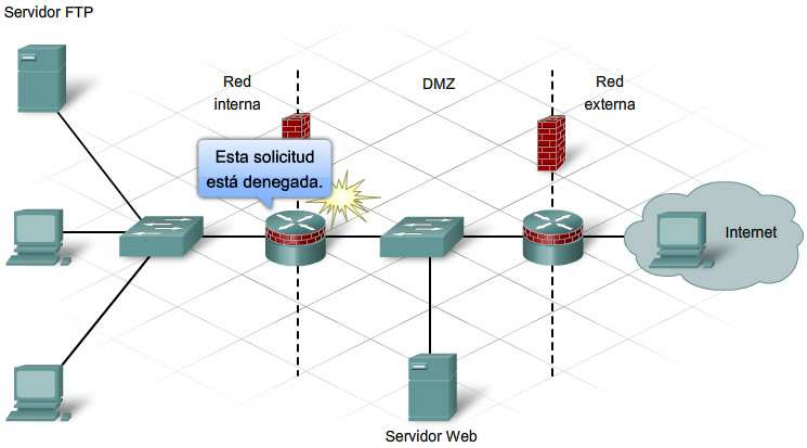


Figura 2.16 (k) Denegación de Solicitud en el Firewall de la red interna

Figura 2.16 Función de un Firewall en redes internas y externas [11]

2.7.1.3 Configuración de un solo Firewall

Un solo firewall tiene tres áreas, una para la red externa, una para la red interna y otra para la DMZ. Desde la red externa se envía todo el tráfico al firewall. A continuación, se requiere el firewall para supervisar el tráfico y determinar qué tráfico debe pasar a la DMZ, qué tráfico debe pasar internamente y qué tráfico debe denegarse por completo.

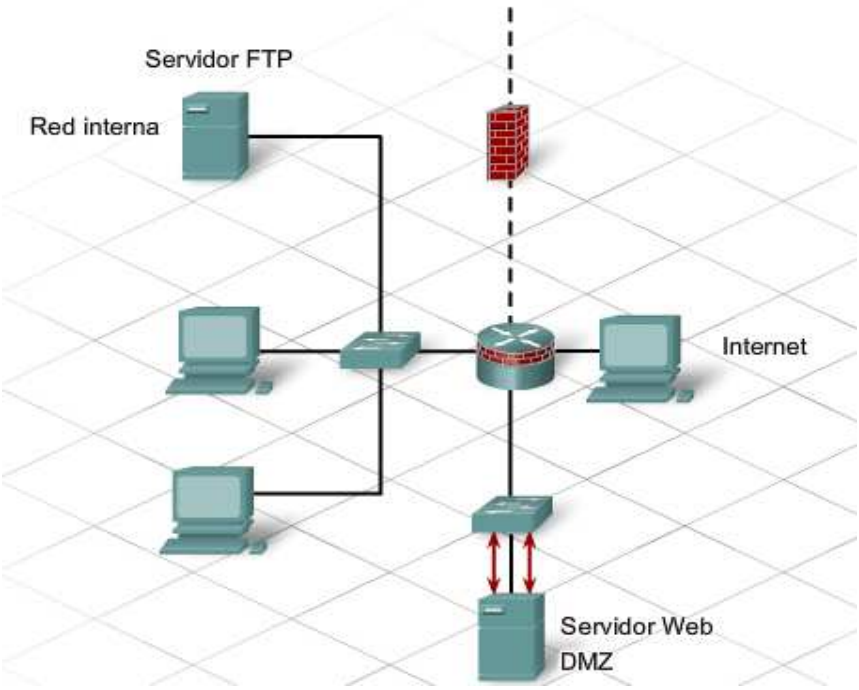


Figura 2.17 Configuración de un solo Firewall [11]

2.7.1.4 Configuración de dos Firewalls

En una configuración de dos firewalls hay un firewall interno y uno externo, con una DMZ ubicada entre ellos. El firewall externo es menos restrictivo y permite al usuario de Internet acceder a los servicios en la DMZ; además, concede al usuario externo cualquier solicitud de atravesar el tráfico. El firewall interno es más restrictivo y protege la red interna contra el acceso no autorizado.

Una configuración de un solo firewall es apropiada para las redes más pequeñas y menos congestionadas. Sin embargo, una configuración de un solo firewall tiene un único punto de falla y puede sobrecargarse. Una configuración de dos firewalls es más adecuada para redes más grandes y complejas que manejan mucho más tráfico.

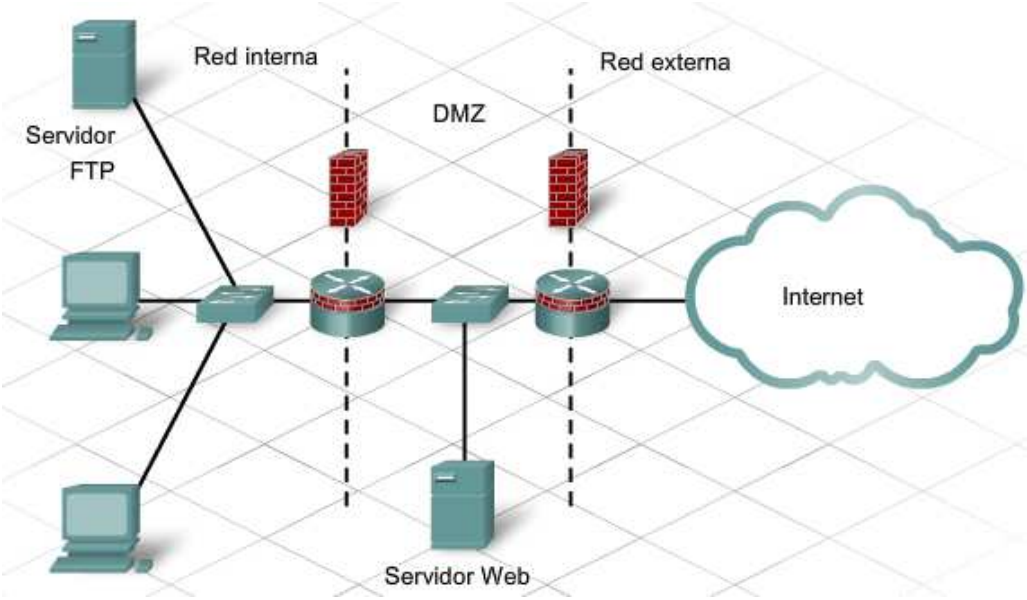


Figura 2.18 Configuración de dos Firewalls [11]

Por lo general, muchos dispositivos de redes domésticas, como los routers integrados, incluyen un software de firewall multifunción. Este firewall proporciona, comúnmente, traducción de direcciones de red (NAT); inspección de paquetes con estado (SPI); funciones de filtrado de IP, de aplicaciones y de sitios Web. También admite funciones de DMZ.

Con el router integrado se puede configurar una DMZ simple que permita a los hosts externos acceder al servidor interno. Para lograr esto el servidor requiere una dirección IP estática que debe especificarse en la configuración DMZ. El router integrado identifica el tráfico destinado a la dirección IP especificada. Posteriormente este tráfico se envía solamente al puerto del switch donde está conectado el servidor. Todos los demás hosts siguen protegidos por el firewall.

Cuando se habilita la DMZ, en su forma más simple, los hosts externos pueden acceder a todos los puertos del servidor, como 80 (HTTP), 21 (FTP) y 110 (correo electrónico POP3), etc.

Se puede configurar una DMZ más restrictiva mediante la capacidad de reenvío de los puertos. Mediante el reenvío de puertos se especifican los puertos que

deben estar accesibles en el servidor. En este caso, sólo el tráfico destinado a estos puertos está permitido, y todo el tráfico restante se excluye.

El punto de acceso inalámbrico dentro del router integrado se considera parte de la red interna. Es importante notar que si el punto de acceso inalámbrico no está protegido por una contraseña, toda persona que se conecte a ese acceso se encontrará dentro de la parte protegida de la red interna y detrás del firewall. Los piratas informáticos pueden utilizar esto para obtener acceso a la red interna e ignorar completamente toda la seguridad.

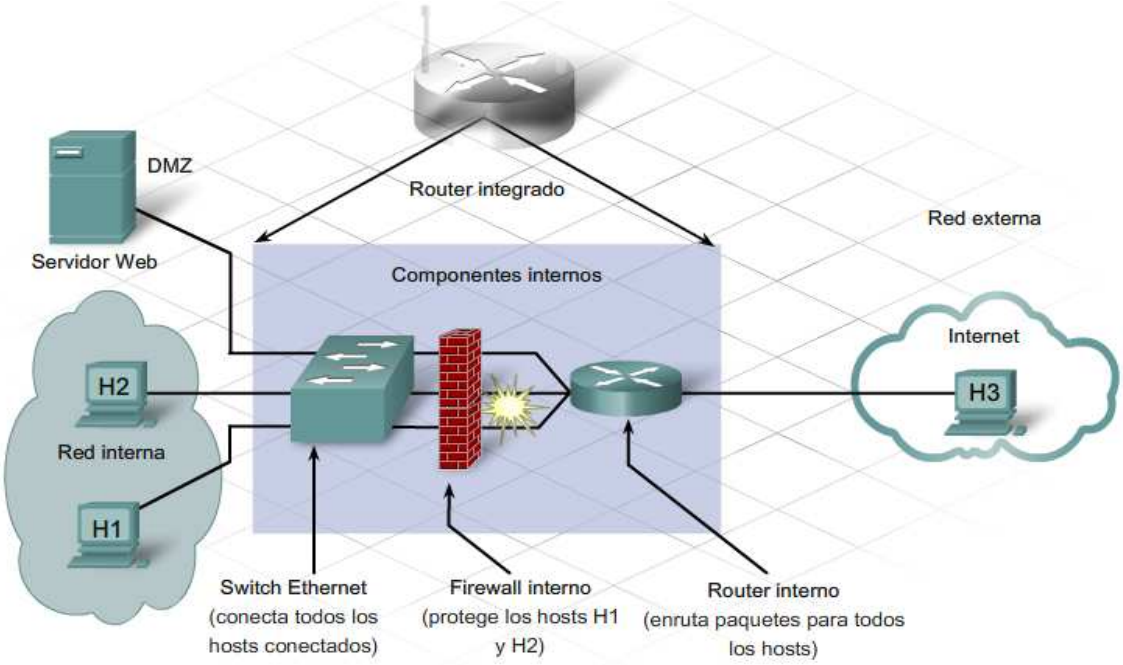


Figura 2.19 Utilización de un Firewall [11]

2.7.2 REDES PRIVADAS VIRTUALES (VPN) [1] [7][11]

2.7.2.1 Redes Privadas

Las redes privadas son utilizadas por las organizaciones para comunicarse con sitios remotos y con otras organizaciones. Las redes privadas se componen de líneas arrendadas a diversas compañías telefónicas y proveedores de servicio de Internet. Las líneas son punto a punto y los bits que viajan sobre estas líneas son

segregados del tráfico restante porque las líneas arrendadas crean un circuito real entre los dos sitios.

Las ventajas de las redes privadas son, que los sitios remotos pueden intercambiar información de manera instantánea y que los usuarios remotos no se sientan aislados.

La desventaja es el alto costo, por lo que muchas organizaciones han comenzado a adoptar las redes privadas virtuales (VPN). Estas ofrecen a las organizaciones muchas ventajas de las redes privadas con un costo menor. Sin embargo las VPN introducen un conjunto completamente nuevo de problemas y riesgos para una organización. Con una arquitectura e implementación adecuadas, las VPN pueden ser ventajosas para la organización. Pero con una arquitectura e implementación deficiente, toda la información que pasa a través de la VPN también puede quedar expuesta a Internet.

2.7.2.2 Características de las VPN

Las VPN tienen las siguientes características:

- El tráfico está encriptado, de modo que se evite la escucha furtiva.
- El sitio remoto está autenticado o validado.
- Múltiples protocolos son soportados por la VPN.
- La conexión es de punto a punto.

A continuación se mira más de cerca cada una de las características de las VPN. Se ha establecido que el tráfico de una VPN está encriptado para evitar la escucha furtiva. La encriptación debe ser lo suficientemente robusta para garantizar la confiabilidad del tráfico durante el período en que la información transmitida es valiosa.

La segunda característica es que el sitio remoto sea autenticado. Esta característica puede requerir que algunos usuarios sean autenticados o validados ante un servidor central, o pueden requerir que ambos extremos de la VPN se

autentifiquen entre sí. El mecanismo de autentificación o validación utilizado estará gobernado por la política.

Las VPN son construidas para manejar protocolos diferentes, especialmente en la capa de aplicación. Por ejemplo un usuario remoto puede utilizar SMTP para comunicarse con un servidor de correo mientras que también utiliza NetBIOS para comunicarse con un servidor de archivos. Ambos protocolos se ejecutarán sobre el mismo canal o circuito de la VPN.

Punto a punto quiere decir que los dos extremos de la VPN establecen un canal único entre ellos. Cada punto extremo puede tener varias VPN abiertas con otros extremos de manera simultánea, pero cada uno es distinto de los otros, y el tráfico es separado mediante la encriptación.

2.7.2.3 Tipos de VPN

VPN de Usuario

Las VPN de usuario son redes privadas virtuales entre la máquina de un usuario individual y la red o el sitio de una organización. Con frecuencia las VPN de usuario son utilizadas por los empleados que viajan o que trabajan desde casa. El servidor de VPN puede ser el Firewall o un servidor VPN separado. El usuario se conecta a Internet para establecer la VPN con la organización.

El sitio de la organización solicita la autenticación del usuario y, si tiene éxito, permite que éste tenga acceso a la red interna de la organización como si dicho usuario estuviera dentro del sitio y físicamente en la red. La VPN de usuario puede permitir que la organización limite los sistemas de archivo a los que puede tener acceso el usuario remoto. Esta limitación debería estar basada en las políticas de la organización y depende de las capacidades del producto de VPN.

Aunque el usuario tiene una VPN hacia la red interna de la organización, también tiene una conexión a Internet y puede navegar en la Web o realizar otras actividades como un usuario normal de Internet. La VPN es manejada mediante una aplicación por separado en la computadora del usuario.

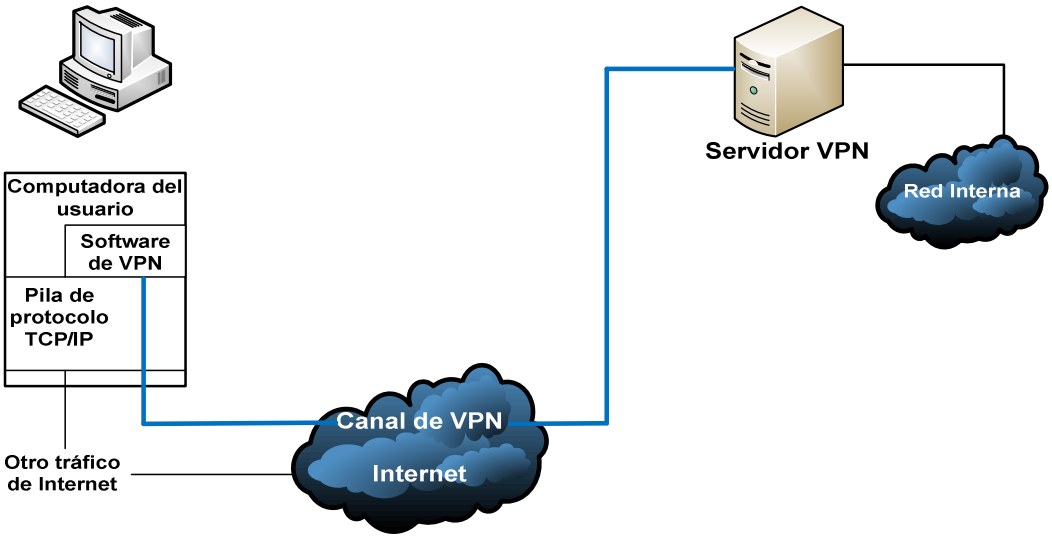


Figura 2.20 Configuración VPN de usuario [1]

VPN de Sitio

Las VPN de sitio son empleadas por las organizaciones para conectar sitios remotos, sin la necesidad de costosas líneas arrendadas o para conectar dos organizaciones diferentes que deseen comunicarse con algún propósito de negocios. Generalmente, la VPN conecta un firewall o un enrutador limítrofe con otro firewall o enrutador limítrofe.

Para iniciar la conexión, un sitio intenta enviar tráfico hacia el otro. Esto causa que los dos extremos de la VPN inicie la VPN. Los dos extremos negociarán los parámetros de la conexión dependiendo de las políticas de los dos sitios. Los dos sitios también se autenticarán entre sí utilizando algún secreto compartido que haya sido configurado previamente. Algunas organizaciones utilizan las VPN de sitio para vínculos de respaldo para líneas arrendadas.

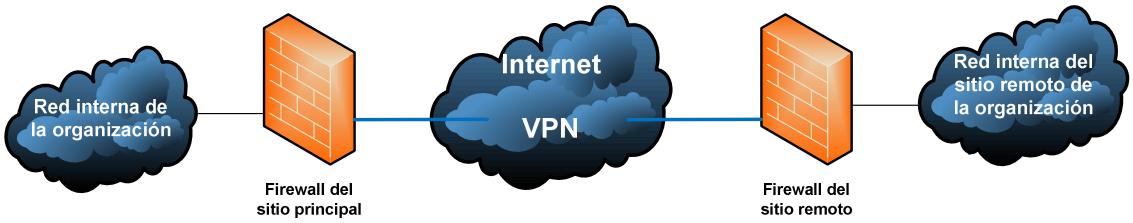


Figura 2.21 Configuración VPN de sitio [1]

2.7.3 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS) [6][11]

Constituyen sistemas administradores competentes que auditan y monitorean continuamente sus sistemas en busca de intrusiones. La detección de intrusiones es el arte de detectar actividades no autorizadas, inapropiadas o extrañas.

Los IDS son capaces de detectar ataques en progreso, generar alarmas en tiempo real y contrarrestar un ataque mediante el lanzamiento de un evento o la reconfiguración del router o Firewall.

Actúan como guardianes de seguridad o centinelas, constantemente están escaneando el tráfico de red o los logs de auditoría de un host.

2.7.3.1 Sistemas de Detección de Intrusos para Host (HIDS)

Reside en el host y es capaz de monitorear y negar servicios automáticamente si una actividad sospechosa es detectada; usan los archivos log y los agentes de auditoría del sistema para realizar el monitoreo.

- **Verificadores de integridad del sistema (SIV).** Es un mecanismo encargado de monitorizar archivos de una máquina en busca de posibles modificaciones no autorizadas.
- **Monitores de registros (LFM).** Monitorizan los archivos de log generados por los programas de una máquina en busca de patrones que puedan indicar un ataque o una intrusión.
- **Sistemas de decepción.** Son mecanismos encargados de simular servicios con problemas de seguridad de forma que un pirata piense que realmente el problema se puede aprovechar para acceder a un sistema, cuando realmente se está aprovechando para registrar todas sus actividades.

2.7.3.2 Sistemas de Detección de Intrusos para Red (NIDS)

Monitoriza los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella; el IDS puede

situarse en cualquiera de los hosts o en un elemento que analice todo el tráfico (como un HUB o un enrutador); éste analiza los siguientes elementos:

- Campos de fragmentación IP.
- Dirección origen y destino.
- Puerto origen y destino.
- Flags TCP.
- Campo de datos.

2.7.3.3 Detección de Anomalías

La base del funcionamiento de estos sistemas es suponer que una intrusión se puede ver como una anomalía del sistema. Estos modelos de detección conocen lo que es normal en la red o las máquinas a lo largo del tiempo, desarrollando y actualizando conjuntos de patrones contra los que se compararán los eventos que se producen en los sistemas, se tiene:

- Métodos estadísticos que determinan los perfiles de comportamiento habitual.
- Especificación de reglas que establecen los perfiles de comportamiento normal.

2.7.3.4 Detección de Usos Indebidos

El funcionamiento de los IDS basados en la detección de usos indebidos presupone que se puede establecer patrones para los diferentes ataques conocidos y algunas de sus variaciones. Este esquema se limita a conocer lo anormal. Para poder detectar intrusiones, se tiene:

- Sistemas expertos
- Transición de estados
- Comparación y emparejamiento de patrones
- Detección basada en modelos

2.7.4 ANALISIS DE VULNERABILIDAD

Existen muchas herramientas de análisis de vulnerabilidad para evaluar la seguridad de los hosts y de la red. Estas herramientas se conocen como escáneres de seguridad y pueden ayudar a identificar áreas donde es posible que se produzcan ataques; además de brindar asistencia acerca de las medidas que se pueden tomar. Si bien las capacidades de las herramientas de análisis de vulnerabilidad pueden variar de acuerdo con el fabricante, algunas de las funciones más comunes incluyen la determinación de:

- La cantidad de hosts disponibles en la red.
- Los servicios que los hosts ofrecen.
- El sistema operativo y las versiones de los hosts.
- Los filtros de paquetes y firewalls en uso.

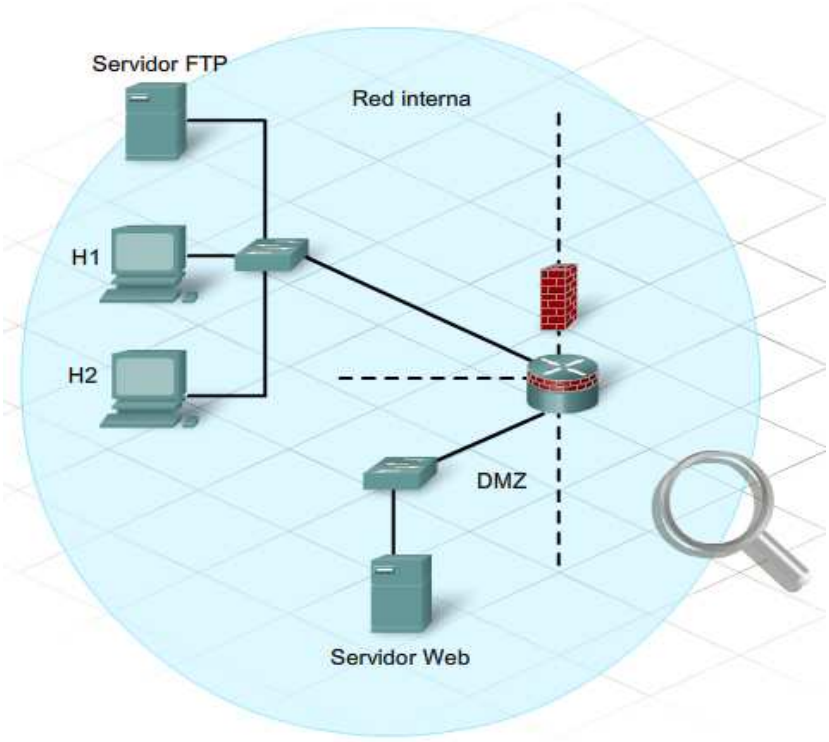


Figura 2.22 Análisis de Vulnerabilidades [11]

2.7.5 OPTIMIZACIONES

Existen varias prácticas recomendadas para ayudar a mitigar los riesgos que presentan, entre ellas:

- Definir las políticas de seguridad
- Asegurar físicamente los servidores y el equipo de la red
- Establecer permisos de inicio de sesión y acceso a archivos
- Actualizar el SO y las aplicaciones
- Cambiar las configuraciones permisivas por defecto
- Ejecutar software antivirus y antispyware
- Actualizar los archivos del software antivirus
- Activar las herramientas del explorador: bloqueadores de elementos emergentes, herramientas contra la suplantación de identidad y monitores de plug-in

El primer paso para asegurar una red es comprender la forma en que se mueve el tráfico a través de la red, además de las diferentes amenazas y vulnerabilidades que existen. Una vez que se implementan las medidas de seguridad, una red verdaderamente segura debe supervisarse constantemente. Los procedimientos y las herramientas de seguridad deben verificarse para poder mantenerse a la vanguardia de las amenazas que se desarrollan.

2.7.6 UTM (UNIFIED THREAT MANAGEMENT)

Los avances de la tecnología y el desarrollo de amenazas cada vez más peligrosas y complejas, ha determinado que las soluciones de seguridad perimetral evolucionen a los sistemas de seguridad multi-amenazas, que constituyen la nueva generación de los sistemas de protección de red en tiempo real.

Los sistemas unificados de administración de amenazas (UTM) detectan y eliminan las más dañinas amenazas basadas en el contenido e-mail o tráfico web

tales como virus, gusanos, intrusiones, contenido web inapropiado y más en tiempo real, sin degradar el rendimiento de la red.

Un sistema de seguridad debe poseer varios componentes que trabajen conjuntamente con el fin de aproximarse a un sistema seguro, es así que los sistemas UTM incorporan varias técnicas y componentes de seguridad para lograr el acercamiento a este objetivo.

Los sistemas reinantes actualmente como los Firewall, VPNs e IDS resultan efectivos proporcionando protección a nivel de red; sin embargo, no cubren las necesidades de protección actual en los ámbitos telemáticos, ya que su capacidad permite el análisis de la cabecera de los paquetes pero no el análisis del contenido de los mismos.

Estos sistemas no pueden comprobar el contenido del paquete y procesarlo para identificar virus, gusanos u otras amenazas; por lo tanto, son ineficaces contra ataques basados en contenido. Así los virus, gusanos, troyanos, etc, transmitidos por correo electrónico y tráfico http atraviesan fácilmente los Firewall, VPN o IDS.

Toda esta evolución de tecnología ha acelerado la necesidad de implantación de soluciones de defensa en profundidad a nivel de contenido. Aparentemente el reto de los fabricantes y proveedores de seguridad es la gestión eficiente de respuesta ante los nuevos ataques que nacen en el Internet y en proporcionar firmas actualizadas y efectivas para controlar dichos ataques.

Los sistemas UTM constituyen el software y hardware específico para la seguridad de redes, sus más comunes y principales características son el uso de tecnología ASIC (Application-Specific Integrated Circuit) y la integración de diferentes módulos de seguridad que garantizan la adecuada protección de la red sin degradar su rendimiento.

Finalmente para complementar la seguridad en entornos extremadamente críticos se incluye HIDS sistemas de seguridad en profundidad encargados de detectar y proteger a un sistema en particular de intrusiones; así se puede controlar de

manera exhaustiva los datos, aplicaciones y accesos que se procesan en una determinada máquina.

Los dispositivos UTM combinan las funciones de diferentes dispositivos de seguridad, administración y análisis dentro de un solo ambiente más flexible, lo cual permite desarrollar en forma integral múltiples características de seguridad (políticas de seguridad) en una sola plataforma.

Estos sistemas están ganando popularidad rápidamente debido al rendimiento que ofrecen en aplicaciones de seguridad, costo de operación e inversión de capital.

2.8 MODELOS DE SEGURIDAD ABIERTOS Y CERRADOS [11]

Con todos los planes de seguridad, hay algún intercambio entre la productividad del usuario y medidas de seguridad. La meta de un plan de seguridad es proporcionar el mínimo impacto y la seguridad máxima en el acceso del usuario y productividad. La seguridad mide la forma de encriptación de datos de red, y que no restrinja acceso y productividad. Por otro lado, la comprobación redundante y la autorización al sistema pueden frustrar a los usuarios y pueden prevenir el acceso a los recursos críticos de la red.

Las necesidades comerciales deben dictar la política de seguridad. Una política de seguridad no debe determinar cómo un negocio opera. Porque las organizaciones constantemente están sujetas al cambio, deben ponerse al día las políticas de seguridad sistemáticamente para reflejar nuevas direcciones comerciales, cambios tecnológicos, y asignaciones del recurso.

Las políticas de seguridad pueden variar considerablemente en el plan. Existen tres tipos generales de modelos de seguridad, estos son: abiertos, restrictivos, y cerrados. En la Figura 2.21 se puede ver una guía para entender las clases de modelos de seguridad.

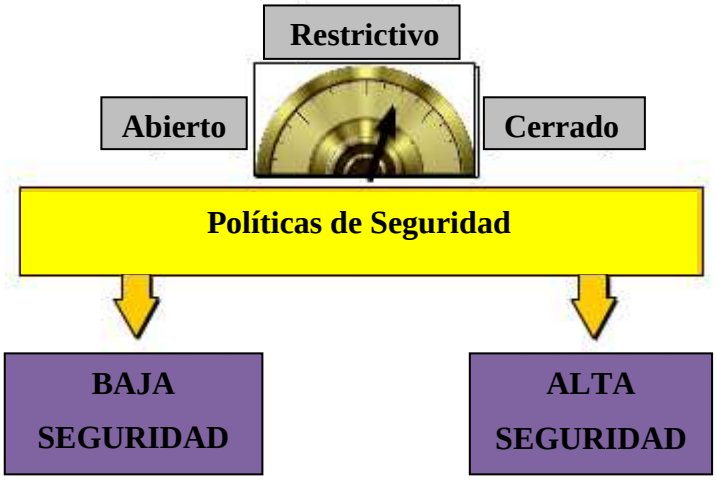


Figura 2.23 Métodos de Seguridad [4]

- El modelo de seguridad puede estar abierto o cerrado como un punto de partida.
- Se escoge un punto de equilibrio para la mejor seguridad.
- La seguridad para los niveles de aplicación puede incluir la tecnología SSL.

Tal como los modelos de seguridad, muchos dispositivos pueden ser clasificados como abiertos, restrictivos o cerrados. Por ejemplo, los routers y switches son los dispositivos típicamente abiertos, ya que permiten funcionalidad alta y servicios por defecto. Por otro lado, un firewall es típicamente un sistema cerrado que no permite ningún servicio hasta que se den los permisos necesarios. Los sistemas operativos del servidor pueden entrar en cualquiera de las tres categorías, dependiendo del fabricante. Es importante entender estos principios al manejar estos dispositivos.

2.8.1 ACCESO ABIERTO

Un modelo de seguridad abierto es el más fácil de llevar a cabo, ya que en este plan se mantienen pocas medidas de seguridad. Los Administradores configuran el hardware y software existente con capacidades de seguridad básicas. El firewall, las Redes Privadas Virtuales (VPN), los Sistemas de Descubrimiento de Intrusión (IDS) y otros medios que representan un costo adicional no son utilizados típicamente. Las contraseñas simples y los servicios de seguridad

llegan a ser lo fundamental para el modelo de acceso abierto. Para los usuarios individuales o para los servidores se puede utilizar la encriptación.

En este modelo se asume que los recursos protegidos son mínimos, por lo que las amenazas se reducen considerablemente. Sin embargo, esto no excluye la necesidad por tener un sistema de respaldo de datos como una buena política para modelos de seguridad abiertos. A este modelo se ajustan las redes LANs que no se conectan a Internet o a redes WANs.

Es un modelo en el cual se da el acceso libre a los usuarios a todas las áreas de la red, por lo que es muy probable que se produzcan daños y perdidas de la información. Normalmente no se tiene administradores de red responsables para controlar este tipo de abuso.

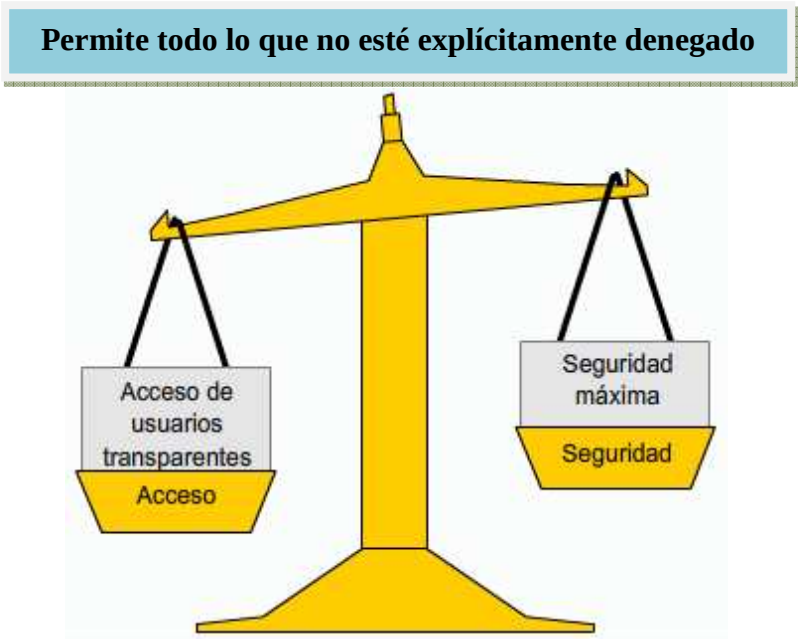


Figura 2.24 Acceso Abierto [4]

2.8.2 ACCESO RESTRICTIVO

Un modelo de seguridad restrictivo es más difícil llevar a cabo, ya que en este plan se mantienen muchas medidas de seguridad. Los Administradores configuran el hardware y software existente para las necesidades de seguridad, además se deben adquirir hardware más costoso y soluciones de software como

los firewall, VPN, IDS, y servidores de identidad. Los firewall y servidores de identidad se convierten en los dispositivos fundamentales para el modelo de acceso restrictivo. Este modelo asume que los recursos protegidos son considerables, algunos usuarios no son confiables, y las amenazas son probables. A este modelo se ajustan las reds LANs que se conectan a la Internet o a redes WANs.

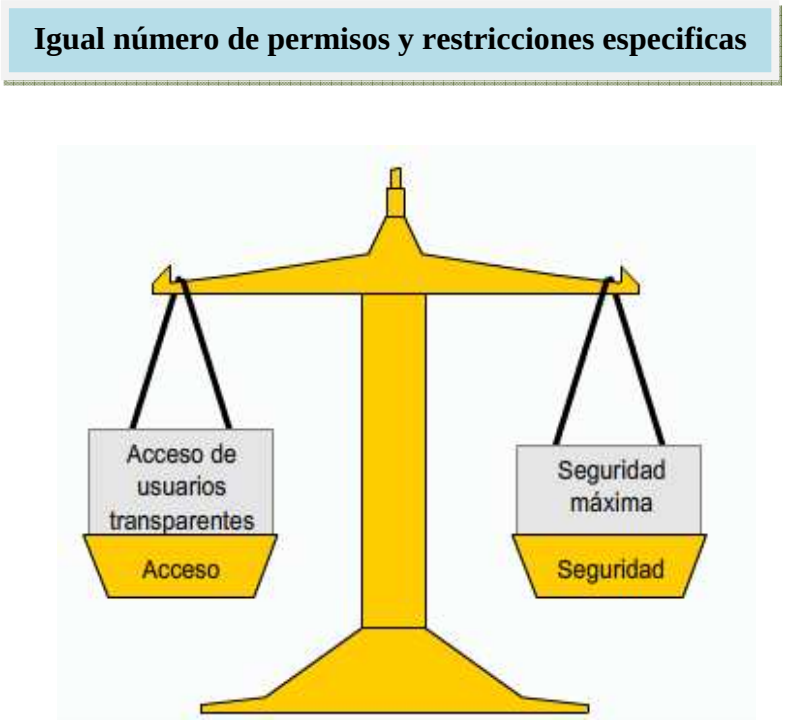


Figura 2.25 Acceso Restrictivo [4]

2.8.3 ACCESO CERRADO

Un modelo de seguridad cerrado es muy difícil llevar a cabo, ya que en este plan se trata de implementar todas las medidas de seguridad. Los Administradores configuran el hardware y software existente con la máxima seguridad, además se adquiere hardware más costoso y soluciones de software como los firewall, VPN, IDS, y servidores de identidad.

Este modelo asume que los recursos protegidos son muy importantes, todos los usuarios no son confiables y las amenazas son frecuentes. El acceso de los

usuarios es muy difícil. Los Administradores de la red requieren de mayores habilidades y más tiempo para realizar su trabajo.

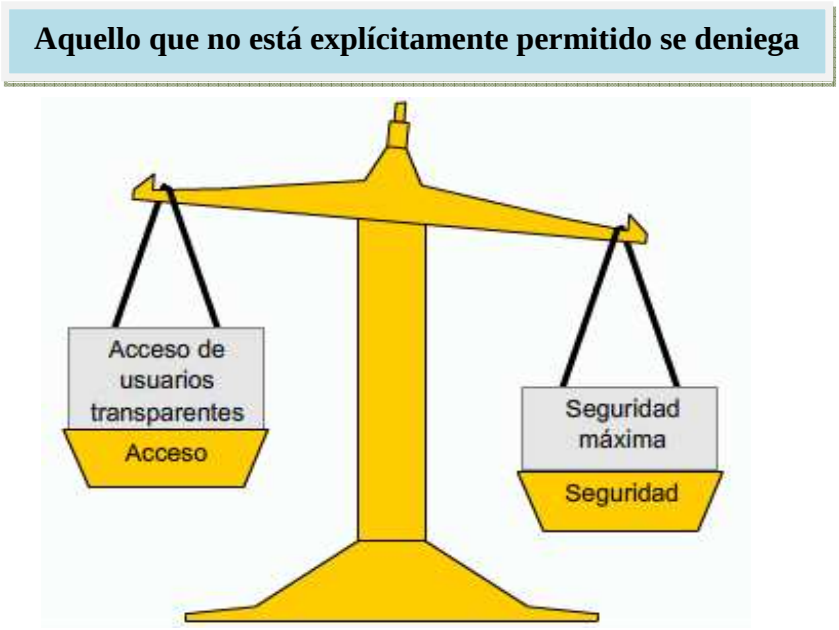


Figura 2.26 Acceso Cerrado [4]

CAPÍTULO 3

DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

3.1 INTRODUCCIÓN

Una vez que se ha estudiado la red actual de Petroindustrial con sus respectivas Refinerías, como también conceptos y tecnologías de seguridad de redes de información, se tiene claro el panorama para proceder al Diseño del Sistema Integral de Seguridad para esta empresa.

3.2 PLANTEAMIENTO DEL PROBLEMA

La situación actual, de la red de Petroindustrial en cuanto a temas de seguridad y funcionalidad, es la siguiente:

Uno de los principales problemas que se suscita en esta empresa es la falta de monitoreo y control exhaustivo del acceso a internet, razón por la cual se provoca el uso inadecuado e innecesario de muchos recursos, que no contribuyen con el trabajo productivo de los empleados y pueden comprometer a diferentes dispositivos e incluso a información confidencial.

El tener libre acceso al mundo de internet es un gran riesgo para los datos que maneja la empresa ya que fácilmente se puede exponer al sistema a diferentes

amenazas como virus, spyware, spam, etc, lo cual puede provocar serias amenazas no sólo a la seguridad sino también a la disponibilidad, privacidad, confidencialidad e integridad de la información.

Petroindustrial posee diferentes proveedores del servicio de internet para los diferentes distritos, lo que aumenta el número de brechas de posibles ataques a la red de datos de la empresa.

El crecimiento de las redes inalámbricas es otro aspecto que puede generar problemas en la seguridad de la red de Petroindustrial, puesto que personas no autorizadas podrían ingresar por estas sin mayor dificultad.

Debido al crecimiento de la red en el último año existe mayor demanda de direcciones IP en las diferentes VLANs que se encuentran creadas en todos y cada uno de los distritos, generándose así dominios de broadcast, que reducen la eficiencia de la red.

También resulta preocupante la situación que enfrentaría esta red ante el daño de los principales dispositivos que constituyen el núcleo del funcionamiento de este sistema, como son los switches de core[1], los servidores y los diferentes dispositivos de conectividad; es decir aquellos que juegan un papel importante para la correcta funcionalidad del sistema.

3.3 PLANTEAMIENTO DE SOLUCIONES

Para solucionar los problemas presentes en la red de Petroindustrial se plantean las siguientes soluciones:

Desarrollar e implementar Políticas de Seguridad que permitan proteger a la red en contra de las diferentes amenazas de seguridad, para de esta manera prever posibles incidentes y reaccionar de forma eficiente ante los mismos.

---

[1] **Switches de Core:** Son dispositivos centrales en las redes LAN de Matriz y de los Distritos de Petroindustrial.

Implementar los módulos de seguridad necesarios como Firewall, Antivirus, IDS, IPS, VPN, entre otros, que permitan la ejecución de las políticas de seguridad.

Establecer un plan de monitoreo que permita el análisis de los diferentes eventos suscitados en el sistema, y manejar un software que permita la administración adecuada de los activos que maneja el Área de Sistemas.

Desarrollar un plan que permita la adecuada organización y asignación de los diferentes dispositivos, direcciones IP; para lo cual se contempla la reasignación de VLANs, que permitan separar los diferentes departamentos y así balancear el tráfico de las redes que se encuentran saturadas.

Todas estas actividades serán hechas con miras al desarrollo tecnológico y crecimiento de la red.

3.4 POLÍTICAS DE SEGURIDAD

La naturaleza dinámica y distribución de las redes modernas, combinada con las amenazas contra las aplicaciones y datos, está cambiando el enfoque de la seguridad perimetral. El nuevo punto de enfoque se basa en controlar el acceso individual a los equipos y usuarios, cumpliendo las políticas y regulaciones. Se debe inspeccionar no solo el número de paquetes, si no la información sensible y valiosa que estos transmiten. Para controlar el mal uso y abuso se requiere de medidas granulares como seguridad endpoint[1], control de acceso a la red basado en identidad y análisis del comportamiento de la red. Las mejores prácticas para el desarrollo de seguridad perimetral son validas, pero deben ser desplegadas con mayor fuerza y convertirse en una parte integral de la red.

En la implementación de políticas de seguridad perimetral se debe tener presente la aplicación de mejores prácticas sobre los puntos mencionados a continuación.

[1] **Seguridad endpoint**: concepto de seguridad de información que especifica que cada dispositivo endpoint es responsable de su propia seguridad.

3.4.1 MANEJO UNIFICADO DE AMENAZAS

La mayoría de los Firewalls configurados para seguridad perimetral, se han convertido en aplicaciones que administran unificadamente las amenazas (UTM, Unified Threat Management) multi-funcionales. Estas plataformas de seguridad todo en uno pueden administrar el firewall, prevención contra intrusos y servicios de antivirus, todo en un solo paquete. Algunos proveen servicios extras como anti-spyware y capacidades de VPN con SPAM y filtros web.

Un UTM no es un producto, pero es un acercamiento contemporáneo a las sofisticadas batallas contra las amenazas. La aplicación adecuada de un UTM requiere una planificación adecuada, como empezar considerando donde los servicios de seguridad deberían ser consolidados totalmente en la red, así como los beneficios e impactos de hacerlo.

Se debe aplicar un UTM dentro de límites de confianza internos elaborando una defensa por capas para distribuir la carga de trabajo y reforzar las políticas con el incremento de granularidad. Por ejemplo, filtros preventivos para evitar la intrusión en la red deberían ser aplicados en el perímetro externo, respaldado por una inspección detallada del correo conforme los mensajes entran al pool de servidores.

3.4.2 CORTAFUEGOS

Conforme los cortafuegos crecen en robustez, los atacantes ajustan sus tácticas. En estos días las amenazas más peligrosas están encaminadas hacia vulnerabilidades específicas de los protocolos, defectos en el código y errores en configuración. Los cortafuegos pueden ayudar a disminuir este tipo de ataques.

Muchos Cortafuegos UTM realizan inspecciones rigurosas de paquetes y técnicas de Proxy para examinar el contenido malicioso en los mensajes, virus y spyware, pero siguen siendo dispositivos de propósito general.

3.4.3 SSL VPN

En una defensa perimetral, las VPNs pueden conectar de manera segura, sucursales y laptops certificadas a la red corporativa, pero socios B2B[1] y mano de obra móvil han borrado los límites de confianza.
Para empleados que usan una PC en casa y proveedores que tienen acceso limitado, los antiguos clientes VPN vía acceso remoto son insuficientes e imprácticos. De acuerdo a una investigación de Forrester[2], las VPNs basadas en Secured Sockets Layer (SSL) se han convertido en la opción para acceso remoto, usadas por el 44% de las empresas Americanas.

Usando VPNs SSL, el negocio puede extenderse al menos en acceso básico a dispositivos no administrados, tales como PCs de casa y laptops de consultores. Debido a que estos puertos pueden estar desprotegidos o comprometidos, las VPNs SSL ofrecen las siguientes características:

1. Escaneo de endpoint. Usan agentes para examinar el estado del dispositivo, tal como determinar si el antivirus está actualizado y corriendo.
2. Controles Granulares. Basados en los resultados del escaneo y la autenticación de la identidad del usuario, pueden restringir usuarios para recursos específicos autorizados y acciones. Por ejemplo, cuando un empleado ingresa su PC al centro de negocios, puede tener acceso read-only para su correo y nada más. Además, para limitar el acceso la VPN SSL detendría al empleado de dejar cookies o archivos temporales. Pero cuando se conecta desde la laptop de la compañía, puede registrar información en la base de datos y guardar archivos.

3.4.4 SEGURIDAD END POINT

Los dispositivos usados para acceso remoto no son los únicos endpoints que pueden y deberían ser protegidos. Los antivirus se han convertido en un estándar

---

[1] **B2B**: Business to business, se refiere a la comunicación de comercio electrónico entre empresas.
[2] **Forrester**: Empresa dedicada a la investigación tecnológica la misma que brinda asesoramiento a diferentes organizaciones a nivel mundial.

en las laptops y PCs, por lo que se establece esta política de seguridad para la empresa.

Conforme la conectividad de internet ha demandado más crecimiento, firewalls personales se han vuelto lo suficientemente importantes como para ser incluidos en los sistemas operativos.

Estas medidas son un punto de partida para detener las más diversas y hostiles amenazas. A diferencia de UTM, las suites de seguridad endpoint son programas que corren en cada host. Los endpoint de clase empresarial van más allá usando un servidor para centralizar la instalación y mantener los clientes.

La seguridad endpoint endurece las PCs contra ataques a información privilegiada y protege laptops conectadas a redes públicas. Juntos UTM y seguridad endpoint son mucho más efectivas que separadas.

3.4.5 CONTROL DE ACCESO A LA RED

La seguridad endpoint es efectiva solo cuando se refuerza. Sin supervisión de IT, los usuarios fallan al mantenerse con parches de software y actualización de firmas.

El control de acceso a la red (NAC Network Access Control) ha emergido como un refuerzo a la seguridad endpoint y la entrega de un acceso adecuado para cada usuario.

NAC autoriza los recursos basado en la combinación de autenticación de identidad de usuario, estado de la seguridad endpoint, y políticas.

NAC hace un refuerzo en las decisiones de acceso al tiempo de conexión de red. No solo la política puede ser reforzada en los endpoints, NAC puede ayudar a documentar el cumplimiento del uso de la red.

3.4.6 MONITOREO DE SEGURIDAD DE RED

Aplicar NAC es parte de la batalla, el resto es mantener vigilado el tráfico y amenazas que sobrepasan esas defensas o se originan dentro de la red.

Los sistemas IDS complementan a Firewalls perimetrales observando pasivamente el trafico y alertando a los administradores de ataques.

IDS han abierto la vía a los IPS, los cuales no solo detectan sino que previenen intrusiones. UTM es una forma de desplegar IPS.

IPS pueden ser aplicadas a ambientes Wireless usando controladores LAN o con el despliegue de servidores IPS y sensores.

IPS compara el tráfico monitoreado para firmas y reglas de protocolos. Cuando las violaciones son descubiertas, IPS puede tomar acciones basadas en políticas para romper la conexión o poner en cuarentena el recurso.

IPS se enfoca en el tráfico en límites de seguridad, detrás del firewall, o detrás del concentrador VPN, en el punto donde el host Wireless se conecta.

Las compañías actualmente deben estar prevenidas sobre la actividad dentro de la red. Una interacción entre los servidores y el host puede ser evidencia de ataque, aun cuando se usen protocolos permitidos.

Finalmente, en redes grandes la seguridad tiene un crecimiento tan complejo que los administradores no pueden analizar efectivamente los logs y alertas sin asistencia.

3.5 ANÁLISIS TÉCNICO

En base al estudio de la red de Petroindustrial se ha llegado a identificar los siguientes requerimientos técnicos para los diferentes equipos de seguridad que se va a utilizar en el presente diseño.

Primeramente, la solución a cotizar deben soportar mínimo el siguiente número de usuarios en cada Unidad Operativa de Petroindustrial.

- Matriz-Quito 200 Usuarios
- REE 350 Usuarios
- RLL 250 Usuarios
- CIS 150 Usuarios

La solución completa de seguridad, tanto en Hardware como en Software, debe permitir:

- Establecer un Sistema de Seguridad Perimetral.
- Establecer un Sistema de Monitoreo, Estadísticas y Alertas para:
  Monitorear redes LAN en las cuatro Unidades Operativas de la Filial.
  Monitorear la red WAN de Petroindustrial.
  Monitorear el Hardware de red: Routers, Switchs.
  Monitorear Hardware de Servidores.
  Monitorear Sistemas Operativos: Windows, Linux y AS/400.
  Monitorear al proveedor de servicio de Internet o ISP.
  Establecer gráficas y alertas en tiempo real.
- Establecer un Sistema de Proxificación completo para la navegación en Internet, que utilice criterios variados y simultáneos como: MAC Address, IP, usuario, horarios, entre otros.
- Establecer un sistema que permita analizar los contenidos que viajan dentro la red en correos electrónicos, chats y paquetes en general de la red.
- Establecer un Sistema que permita optimizar el ancho de banda que posee la empresa en Matriz y en cada uno de los distritos.

- Establecer un Sistema que permita investigar todo el equipamiento de hardware IP de la empresa.

3.5.1 REQUERIMIENTOS MÍNIMOS DE SERVIDORES

El diseño del sistema de seguridad debe contar con un servidor por distrito, el mismo que, de acuerdo a las necesidades de la empresa en cuanto a la cantidad de usuarios, se indica en la Tabla 3.1 donde se listan las características más relevantes.

Servidores HP Proliant DL380 G5 Xeon Quad Core E5430, Base Rack Server	
Procesador	
Descripción del procesador	Intel Quad-Core Xeon E5430 / 2,66GHz (Quad-Core)
Cantidad de procesadores	2
Velocidad del procesador	2,66GHz
Tipo de procesador	Intel Quad-Core Xeon E5430 / 2,66GHz (Quad-Core)
“Front Side Bus” del procesador	1066MHz
Memoria	
Memoria estándar	4GB 4x1GB of 2-way interleaved PC2-5300 Fully Buffered DIMMs DDR2-667 (at 533MHz on processors witch 1066 MHZ FSB) with Advanced ECC,mirrored and online spare memory capabilities.
Características de protección de memoria	Advanced ECC,mirrored and online spare memory capabilities.
Descripción de Cache	12MB (2 x 6MB (6MB per core pair))
Almacenamiento	
Capacidad de Almacenamiento	4 HP Hard Disk: 146GB 10K SAS 2,5 Hard Drive
Conexión de almacenamiento etándar	Hot Plug 2.5- inch SAS

Tabla 3.1 Características del Servidor HP Proliant DL 380 G5

El Software para seguridad Perimetral y Administración de redes LAN y WAN debe tener las siguientes características:

- Debe contar con una consola Universal e Integrada de Administración, que sea 100% Web Enable, que permita administrar la solución remota y localmente; es decir todo el software ofertado deben ser módulos de una misma solución.
- La solución debe estar completamente integrada al Directorio Activo (Active Directory) de Petroindustrial instalado en servidores Windows 2003.
- En cada Distrito de Petroindustrial debe tener los siguientes servidores:

  Firewall

  IPS

  IDS

  Servidores de Monitoreo

  Servidores de Proxificación

  Servidores Inspectores de Contenido

  Optimizadores de Ancho de Banda

3.5.2 REQUERIMIENTOS MÍNIMOS DE LOS SERVIDORES FIREWALL

- Integrable con Microsoft Active Directory de Windows 2003 Server que posee Petroindustrial.
- Capacidad de procesamiento en Firewall de al menos 1Gbps y de al menos 400 Mbps en tráfico VPN.
- Memoria 2048MB
- 6 Interfaces de Red 10/100 Mbps
- Alta disponibilidad en modo active/active con balanceo de carga.
- Alta disponibilidad active/active y active/standby
- 400000 Sesiones concurrentes.
- 15000 Sesiones nuevas por segundo.
- Filtrado de paquetes a nivel 3 y 4
- QoS en IPv4 a nivel 3 y 4
- Inspección de paquetes a nivel Stateful
- Detección y rechazo de al menos los siguientes tipos de ataques: suplantación IP, inundación SYN, ping de la muerte, ataques de negación de servicio, paquetes malformados, fragmentos IP.

- Capacidad de hacer filtraje dentro de puertos TCP conocidos (por ejemplo el puerto 80 de http), aplicaciones potencialmente peligrosas como P2P (KaZaA, Gnutella) o Messengers (Yahoo, MSN), aun cuando se haga “tunneling” de estos simulando ser trafico legítimo del puerto (ejemplo: tráfico legitimo HTTP).
- Rechazar códigos Active X o Java.
- 150 Vlans (802.1q)
- Doble pila IPv4 e IPv6
- NAT/PAT dinámico y estático
- NAT transversal para H.323
- 1000 conexiones IPSec VPN
- Software para clientes VPN, al menos 1000
- 100 conexiones simultáneas SSL VPN
- Soportes de algoritmo de cifrado simétrico: 256 bits AES, DES, 3DES
- Compatibilidad con equipos IPS e IDS
- Capacidad de interoperar automáticamente con el inspector de contenido, y el hardware de red de Petroindustrial para realizar acciones proactivas sobre ataques detectados.
- Generación de alarmas por medio de snmp, syslog, consola
- Análisis de logs del sistema en tiempo real.
- Administración gráfica, remota y segura, desde la consola web y el servidor de administración.
- Reportes detallados y configurables de acuerdo a las necesidades de la Empresa.

3.5.3 REQUERIMIENTOS MÍNIMOS DE SERVIDORES IPS

- Performance 500Mbps
- 5000 nuevas conexiones TCP por segundo
- 4 interfaces de red 10/100/1000 y 1 interfaz 10/100 Mbps
- Capacidad de interoperar automáticamente con el Firewall, el inspector de Contenido, y el Hardware de red de Petroindustrial para realizar acciones proactivas sobre ataques detectados.
- Interfaz de línea de comando consola

- Administración gráfica, dinámica y segura, desde la consola y el servidor de administración.
- Administración basada en GUI integrada.
- Sistema de prevención y control de incidentes: detectar y detener ataques maliciosos, detectar y detener virus, detectar y detener Worms.
- Detección de tráfico IPv6 malicioso.
- Inspección y análisis de ataques en capa 2 a capa 7.
- Monitoreo de puertos SPAN.
- 150 Vlans (802.1q).
- Desfragmentación de IP.
- Reensamblaje del flujo TCP.
- Identificación y análisis de protocolos (TCP/IP, ICMP, SMTP, HTTP, DNS, RPC, NETBIOS, NNTP, GRE)
- Protección avanzada contra evasiones al IPS.
- Implementación de políticas en tiempo real.
- Protección contra ataques de día cero.
- Detección de tráfico anómalo: anomalías en protocolos y anomalías en aplicaciones.
- Detección y Prevención de ataques de Denegación de servicio.
- Prevención de intrusos en tiempo real.
- Reconocimiento de patrones stateful
- Capacidad de acciones de respuesta contra ataques (Clear, Reset, Drop)
- Actualización del sistema operativo
- Detección y rechazo de al menos los siguientes tipos de ataques: Suplantación IP, inundación SYN, ping de la muerte, rastreo de puertos, ataques de negación de servicio, paquetes malformados, fragmentos IP, gusanos.
- Generación de alarmas por medio de Email, snmp, syslog, consola.
- Reportes detallados y configurables de acuerdo a las necesidades de la empresa.

3.5.4 REQUERIMIENTOS MÍNIMOS DE SERVIDORES IDS

- El Sistema operativo debe estar basado en Linux o VxWorks.

- Debe proveer simultaneidad en la administración de ancho de banda y bloquear tipos de tráfico específicos como tráfico peer-to-peer.
- El equipo debe bloquear tráfico en una sola dirección o en ambas direcciones y debe operar en ambientes de red con enrutamiento asimétrico.
- En cuanto al filtrado del tráfico, el equipo debe bloquearlo, alertar sobre ataques y anomalías, administrar el ancho de banda, generar bitácoras o dejar pasar al mismo en función de cada uno de los sistemas de filtrado de la unidad.
- Capacidad para administrar el ancho de banda por aplicación o servicio que se defina por el administrador del sistema. La administración de este tráfico podrá implementarse por IP, TCP, UDP, ICMP, protocolo o por dirección IP.
- El sistema debe bloquear propagación de gusanos y virus previniendo la infección de otros equipos y consumo de ancho de banda en los segmentos que protege.
- El equipo debe proveer mínimo protección contra DoS y DDoS (Inundación por conexiones por segundo o por conexiones establecidas).

3.5.5 REQUERIMIENTOS MÍNIMOS DE SERVIDORES DE MONITOREO Y ESTADÍSTICAS

- Debe ser integrable con Microsoft Active Directory de Windows 2003 Server que tiene Petroindustrial.
- Monitoreo de Factores de Sistema Operativo; Linux, Windows, AS/400
- Generación de Estadísticas.
- Generación de mensajería SNMTP con alertas de caídas.
- Generación de gráficas de Análisis ON-LINE.
- Capacidad de recolección de datos vía SNMP.
- Elaboración de gráficas de utilización de recursos.
- Presentación de Resultados mediante interfaces HTML

3.5.6 REQUERIMIENTOS MÍNIMOS DE SERVIDORES DE CONTENIDO

- Debe ser integrable con Microsoft Active Directory de Windows 2003 Server que tiene Petroindustrial.
- Capacidad de integración con los firewalls escogidos para el diseño.
- 2 interfaces 10/100/1000Mbps
- Capacidad de procesamiento de al menos 400Mbps
- Operación en tiempo real
- Administración gráfica remota y segura, desde la consola y el servidor de administración.
- Envío de alarmas por medio de snmp, syslog, consola.
- Reportes detallados a nivel de IP.

3.5.7 REQUERIMIENTOS MÍNIMOS DE LOS OPTIMIZADORES DE ANCHO DE BANDA

- Debe ser integrable con Microsoft Active Directory de Windows 2003 Server que tiene Petroindustrial.
- Throughput[1] mínimo de 45Mbs con capacidad de crecimiento a 100Mbps full dúplex.
- Número de políticas soportadas: 1024
- Número de Hosts IP: 20000
- Número de Flujos IP: 150000
- 2 Interfaces de Red 10/100/1000Mbps
- Puerto de consola
- Capacidad de inspección de contenidos y clasificar tráfico tales como: P2P, Web, Mail, Juegos, Messenger, VoIP, Protocolos de Multimedia, Protocolos de Seguridad.
- Control de ancho de banda por aplicación.
- Control de ancho de banda por sesión.
- Asignación dinámica de ancho de banda por aplicación, usuario o cliente.

[1] **Throughput:** Volumen de información que fluye a través de un sistema.

- Control de flujo en sesiones TCP y UDP.
- Generación de políticas para regular el tráfico.
- Protección contra ataques tipo DoS.
- Capacidad de clasificar el tráfico por aplicación.
- Monitoreo gráfico en tiempo real del tráfico que está circulando por el dispositivo.
- Administración gráfica, remota y segura, desde la consola y el servidor de administración.
- Envío de alarmas por medio de email, snmp, syslog.
- Monitoreo de la utilización de ancho de banda.
- Generación de reportes detallados y gerenciales del comportamiento de las aplicaciones que pasa por el equipo.

3.5.8 REQUERIMIENTOS MÍNIMOS DE SERVIDORES DE PROXIFICACIÓN

- Debe ser integrable con Microsoft Active Directory de Windows 2003 Server que tiene Petroindustrial.
- Gestor de reportes y estadísticas para la navegación.
- Control de acceso por factores múltiples y simultáneos como: grupos, usuarios, IP, Mac Address, Equipo, entre otros.

3.6 ANÁLISIS DE EQUIPO

Una vez que se ha estudiado los requerimientos de Petroindustrial en materia de requerimientos técnicos, se procede a escoger el equipo que brinde las mejores ventajas para poder desarrollar un sistema de seguridad acorde con las peticiones de esta empresa.

Los equipos a analizar han sido escogidos por su prestigio en el ámbito de seguridad de redes, de los cuales se analizarán los siguientes: Juniper y Linserver UCNC (Universal Corporate Networking Center).

3.6.1 DETALLE DEL EQUIPO JUNIPER [16]

La solución de seguridad de alto rendimiento de Juniper Networks puede atenuar los riesgos asociados a conectar y ejecutar servicios de red y aplicaciones empresariales críticas.

Juniper Networks, ha desarrollado una gama de dispositivos de gestión unificada de amenazas (Unified Threat Management o UTM) que combinan las mejores tecnologías de seguridad de redes como: cortafuegos, detección y prevención de intrusiones, VPN IPSec, así como antivirus, antispam y filtrado web. UTM no sólo simplifica notablemente la implementación, también la administración y supervisión se unifican en un mismo proceso, con el objetivo de crear redes grandes, rápidas, inteligentes y seguras.

Para el presente diseño se pretende utilizar el equipo Secure Service Gateway (SSG) 550 de Juniper Networks para reforzar la protección frente a amenazas dirigidas contra equipos de escritorio y servidores mediante el bloqueo en el perímetro mismo de las amenazas contenidas en mensajes.

El SSG 550 es un dispositivo de seguridad diseñado específicamente para proporcionar elevados niveles de rendimiento, seguridad y conectividad LAN/WAN. El tráfico que pasa por el SSG 550 está protegido contra gusanos, software espía, troyanos y software malévolo gracias a un completo conjunto de funciones de seguridad, como cortafuegos con inspección de estado, VPN IPSec, IPS, antivirus (incluyendo anti-spyware, anti-adware y anti-phishing), antispam y filtrado web.

El SSG 550 protege la red contra ataques a nivel de red, aplicación y contenido, al tiempo que maximizan el rendimiento. Entre los múltiples mecanismos de administración se encuentran la completa interfaz de línea de comandos (CLI), la interfaz de usuario web WebUI y el sistema centralizado de administración NetScreen-Security Manager, que facilitan la implementación rápida al tiempo que

minimizan los costos operativos. Las principales características y ventajas de este equipo son:

- Soluciones basadas en dispositivos que permiten reducir el capital de inversión y los costos operativos y, por consiguiente, el costo total de propiedad.
- Funciones de seguridad aceleradas por hardware, que proporcionan un rendimiento predecible y fiable para disponer de una red altamente fiable, disponible y segura.
- Rica funcionalidad de seguridad que ejecuta control de accesos y autenticación de usuarios al tiempo que protege contra ataques a nivel de red y de aplicación.
- Integración de las mejores funciones UTM existentes, para proteger sucursales y puestos de trabajo remotos contra gusanos, troyanos, virus y otros programas malévolos.
- Dispositivos modulares y con factor de forma fijo para garantizar la redundancia a nivel de hardware y proporcionar opciones de E/S para WAN y LAN con el fin de maximizar la flexibilidad y rentabilizar la inversión.

El elemento controlador de los dispositivos de Juniper Networks es ScreenOS, un sistema operativo con funciones específicas de seguridad que incorpora un potente motor de enrutamiento y un robusto conjunto de aplicaciones de seguridad. Para maximizar el rendimiento en seguridad, ScreenOS está íntimamente integrado en una plataforma de hardware diseñada específicamente. Características y ventajas clave de ScreenOS:

- Sistema operativo en tiempo real diseñado específicamente para seguridad, con potentes funciones de enrutamiento y aplicaciones de seguridad clave, integradas íntimamente para eliminar las vulnerabilidades propias de los sistemas operativos de uso general.
- Aceleración por hardware cuidadosamente diseñada para la ejecución de funciones de seguridad que consumen mucha potencia de cálculo, sin comprometer el rendimiento.

- Instalación fácil incluso en los entornos de red más complejos, con un amplio conjunto de funciones de fiabilidad, resistencia, enrutamiento de red e implementación.
- Protección de la red con un conjunto integrado de aplicaciones de seguridad, incluyendo: cortafuegos con inspección de estado, sistema de prevención de intrusiones (IPS), mitigación de ataques de denegación de servicio (DoS), VPN IPSec, antivirus, anti-phishing, anti-spam, antispyware y filtrado web (con algunas aplicaciones disponibles en un conjunto limitado de productos).

3.6.2 DETALLE DE EQUIPO LINSERVER UCNC [17]

Linserver UCNC Universal Corporate Networking Center es un producto creado para reemplazar todo el equipamiento de software y de hardware que para el Middleware[1] posee una organización. Y cuyo objetivo principal es eliminar el licenciamiento de productos para el funcionamiento de una red corporativa.

Esta plataforma incluye la migración del sistema de correo a uno más moderno y mucho más sofisticado que incluye el uso del LDAP[2], capas de seguridad, capas de filtrado y que incluye políticas de administración de correo electrónico personalizadas y de mayor flexibilidad entregando propiedades a todo el conjunto de usuarios de manera fácil y sencilla como a su vez de manera puntual a un usuario y a grupos de usuarios definidos por el administrador.

Lo más importante es que este producto es modular y puede instalarse completo como de manera separada módulo por módulo, por ejemplo puede adecuarse a servidores de Correo como Exchange o Lotus Domino, sin interferir en su configuración original. Las aplicaciones principales que ofrece este Servidor se observa a continuación:

---

[1] **Middleware:** es un software de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas.

[2] **LDAP:** (Lightweight Directory Access Protocol), (Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

3.6.2.1 Sistema Operativo

La implementación de la nueva topología y servidores se basará en plataforma Open Source específicamente Enterprise Linux Red Hat Advanced Server 4.4. Plataforma que junto a Suse dentro de los Enterprise Linux a nivel mundial son de las más reconocidas por su confiabilidad dentro de sistemas de misión crítica como Bases de Datos DB2 y Oracle, SQL, servidores de comunicaciones corporativos, servidores de procesamiento de datos especiales, etc. Esta plataforma permite obtener servicios de alto manejo tráfico como Mail, DNS, Web, Webmail, AntiSpam, Antivirus de Gateway, Proxy, VPN, IDS, IPS y Firewall. Es decir sobre esta plataforma se puede instalar y configurar cualquier servicio de Red que se requiera en el futuro, de manera fácil y sencilla.

3.6.2.2 Servidor de Balanceo de Carga

Linserver UCNC puede balancear el tráfico de una red que viaja sobre TCP/IP logrando balancear aplicativos, servidores de aplicación, carga hacia routers y switchs. Acoplandose a VLANs estructuradas, o en su defecto formando VLANs con tráfico controlado y balanceado. Se puede balancear carga y distribuir carga en varios servidores tanto para aplicativos como para tráfico.

3.6.2.3 Virtualización de Servidores

Linserver UCNC genera un servidor de Virtualización para Servidores tanto en Windows con Linux o Unix, una poderosa herramienta para aprovechar al máximo el equipamiento de Hardware que posee una compañía. Permite correr en un mismo equipo varios servidores de plataformas de sistemas operativos diferentes y hasta no compatibles como Linux y Windows.

3.6.2.4 Servidor de Monitoreo

Permite generar estadísticas de todo lo que monitoree, en tiempo real e histórico.

El servidor de monitoreo ofrece al Cliente, un análisis completo de los servicios de red, como son: Ancho de Banda por canal y monitoreo al proveedor, servicios Web, Mail, POP, DHCP, Bases de datos, control de inventarios entre otros, actuando con alarmas en tiempo real en el momento que se quede fuera de servicio cada uno de ellos. Además permite analizar el tipo de tráfico que atraviesa en cada segmento de red, facilitando tareas de búsqueda de posibles errores, así como de ataques.

3.6.2.5 Establecimiento de VPN y túneles privados

Se puede establecer una VPN con cualquier cliente en el Internet poniendo a disposición recurso de la red local de manera segura. También se puede establecer túneles privados y seguros con cualquier otra red, necesitando solamente poseer un enlace al menos 64kbps.

3.6.2.6 Acceso Remoto Seguro

El servidor estará listo para poder acceder a él desde cualquier lugar del mundo a través de una consola bajo el protocolo SSH, llevando su información cifrada de un lugar a otro, monitorear, configurar y administrar el servidor. Podrá transferir, de igual forma, archivos de cualquier tamaño y para cualquier fin.

3.6.2.7 Inventarios de la Red

Gracias a los modernos sistemas de Open LDAP se puede mostrar un completo inventario de equipos, dispositivos y usuarios en tiempo real.

3.6.2.8 Servidor Firewall

El servidor de firewall garantiza en un 99% que los ataques que se sufran de manera externa serán contenidos y repelidos; pero lo más importante alertará al administrador de estos ataques, para tomar acciones de monitoreo.

Permite implementar reglas de filtrado de paquetes diseñadas, exclusivamente para el cliente, de acuerdo a la nueva topología de seguridad. Permite hacer redirección de puertos a servidores internos para balancear la carga dependiendo el servicio.

Permite mantener un control total sobre los protocolos y puertos que se estén ejecutando sobre la red del cliente. Permite manejar políticas, por default, DROP tanto en INPUT, OUTPUT y FORWARD hacia las diferentes subredes. Soporta una velocidad de procesamiento de paquetes de hasta 155Mbps. Permite dar acceso exclusivo por servicio, protocolo, aplicación a todos los usuarios.

3.6.2.9 Servidor Web

Se ofrece un servidor Web seguro para proyectar al cliente a aplicaciones presentes o futuras que necesiten acceso desde el Internet y hacia la misma, convergiendo en una Intranet, para facilitar los servicios que presente.

El tráfico será cifrado en ambas vías, soportando aplicaciones PHP y JSP dependiendo de la necesidad del cliente, y sobre todo sin tener un costo económico adicional por licenciamiento.

3.6.2.10 Servidor Mail

Debido a los problemas que se encuentran actualmente en el Internet sobre los correos no deseados, virus, límite de espacio en disco, spam, etc., se implementará un servidor SMTP e IMAP basado en Cyrus con capacidad de procesamiento sobre los 100 mil correos diarios, límite de espacio controlado para usuarios, límite de envío de correos, manejo de las colas remotas y/o locales.

Es posible implementar control de archivos por extensiones y contenido. Evitando que ciertas personas, grupos de usuarios o toda la base de usuarios; cualquiera que sea el caso tengan restricciones de envío de archivos de música, video, ejecutables de Windows, etc.

3.6.2.11 Control de Navegación por usuarios

Se puede controlar la navegación por los siguientes ítems:

- Horarios.
- Direccionamiento IP.
- Direcciones MAC.
- Acceso y Bloqueo a páginas Permitidas y/o Prohibidas.
- Número de conexiones.
- ACLs.
- Bloqueo de descargas de archivos puntuales (mp3, mov, etc.). Esto permite controlar que el ancho de banda sea usado para los fines que son destinados. Evita descargas de música, archivos de video, etc.
- Validación por Claves.

En este ítem se debe tener en cuenta las reglas y políticas de navegación pueden ser usadas de manera que se combinen las características es decir por ejemplo: En horario de 8h00 – 20h00 los usuarios del grupo operador 1, no pueden realizar descargas de ningún tipo, fuera de él pueden realizar descargas a 128kbps, excepto de archivos de música y videos.

3.6.2.12 Reportes de Navegación

Una vez implementado los controles evidentes, se pueden producir excepciones a las reglas debido a un abuso de confianza con el personal, niveles de acceso, entre otros, el servidor contará con reportes de la navegación para continuar el bloqueo pero de manera específica, sacar reportes diarios, semanales y mensuales para estadísticas, etc.

3.6.2.13 Sistema automático de detección y prevención de intrusos (IDS/IPS)

El sistema automático de detección de intrusos sirve para detectar ataques de cualquier segmento de red en tiempo real, mostrando estadísticas completas de los mismos, así como alertas. Además permite personalizar el acceso por

usuarios y que el sistema tome decisiones en tiempo real para bloquear cualquier tipo de ataque que se haya detectado.

3.6.2.14 Políticas Corporativas de Seguridad LAN (Dominio de Red)

El servidor permite manejar un dominio de red seguro y confiable bajo los mismos criterios que los productos de Microsoft Windows 2000 y 2003 Server lo hacen, salvo que de manera gratuita y mucho más ligera. Esto permite usar el mismo usuario y clave en el mail y en el dominio de red.

Permite crear todas las políticas de seguridad interna como:

- Grupos de Trabajo por Departamento.
- Asociar un IP determinado a cada máquina de la red.
- Identificando por MAC Address a las máquinas de la red.
- Eliminar los archivos compartidos de las máquinas de la red.
- Utilizar un File Server de Directorios en el Servidor con control de usuarios y permisos. Ejemplo: Directorio Contabilidad.
- Accesos a máquinas de la red con permisos y seguridad de Auditoría.
- Monitorear desde la matriz cualquier máquina de la red, incluso en las sucursales.
- Manejar remotamente cualquier máquina de la red, incluso en las sucursales.
- Alertar al administrador si existe violaciones de seguridad de un funcionario en específico a las políticas de calidad.
- Guardar configuraciones predeterminadas para los usuarios del dominio en el servidor.

3.6.3 ELECCIÓN DEL EQUIPO A UTILIZAR

Una vez que se conoce las bondades que presentan estos dos dispositivos se procede a elegir el más óptimo para el presente diseño, en base a una comparación de sus principales características, las mismas que se son evaluadas de acuerdo a los requerimientos de la empresa.

En la Tabla 3.2 se puede observar una comparación de los equipos citados, de esta forma se hace una comparación de las características ofrecidas por cada uno de estos, para de esta forma analizarlos y escoger el equipo que está más acorde a las necesidades planteadas para Petroindustrial.

DESCRIPCIÓN DE CARACTERÍSTICAS DE EQUIPOS	(SSG) 550 de Juniper Networks	LINSERVER UCNC
Capacidad para trabajar con el número de usuarios requeridos.	SI CUMPLE	SI CUMPLE
Capacidad para establecer un Sistema de Seguridad Perimetral.	SI CUMPLE	SI CUMPLE
Capacidad para Establecer un Sistema de Monitoreo, Estadísticas y Alertas.	SI CUMPLE	SI CUMPLE
Capacidad para Establecer un Sistema de Proxificación completo para la navegación en Internet, que utilice criterios variados y simultáneos como: MAC Address, IP, usuario, horarios, entre otros.	SI CUMPLE	SI CUMPLE
Capacidad para Establecer un sistema que permita analizar los contenidos que viajan dentro de una red en correos electrónicos, chats y paquetes en general de la red.	SI CUMPLE	SI CUMPLE
Capacidad para Establecer un Sistema que permita optimizar el ancho de banda que posee la empresa en Matriz y en cada uno de los distritos.	SI CUMPLE	SI CUMPLE
Capacidad para Establecer un Sistema que permita investigar todo el equipamiento de hardware IP de la empresa.	NO CUMPLE	SI CUMPLE
2 Procesadores Intel Quad-Core Xeon E5430 / 2,66GHz (Quad-Core)	SI CUMPLE	SI CUMPLE
Velocidad del procesador 2,66GHz	SI CUMPLE	SI CUMPLE
“Front Side Bus” del procesador 1066MHz	NO CUMPLE	SI CUMPLE
Memoria estándar de 4GB 4x1GB of 2-way interleaved PC2-5300 Fully Buffered DIMMs DDR2-667 (at 533MHz on processors witch 1066 MHZ FSB) with Advanced ECC,mirrored and online spare memory capabilities.	NO CUMPLE	SI CUMPLE
Descripción de Cache 12MB (2 x 6MB (6MB per core pair))	NO CUMPLE	SI CUMPLE
Capacidad de Almacenamiento de 4 HP Hard Disk: 146GB 10K SAS 2,5 Hard Drive	NO CUMPLE	SI CUMPLE
Debe contar con una consola Universal e Integrada de Administración, que sea 100% Web Enable, que permita administrar la solución remota y localmente; es decir todo el software ofertado deben ser módulos de una misma solución.	SI CUMPLE	SI CUMPLE
La solución debe estar completamente integrada al Directorio Activo (Active Directory) de Petroindustrial instalado en servidores Windows 2003.	SI CUMPLE	SI CUMPLE
En cada Distrito de Petroindustrial debe tener los siguientes servidores: Firewall IPS IDS Servidores de Monitoreo Servidores de Proxificación Optimizadores de Ancho de Banda	SI CUMPLE	SI CUMPLE

REQUERIMIENTOS MÍNIMOS DEL SERVIDOR FIREWALL		
Integrable con Microsoft Active Directory de Windows 2003 Server que posee Petroindustrial.	SI CUMPLE	SI CUMPLE
Capacidad de procesamiento en Firewall de al menos 1Gbps y de al menos 400 Mbps en tráfico VPN.	SI CUMPLE	SI CUMPLE
Memoria 2048MB	SI CUMPLE	SI CUMPLE
6 Interfaces de Red 10/100 Mbps	NO CUMPLE	SI CUMPLE
Alta disponibilidad en modo active/active con balanceo de carga.	NO CUMPLE	SI CUMPLE
Detección y rechazo de al menos los siguientes tipos de ataques: suplantación IP, inundación SYN, ping de la muerte, ataques de negación de servicio, paquetes malformados, fragmentos IP.	SI CUMPLE	SI CUMPLE
Capacidad de hacer filtraje dentro de puertos TCP conocidos (por ejemplo el puerto 80 de http), aplicaciones potencialmente peligrosas como P2P (KaZaA, Gnutella) o Messengers (Yahoo, MSN), aun cuando se haga "tunneling" de estos simulando ser trafico legítimo del puerto (ejemplo: tráfico legitimo HTTP).	SI CUMPLE	SI CUMPLE
150 Vlans (802.1q)	NO CUMPLE	SI CUMPLE
1000 conexiones IPSec VPN	NO CUMPLE	SI CUMPLE
Compatibilidad con equipos IPS e IDS	SI CUMPLE	SI CUMPLE
Capacidad de interoperar automáticamente con el inspector de contenido, y el hardware de red de Petroindustrial para realizar acciones proactivas sobre ataques detectados.	SI CUMPLE	SI CUMPLE
Generación de alarmas por medio de snmp, syslog, consola	NO CUMPLE	SI CUMPLE
Administración gráfica, remota y segura, desde la consola web y el servidor de administración.	SI CUMPLE	SI CUMPLE
Reportes detallados y configurables de acuerdo a las necesidades de la Empresa.	SI CUMPLE	SI CUMPLE
REQUERIMIENTOS MÍNIMOS DE SERVIDORES IPS		
Performance 500Mbps.	SI CUMPLE	SI CUMPLE
5000 nuevas conexiones TCP por segundo.	NO CUMPLE	SI CUMPLE
4 interfaces de red 10/100/1000 y 1 interfaz 10/100 Mbps	SI CUMPLE	SI CUMPLE
Capacidad de interoperar automáticamente con el Firewall, el inspector de Contenido, y el Hardware de red de Petroindustrial para realizar acciones proactivas sobre ataques detectados.	SI CUMPLE	SI CUMPLE
Interfaz de línea de comando consola Administración gráfica, dinámica y segura, desde la consola y el servidor de administración.	SI CUMPLE	SI CUMPLE
Sistema de prevención y control de incidentes: detectar y detener ataques maliciosos, detectar y detener virus, detectar y detener Worms.	SI CUMPLE	SI CUMPLE
Inspección y análisis de ataques en capa 2 a capa 7.	NO CUMPLE	SI CUMPLE
Identificación y análisis de protocolos (TCP/IP, ICMP, SMTP, HTTP, DNS, RPC, NETBIOS, NNTP, GRE)	SI CUMPLE	SI CUMPLE
Implementación de políticas en tiempo real.	NO CUMPLE	SI CUMPLE
Generación de alarmas por medio de Email, snmp, syslog, consola.	SI CUMPLE	SI CUMPLE

REQUERIMIENTOS MÍNIMOS DE SERVIDORES IDS		
El Sistema operativo debe estar basado en Linux o VxWorks.	NO CUMPLE	SI CUMPLE
Debe proveer simultaneidad en la administración de ancho de banda y bloquear tipos de tráfico específicos como tráfico peer-to-peer.	SI CUMPLE	SI CUMPLE
El equipo debe bloquear tráfico en una sola dirección o en ambas direcciones y debe operar en ambientes de red con enrutamiento asimétrico.	SI CUMPLE	SI CUMPLE
En cuanto al filtrado del tráfico, el equipo debe bloquearlo, alertar sobre ataques y anomalías, administrar el ancho de banda, generar bitácoras o dejar pasar al mismo en función de cada uno de los sistemas de filtrado de la unidad.	SI CUMPLE	SI CUMPLE
Capacidad para administrar el ancho de banda por aplicación o servicio que se defina por el administrador del sistema. La administración de este tráfico podrá implementarse por IP, TCP, UDP, ICMP, protocolo o por dirección IP.	SI CUMPLE	SI CUMPLE
El sistema debe bloquear propagación de gusanos y virus previniendo la infección de otros equipos y consumo de ancho de banda en los segmentos que protege.	SI CUMPLE	SI CUMPLE
El equipo debe proveer mínimo protección contra DoS y DDoS (Inundación por conexiones por segundo o por conexiones establecidas).	SI CUMPLE	SI CUMPLE
REQUERIMIENTOS MÍNIMOS DE SERVIDORES DE MONITOREO Y ESTADÍSTICAS		
Debe ser integrable con Microsoft Active Directory de Windows 2003 Server que tiene Petroindustrial.	SI CUMPLE	SI CUMPLE
Monitoreo de Factores de Sistema Operativo; Linux, Windows, AS/400	SI CUMPLE	SI CUMPLE
Generación de Estadísticas.	SI CUMPLE	SI CUMPLE
Generación de mensajería SNMTP con alertas de caídas.	SI CUMPLE	SI CUMPLE
Generación de gráficas de Análisis ON-LINE.	SI CUMPLE	SI CUMPLE
Capacidad de recolección de datos vía SNMP	SI CUMPLE	SI CUMPLE
Elaboración de gráficas de utilización de recursos.	SI CUMPLE	SI CUMPLE
Presentación de Resultados mediante interfaces HTML	SI CUMPLE	SI CUMPLE
REQUERIMIENTOS MÍNIMOS DE SERVIDORES DE CONTENIDO		
Debe ser integrable con Microsoft Active Directory de Windows 2003 Server que tiene Petroindustrial.	SI CUMPLE	SI CUMPLE
2 interfaces 10/100/1000Mbps	SI CUMPLE	SI CUMPLE
Capacidad de procesamiento de al menos 400Mbps	SI CUMPLE	SI CUMPLE
Operación en tiempo real	SI CUMPLE	SI CUMPLE
Administración gráfica remota y segura, desde la consola y el servidor de administración.	SI CUMPLE	SI CUMPLE
Envío de alarmas por medio de snmp, syslog, consola.	SI CUMPLE	SI CUMPLE
Reportes detallados a nivel de IP.	SI CUMPLE	SI CUMPLE

REQUERIMIENTOS MÍNIMOS DE LOS OPTIMIZADORES DE ANCHO DE BANDA		
Debe ser integrable con Microsoft Active Directory de Windows 2003 Server que tiene Petroindustrial.	SI CUMPLE	SI CUMPLE
Throughput mínimo de 45Mbs con capacidad de crecimiento a 100Mbps full dúplex.	SI CUMPLE	SI CUMPLE
Número de políticas soportadas: 1024	SI CUMPLE	SI CUMPLE
Número de Hosts IP: 20000	SI CUMPLE	SI CUMPLE
Número de Flujos IP: 150000	SI CUMPLE	SI CUMPLE
2 Interfaces de Red 10/100/1000Mbps	SI CUMPLE	SI CUMPLE
Puerto de consola	SI CUMPLE	SI CUMPLE
Capacidad de inspección de contenidos y clasificar tráfico tales como: P2P, Web, Mail, Juegos, Messenger, VoIP, Protocolos de Multimedia, Protocolos de Seguridad.	SI CUMPLE	SI CUMPLE
Control de ancho de banda por aplicación.	SI CUMPLE	SI CUMPLE
Control de ancho de banda por sesión.	SI CUMPLE	SI CUMPLE
Asignación dinámica de ancho de banda por aplicación, usuario o cliente.	SI CUMPLE	SI CUMPLE
Control de flujo en sesiones TCP y UDP	SI CUMPLE	SI CUMPLE
Generación de políticas para regular el tráfico.	SI CUMPLE	SI CUMPLE
Protección contra ataques tipo DoS.	SI CUMPLE	SI CUMPLE
Capacidad de clasificar el tráfico por aplicación.	SI CUMPLE	SI CUMPLE
Monitoreo gráfico en tiempo real del tráfico que está circulando por el dispositivo.	SI CUMPLE	SI CUMPLE
Administración gráfica, remota y segura, desde la consola y el servidor de administración.	SI CUMPLE	SI CUMPLE
Envío de alarmas por medio de email, snmp, syslog.	SI CUMPLE	SI CUMPLE
Monitoreo de la utilización de ancho de banda.	SI CUMPLE	SI CUMPLE
Generación de reportes detallados y gerenciales del comportamiento de las aplicaciones que pasa por el equipo.	SI CUMPLE	SI CUMPLE
REQUERIMIENTOS MÍNIMOS DE SERVIDORES DE PROXIFICACIÓN		
Debe ser integrable con Microsoft Active Directory de Windows 2003 Server que tiene Petroindustrial.	SI CUMPLE	SI CUMPLE
Gestor de reportes y estadísticas para la navegación.	SI CUMPLE	SI CUMPLE
Control de acceso por factores múltiples y simultáneos como: grupos, usuarios, IP, Mac Address, Equipo, entre otros.	SI CUMPLE	SI CUMPLE

Tabla 3.2 Comparación de características de Equipos a elegir

3.7 CRITERIOS DE DISEÑO

Una vez que se conoce las bondades que presentan estos dos dispositivos estudiados se escoge el segundo: Linserver UCNC ya que presenta las

características más afines con los requerimientos estudiados para un mejor sistema de seguridad. Además, por tener un sistema operativo basado en Linux se torna más robusto y manejable para poder brindar seguridad a Petroindustrial, y de esta manera conseguir un sistema integrable y que sea capaz de ser modificado en el momento que la empresa presente cambios tecnológicos en el transcurso del tiempo.

De igual forma cuenta con características fundamentales que requiere la empresa como son:

Puertos necesarios para conectar los dispositivos que pertenecen a la red interna, manejar una DMZ (zona desmilitarizada) para los servicios públicos que ofrece el sistema y un acceso para Internet de alta capacidad.

La capacidad de operación de 10/100/1000 Mbps debido a la existencia de dispositivos que trabajan con estas capacidades de transmisión.

Un dispositivo de control e inspección completa integrado por un Firewall, Motor de detección y prevención de intrusiones (IDS/IPS), Motor de Antivirus, Mecanismos para el Filtrado de contenido y Filtrado Web, Tecnología para la creación de redes privadas virtuales (VPN) mediante el uso de tecnologías difundidas (IPSec, SSL, etc) con características de encriptación de alta velocidad y capacidad para creación de VLANs para segmentación de redes por protección y balanceo de carga de tráfico.

El sistema operativo cuenta con una fortaleza tanto en aspectos de seguridad como funcionalidad, ya que es un sistema operativo propietario el cual presenta alta capacidad de procesamiento.

Cuenta con la tecnología necesaria para administrar conexiones inalámbricas con las respectivas consideraciones de seguridad y funcionalidad.

3.8 DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL

Una vez que se tienen todos los elementos necesarios para realizar el diseño del sistema de seguridad operacional para mejorar la protección de las redes LAN y WAN de Petroindustrial, se procede con el proyecto.

Tomando en consideración el estudio en detalle en el Capítulo 1, la infraestructura que posee Petroindustrial Matriz como también de sus distritos, Refinería Estatal Esmeraldas, Refinería La Libertad y Complejo Industrial Shushufindi, se ve la necesidad de instalar un servidor que brinde las tecnologías necesarias para una adecuada protección de la red, tales como: Firewall, Proxy, IPS, IDS, Segmentador de Ancho de Banda, para cada una de las Refinerías ya que estas cuentan con su proveedor independiente de Internet y es administrado por su respectivo departamento de sistemas de cada área operativa.

Para mayor facilidad se va a dividir el Diseño del Sistema de Seguridad Perimetral en cuatro unidades operativas, es decir, Matriz y los tres distritos.

El Diseño del Sistema de Seguridad Perimetral será integrable con la infraestructura actual de Petroindustrial, razón por la cual se deberá tener conocimiento suficiente de la estructura de la red, de las unidades operativas, así como de sus constantes cambios para de esta manera conseguir una completa integridad del proyecto y tener una red protegida que brinde las garantías necesarias a los usuarios.

Además se pretende contratar los servicios de comunicación para datos a la empresa Global Crossing ya que ofrece un mejor enlace de 2Mbps, para que ésta sea la encargada de la comunicación entre Petroindustrial Matriz y sus diferentes distritos con lo que el enlace que proporciona Petrocomercial, que es de 640Kbps quede como backup en caso de fallar la nueva conexión. Este importante aspecto se considerará para realizar el diseño del sistema de seguridad perimetral.

3.8.1 DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL DE PETROINDUSTRIAL MATRIZ

3.8.1.1 Requerimientos de Diseño

Para realizar el Diseño del Sistema de Seguridad Perimetral en Petroindustrial Matriz se requiere definir una nueva VLAN para seguridad perimetral, además nuevas rutas para re direccionar el tráfico hacia las Unidades Operativas de los diferentes distritos como también a la red de Petroecuador y a Internet. También se necesita definir las políticas de tráfico que se van a controlar en el firewall, clasificadas de la siguiente manera, tráfico hacia las Unidades Operativas, hacia la red de Petroecuador y hacia Internet. A su vez el nuevo enlace con Global Crossing obliga a realizar una restructuración a nivel de la red WAN.

3.8.1.2 Soluciones para el Diseño

Para el Diseño del Sistema de Seguridad Perimetral se utilizará un Servidor Linserver UCNC como infraestructura de Core, el mismo que cuenta con un Firewall Integrado, Proxy, IDS, IPS, Segmentador de Ancho de Banda y un Sistema de Monitoreo.

Linserver UCNC permite configurar una consola centralizada para gestionar y administrar a todos los elementos de la red. Esto implica que la gestión de todo el sistema se haría desde la ciudad de Quito. La caída de los enlaces hacia los diferentes puntos no afectaría el funcionamiento de la infraestructura, únicamente su configuración. En caso de decidir implementar un esquema de gestión independiente para cada punto, la única diferencia es que el respaldo de configuraciones del sistema se lo administra en cada unidad y puede ser manejado remotamente desde cualquier punto de la red de Petroindustrial, que tenga acceso y permisos para este fin.

El Servidor Linserver UCNC cuenta con 6 puertos G-Ethernet los cuales se distribuirán en las siguientes zonas:

- Zona 1: G-Ethernet 1 - Internet
- Zona 2: G-Ethernet 2 - Red Wan Petroindustrial Matriz
- Zona 3: G-Ethernet 3 - Red Lan Petroindustrial Matriz
- Zona 4: G-Ethernet 4 - DMZ (Zona Desmilitarizada)
- Zona 5 y 6: G-Ethernet 5 y 6 – Libres para futuras necesidades

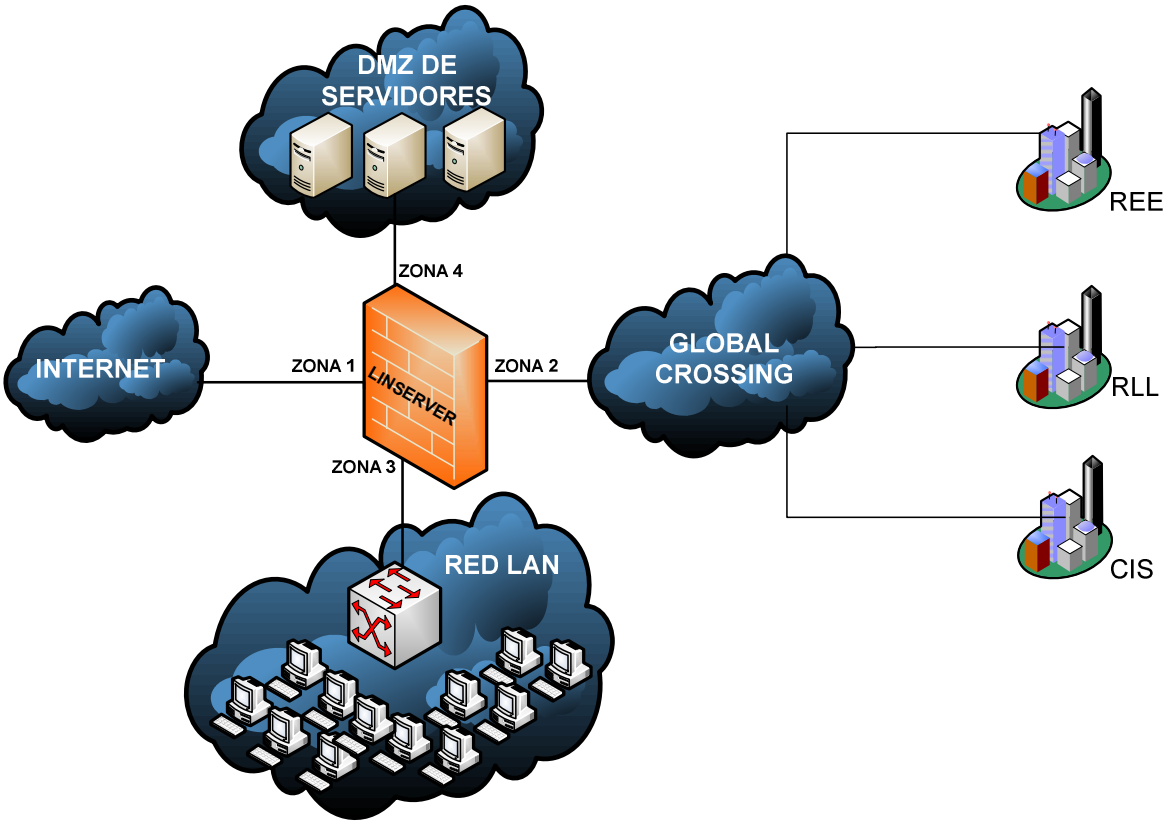


Figura 3.1 Definición de Zonas del Sistema de Seguridad Integral de Petroindustrial-Matriz

De acuerdo al estudio realizado en la Matriz de Petroindustrial se definirá el tráfico hacia la DMZ de servidores de la siguiente manera:

- Tráfico entrante desde la red Wan hacia Petroindustrial-Matriz.
- Tráfico saliente hacia la red Wan desde Petroindustrial-Matriz.
- Tráfico entrante desde redes externas tales como: Petroecuador, Dirección Nacional de Hidrocarburos, Banco Central del Ecuador, Petrocomercial.

- Tráfico saliente hacia redes externas tales como: Petroecuador, Dirección Nacional de Hidrocarburos, Banco Central del Ecuador, Petrocomercial.
- Tráfico hacia la nube de Internet.

Debido a que no se tienen claramente definidos los requerimientos de conectividad en la red; es decir, todos los servicios y políticas de tráfico que funcionan actualmente en el esquema general de Petroindustrial, se toman las siguientes decisiones técnicas:

- Mantener el tráfico abierto completamente hacia y desde la zona de servidores de Petroindustrial-Matriz.
- Todos los equipos de la red de Petroindustrial-Matriz pueden acceder hacia cualquier servidor AS400 a nivel nacional.
- Todos los equipos de la red WAN de Petroindustrial pueden acceder libremente hacia los servidores AS400 de Matriz.
- Los servidores AS400 tienen libre acceso hacia cualquier equipo en la red a nivel nacional.

La definición de políticas relacionadas al tráfico hacia internet se cumple de acuerdo al esquema denominado “Tráfico hacia la nube de Internet”, resumido de la siguiente forma:

- Todos los equipos de la Red de Petroindustrial-Matriz saldrán hacia Internet por medio de un proxy, el cual responde al puerto 3128 únicamente en la RED LAN en la dirección IP 172.30.16.23.
- El único equipo que puede conectarse hacia los puertos de navegación y FTP es el Servidor FIREWALL por medio de la ZONA de Internet.
- El Firewall no recibe ningún tipo de tráfico desde Internet.
- El Firewall está en condiciones de recibir y reenviar tráfico que se origina en Internet hacia equipos de la red local de acuerdo a las necesidades que se presenten.

3.8.1.3 Definición de Direccionamiento IP a aplicarse en Linserver UCNC y Routers de Frontera

Debido a que se crearon diferentes zonas al incorporar el servidor firewall a la red, se debe reestructurar el direccionamiento IP de los equipos de frontera como también de las correspondientes interfaces del Servidor Linserver.

A continuación se detalla el esquema que se propone para el presente diseño de seguridad perimetral en lo que se refiere a direccionamiento IP.

Para la Zona 1, que corresponde a Internet, se tiene la dirección 190.216.222.105/29 que pertenece al router del proveedor y para el servidor Linserver UCNC la dirección 190.216.222.107/29.

Para la Zona 2, que corresponde al enlace de datos a través de Global Crossing se asigna la dirección 172.30.117.4/26 para el router de Global y la dirección 172.30.117.1/26 para la interfaz correspondiente al servidor Linserver UCNC. En este caso la dirección 172.30.117.4 es virtual ya que se utiliza el protocolo HSRP (Hot Standby Router Protocol) entre dos routers de Global Crossing.

HSRP es un protocolo propietario de cisco que permite el despliegue de routers redundantes tolerantes a fallos en la red. Este protocolo evita la existencia de puntos de fallos únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers. El funcionamiento del protocolo HSRP es el siguiente: Se crea un grupo (también conocido por el término Clúster) de routers en el que uno de ellos actúa como maestro, enrutando el tráfico, y los demás actúa como respaldo a la espera que se produzca un fallo en el maestro. HSRP es un protocolo que actúa en la capa 3 del modelo OSI administrando las direcciones virtuales que identifican al router que actúa como maestro en un momento dado.

Para la Zona 3, que corresponde a la conexión de la red LAN de Petroindustrial Matriz, se conserva la dirección 172.30.16.19/24 que corresponde a la puerta de enlace de la Vlan de servidores en el Switch Cisco 6509E y se asigna la dirección 172.30.16.23/24 para la interfaz correspondiente al servidor Linserver UCNC.

Para la Zona 4, que corresponde a la DMZ de servidores, se asigna la dirección 172.30.15.1/24 y para la interfaz del servidor Linserver UCNC se asigna la dirección 172.30.15.2/24

Con estas nuevas direcciones asignadas se garantiza que el presente diseño del sistema de seguridad perimetral sea integrable con la actual infraestructura que cuenta Petroindustrial.

3.8.1.4 Rutas a Implementarse en Linserver UCNC

De acuerdo al estudio realizado de la red de Petroindustrial se establece en la Tabla 3.1 las rutas que se deben crear en el Servidor Linserver UCNC para que se integre en forma satisfactoria a la infraestructura existente en la Matriz de Petroindustrial.

RED DESTINO	GATEWAY	MÁSCARA	INTERFAZ	DESCRIPCIÓN
190.216.222.104	0.0.0.0	255.255.255.248	ETH1	Acceso Internet
0.0.0.0	190.216.222.105	0.0.0.0	ETH1	Acceso a Internet
172.30.117.0	0.0.0.0	255.255.255.192	ETH2	Acceso Perimetral
172.30.20.0	172.30.117.4	255.255.255.0	ETH2	Acceso a Red LAN-REE
172.30.21.0	172.30.117.4	255.255.255.0	ETH2	Acceso a Red LAN-REE
172.30.22.0	172.30.117.4	255.255.255.128	ETH2	Acceso a Red LAN-REE
172.30.22.128	172.30.117.4	255.255.255.128	ETH2	Acceso a Red LAN-REE
172.30.23.0	172.30.117.4	255.255.255.224	ETH2	Acceso a Red LAN-REE
172.30.23.32	172.30.117.4	255.255.255.224	ETH2	Acceso a Red LAN-REE
172.30.23.64	172.30.117.4	255.255.255.224	ETH2	Acceso a Red LAN-REE
172.30.23.96	172.30.117.4	255.255.255.224	ETH2	Acceso a Red LAN-REE
172.30.23.128	172.30.117.4	255.255.255.224	ETH2	Acceso a Red LAN-REE
172.30.23.160	172.30.117.4	255.255.255.224	ETH2	Acceso a Red LAN-REE

RED DESTINO	GATEWAY	MÁSCARA	INTERFAZ	DESCRIPCIÓN
172.30.23.192	172.30.117.4	255.255.255.224	ETH2	Acceso a Red LAN-REE
172.30.23.224	172.30.117.4	255.255.255.224	ETH2	Acceso a Red LAN-REE
172.30.24.0	172.30.117.4	255.255.255.0	ETH2	Acceso a Red LAN-CIS
172.30.25.0	172.30.117.4	255.255.255.240	ETH2	Acceso a Red LAN-CIS
172.30.25.16	172.30.117.4	255.255.255.240	ETH2	Acceso a Red LAN-CIS
172.30.25.32	172.30.117.4	255.255.255.240	ETH2	Acceso a Red LAN-CIS
172.30.25.48	172.30.117.4	255.255.255.240	ETH2	Acceso a Red LAN-CIS
172.30.25.64	172.30.117.4	255.255.255.240	ETH2	Acceso a Red LAN-CIS
172.30.25.80	172.30.117.4	255.255.255.240	ETH2	Acceso a Red LAN-CIS
172.30.25.96	172.30.117.4	255.255.255.240	ETH2	Acceso a Red LAN-CIS
172.30.25.112	172.30.117.4	255.255.255.240	ETH2	Acceso a Red LAN-CIS
172.30.25.128	172.30.117.4	255.255.255.224	ETH2	Acceso a Red LAN-CIS
172.30.25.160	172.30.117.4	255.255.255.224	ETH2	Acceso a Red LAN-CIS
172.30.28.0	172.30.117.4	255.255.255.0	ETH2	Acceso a Red LAN-RLL
172.30.29.0	172.30.117.4	255.255.255.192	ETH2	Acceso a Red LAN-RLL
172.30.29.64	172.30.117.4	255.255.255.192	ETH2	Acceso a Red LAN-RLL
172.30.29.128	172.30.117.4	255.255.255.192	ETH2	Acceso a Red LAN-RLL
172.30.29.192	172.30.117.4	255.255.255.192	ETH2	Acceso a Red LAN-RLL
172.30.30.0	172.30.117.4	255.255.255.192	ETH2	Acceso a Red LAN-RLL
172.30.30.64	172.30.117.4	255.255.255.192	ETH2	Acceso a Red LAN-RLL
172.30.30.128	172.30.117.4	255.255.255.192	ETH2	Acceso a Red LAN-RLL
172.30.30.192	172.30.117.4	255.255.255.192	ETH2	Acceso a Red LAN-RLL
172.30.31.0	172.30.117.4	255.255.255.192	ETH2	Acceso a Red LAN-RLL
172.30.31.64	172.30.117.4	255.255.255.192	ETH2	Acceso a Red LAN-RLL
172.30.31.128	172.30.117.4	255.255.255.192	ETH2	Acceso a Red LAN-RLL
172.19.226.7	172.30.16.19	255.255.255.255	ETH3	Acceso a Petroecuador
172.19.230.0	172.30.16.19	255.255.255.0	ETH3	Acceso a Petroecuador
172.30.16.0	0.0.0.0	255.255.255.0	ETH3	Acceso a Red LAN-PIN
172.30.17.0	172.30.16.19	255.255.255.192	ETH3	Acceso a Red LAN-PIN
172.30.17.64	172.30.16.19	255.255.255.192	ETH3	Acceso a Red LAN-PIN
172.30.17.128	172.30.16.19	255.255.255.192	ETH3	Acceso a Red LAN-PIN
172.30.17.192	172.30.16.19	255.255.255.192	ETH3	Acceso a Red LAN-PIN
172.30.18.0	172.30.16.19	255.255.255.192	ETH3	Acceso a Red LAN-PIN
172.30.18.64	172.30.16.19	255.255.255.192	ETH3	Acceso a Red LAN-PIN
172.30.18.128	172.30.16.19	255.255.255.192	ETH3	Acceso a Red LAN-PIN
172.30.18.192	172.30.16.19	255.255.255.192	ETH3	Acceso a Red LAN-PIN
172.30.15.0	0.0.0.0	255.255.255.0	ETH4	Acceso DMZ

Tabla 3.3 Rutas a implementarse en el Servidor LINSERVER UCNC de Matriz

3.8.1.5 Políticas de Tráfico a Controlar con Linserver UCNC

Las Políticas de Tráfico son uno de los aspectos más importantes en el momento de una futura implementación del Sistema de Seguridad Perimetral, ya que de esto depende el grado de protección que tendrá la red de Petroindustrial, es por esto, que dichas políticas deberán ser creadas y validadas una vez que se implemente el Sistema.

A continuación se detalla las políticas básicas que se deben crear en el sistema, basados en el estudio de los principales requerimientos y del tráfico más importante que se genera en esta Empresa.

- El tráfico hacia la DMZ que pertenece a servidores permanecerá abierta completamente ya que se necesita muchas aplicaciones a los diferentes distritos como también a Petroecuador, Banco Central, Dirección Nacional de Hidrocarburos.
- El tráfico hacia Internet se lo hará por medio del Proxy, el mismo que sirve para que ciertos equipos puedan acceder directamente al servicio y para que el equipo con WEBSecurity pueda acceder como servidor Caching. Con esto se consigue una migración progresiva al nuevo Sistema de Seguridad y sin dejar por completo la infraestructura anterior, para que de esta forma se pueda alcanzar una integración adecuada del Sistema.
- Acceso al terminal server libre entre redes de servidores para que todas las Unidades Operativas de Petroindustrial tengan todas las facilidades para la transferencia de información importante que se maneja en la empresa.
- Acceso libre de las unidades operativas al servidor de Cisco Works el mismo que sirve para una mejor administración y conocimiento del estado de la red.
- Acceso libre desde Petroecuador a los servidores AS400.
- Tráfico SNMP libre entre todas las unidades operativas.

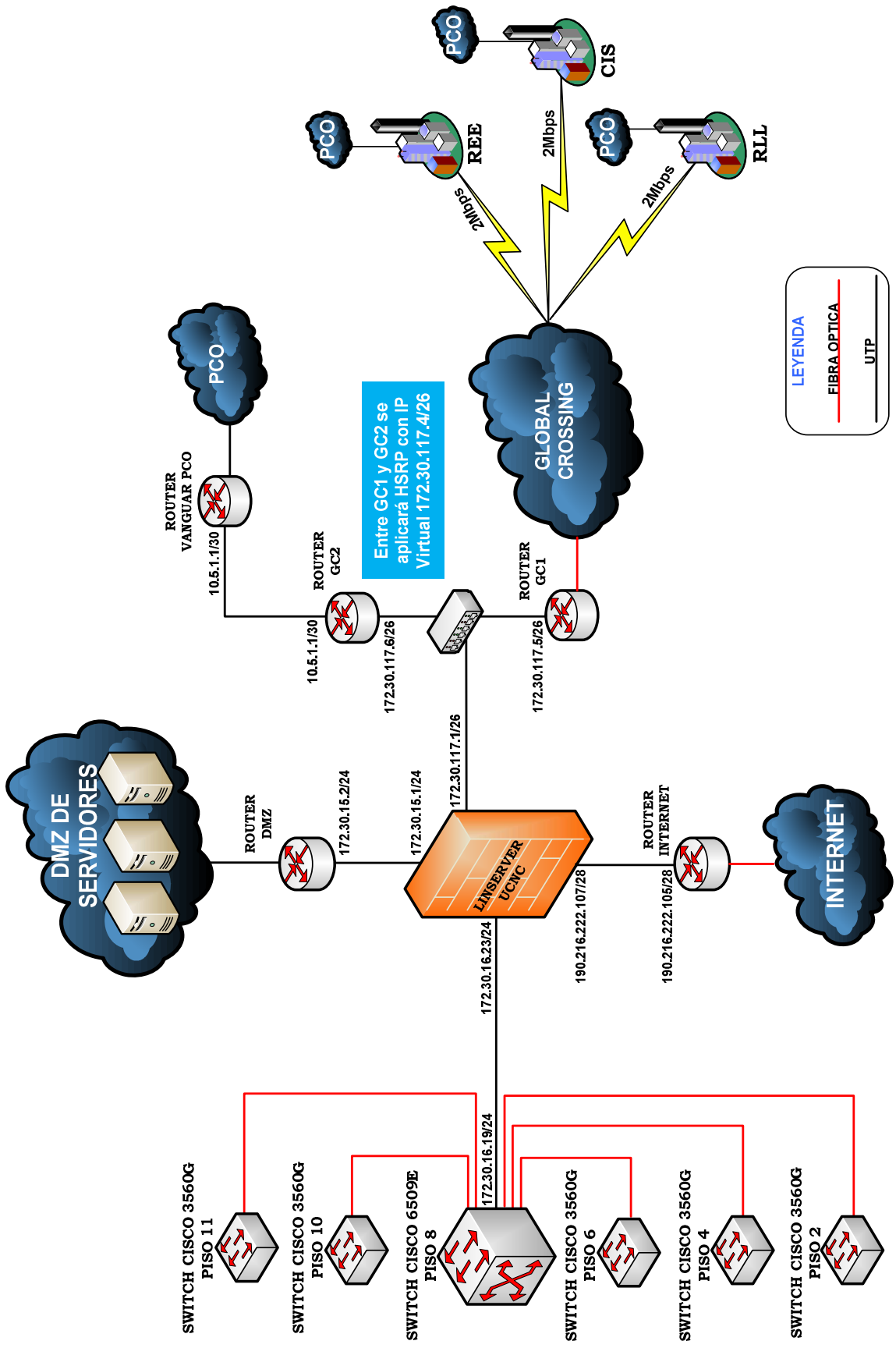


Figura 3.2 Esquema del Sistema de Seguridad Integral de Petroindustrial-Matriz

3.8.2 DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL DE REFINERÍA ESTATAL DE ESMERALDAS

3.8.2.1 Requerimientos del Diseño

Para realizar el Diseño del Sistema de Seguridad Perimetral en la Refinería Estatal de Esmeraldas se requiere definir una nueva VLAN para seguridad perimetral. Además, añadir nuevas rutas y políticas para re direccionar y controlar el tráfico hacia Matriz y hacia el proveedor de Internet. De igual forma, el nuevo enlace con Global Crossing obliga a realizar una restructuración a nivel de la red WAN.

3.8.2.2 Soluciones para el Diseño

Se debe crear una nueva VLAN en el Switch de core, que se la designará como Red Perimetral REE la misma que se la ubicará en la red 172.30.118.0/26 y esta será completamente independiente y sin ninguna relación a las que se encuentran creadas.

Para el Diseño del Sistema de Seguridad Perimetral se utilizará un Servidor LINSERVER UCNC como infraestructura de Core, de las mismas características que en Matriz.

Este Servidor estará administrado por personal de esta Unidad Operativa, el mismo que cuenta con las siguientes Zonas:

- Zona 1: G-Ethernet 1 - Internet
- Zona 2: G-Ethernet 2 - Red Wan REE
- Zona 3: G-Ethernet 3 - Red Lan REE
- Zona 4, 5 y 6: G-Ethernet 4, 5 y 6 – Libres para futuras necesidades

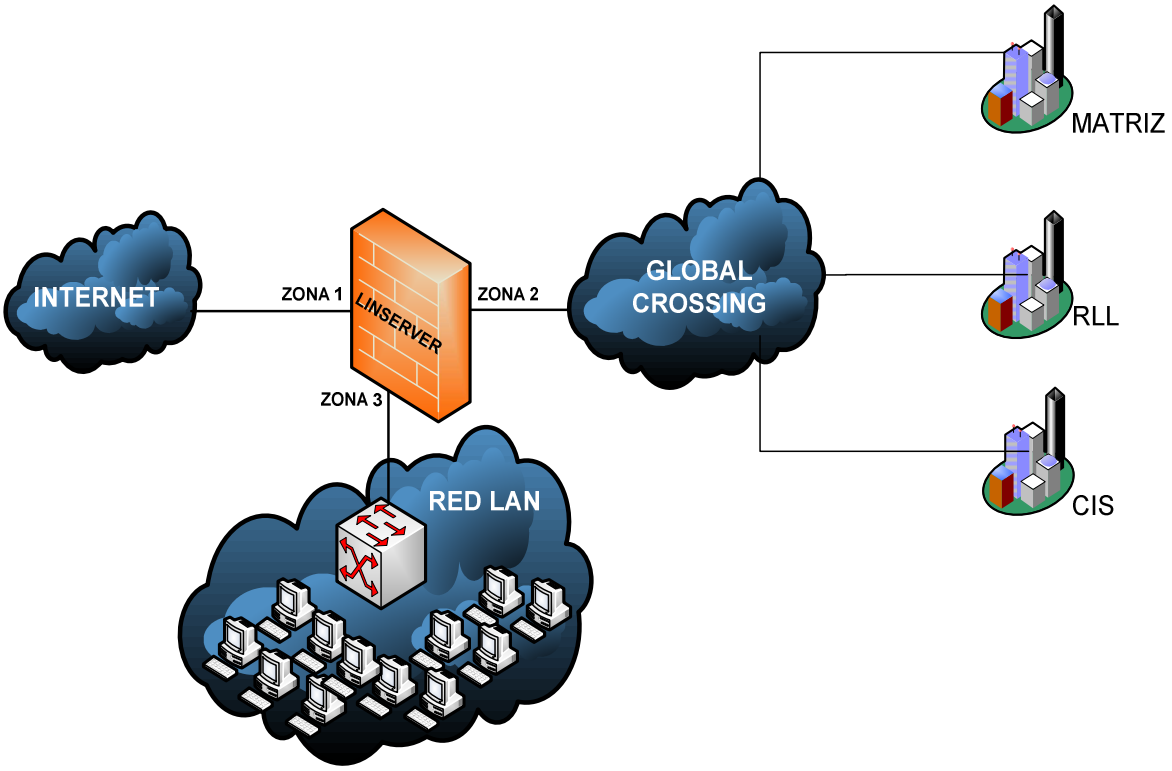


Figura 3.3 Definición de Zonas del Sistema de Seguridad Integral de Petroindustrial-REE

En esta Refinería no se diseña una DMZ ya que en el Switch de core existe una VLAN exclusiva para servidores; además, no existe alguno de ellos que se necesite conectar y dar servicio hacia Internet, todo el tráfico hacia los servidores será controlado por rutas existentes en el switch.

3.8.2.3 Diseño del Direccionamiento IP a aplicarse en Linserver UCNC y Routers de Frontera

Para independizar la red LAN de REE se debe realizar una restructuración del direccionamiento IP de los equipos de frontera, como también se debe asignar las direcciones respectivas a las interfaces del servidor LINSERVER.

A continuación se detalla el esquema que se propone para el presente diseño de seguridad perimetral en lo que se refiere a direccionamiento IP para este Distrito.
Para la Zona 1, que corresponde a Internet, se tiene la dirección 190.11.15.110/29 que corresponde al router del proveedor y para el servidor LINSERVER UCNC la dirección 190.11.15.109/29.

Para la Zona 2, que corresponde al enlace de datos a través de Global Crossing, se asigna la dirección 172.30.118.4/26 para el router de Global y la dirección 172.30.118.1/26 para la interfaz correspondiente al servidor LINSERVER UCNC.

Para la Zona 3, que corresponde a la conexión de la red LAN de REE, se asigna la dirección 172.30.20.50/24 que corresponderá a la puerta de enlace de la VLAN de servidores en el Switch Cisco 4507R y la dirección 172.30.20.22/24 para la interfaz correspondiente al servidor LINSERVER UCNC.

En un futuro se pretende crear en este Distrito una DMZ, a la cual se recomienda asignar la dirección de red 172.30.118.64/26 para una buena distribución de los equipos que se administren en esta área.

3.8.2.4 Rutas a Implementarse en Linserver UCNC

Según el estudio realizado de la red de REE se establece en la Tabla 3.2 las rutas que se deben crear en el servidor LINSERVER UCNC para que se integre en forma satisfactoria a la infraestructura existente en este Distrito.

RED DESTINO	GATEWAY	MASCARA	INTERFAZ	DESCRIPCIÓN
190.11.15.104	0.0.0.0	255.255.255.248	ETH1	Acceso Internet
0.0.0.0	190.11.15.110	0.0.0.0	ETH1	Acceso a Internet
172.30.118.0	0.0.0.0	255.255.255.192	ETH2	Acceso Perimetral
172.30.15.0	172.30.118.4	255.255.255.0	ETH2	Acceso a DMZ-MATRIZ
172.30.16.0	172.30.118.4	255.255.255.0	ETH2	Acceso Red LAN-MATRIZ
172.30.17.0	172.30.118.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.17.64	172.30.118.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.17.128	172.30.118.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.17.192	172.30.118.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.0	172.30.118.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.64	172.30.118.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.128	172.30.118.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.192	172.30.118.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.19.226.7	172.30.20.50	255.255.255.255	ETH3	Acceso a Petroecuador
172.19.230.0	172.30.20.50	255.255.255.0	ETH3	Acceso a Petroecuador
172.30.20.0	0.0.0.0	255.255.255.0	ETH3	Acceso a Red LAN-REE
172.30.21.0	172.30.20.50	255.255.255.0	ETH3	Acceso a Red LAN-REE
172.30.22.0	172.30.20.50	255.255.255.128	ETH3	Acceso a Red LAN-REE
172.30.22.128	172.30.20.50	255.255.255.128	ETH3	Acceso a Red LAN-REE
172.30.23.0	172.30.20.50	255.255.255.224	ETH3	Acceso a Red LAN-REE
172.30.23.32	172.30.20.50	255.255.255.224	ETH3	Acceso a Red LAN-REE
172.30.23.64	172.30.20.50	255.255.255.224	ETH3	Acceso a Red LAN-REE
172.30.23.96	172.30.20.50	255.255.255.224	ETH3	Acceso a Red LAN-REE
172.30.23.128	172.30.20.50	255.255.255.224	ETH3	Acceso a Red LAN-REE
172.30.23.160	172.30.20.50	255.255.255.224	ETH3	Acceso a Red LAN-REE
172.30.23.192	172.30.20.50	255.255.255.224	ETH3	Acceso a Red LAN-REE
172.30.23.224	172.30.20.50	255.255.255.224	ETH3	Acceso a Red LAN-REE

Tabla 3.4 Rutas a implementarse en el Servidor LINSERVER UCNC de REE

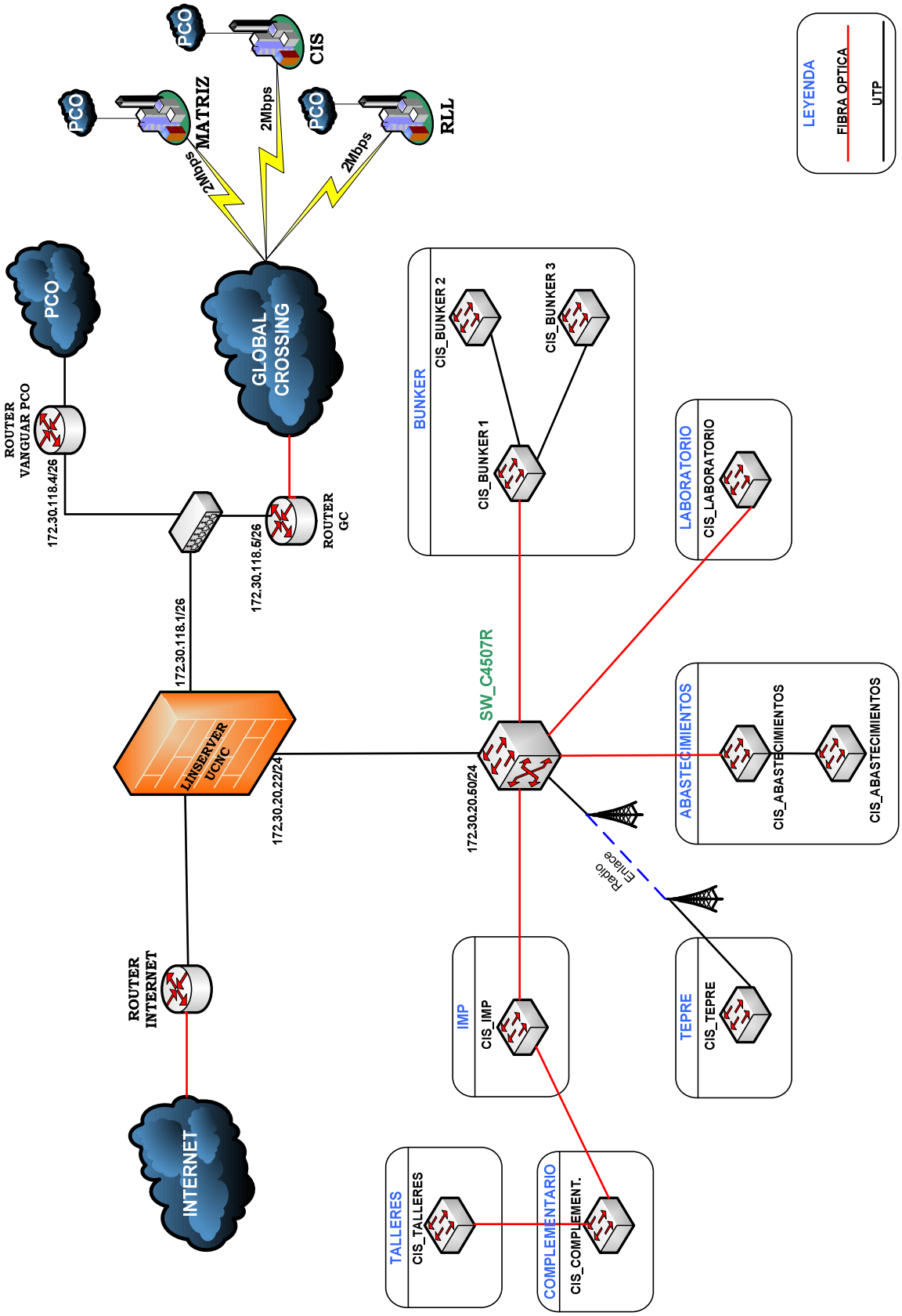


Figura 3.4 Esquema del Sistema de Seguridad Integral de Petroindustrial-REE

3.8.3 DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL DE COMPLEJO INDUSTRIAL SHUSHUFINDI

3.8.3.1 Requerimientos del Diseño

Para realizar el Diseño del Sistema de Seguridad Perimetral en el Complejo Industrial Shushufindi se requiere definir una nueva VLAN para seguridad perimetral. Además, se crean nuevas rutas y políticas para re direccionar y controlar el tráfico hacia Matriz y hacia el proveedor de Internet. De igual forma el nuevo enlace con Global Crossing obliga a realizar una restructuración a nivel de la red WAN.

3.8.3.2 Soluciones para el Diseño

Se creará una nueva VLAN en el switch de core, que se la denominará como Red Perimetral CIS con la dirección de red 172.30.120.0/26, y esta será completamente independiente y sin ninguna relación a las que se encuentran creadas.

Para el Diseño del Sistema de Seguridad Perimetral se utilizará un Servidor LINSERVER UCNC como infraestructura de Core, de las mismas características que en Matriz.

Este Servidor estará administrado por personal de esta Unidad Operativa, el mismo que cuenta con las siguientes Zonas:

- Zona 1: G-Ethernet 1 - Internet
- Zona 2: G-Ethernet 2 - Red Wan CIS
- Zona 3: G-Ethernet 3 - Red Lan CIS
- Zona 4, 5 y 6: G-Ethernet 4, 5 y 6 – Libres para futuras necesidades

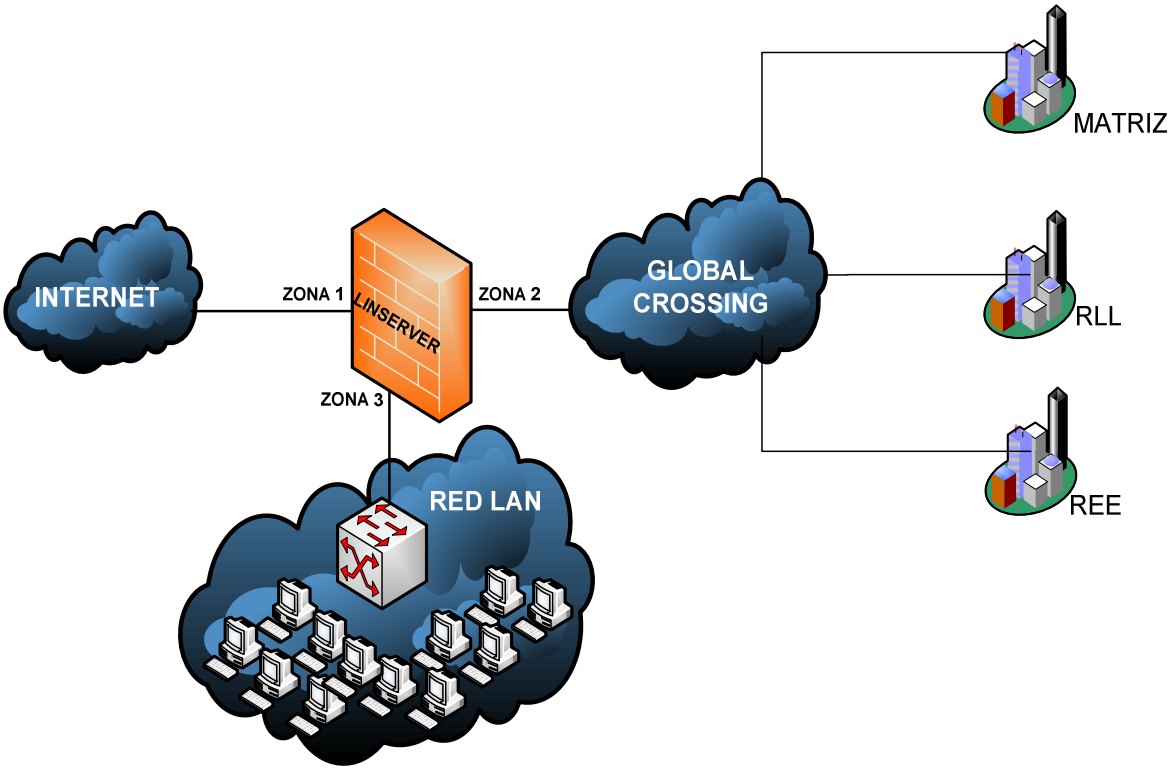


Figura 3.5 Definición de Zonas del Sistema de Seguridad Integral de Petroindustrial-CIS

En esta Refinería no se diseña una DMZ ya que en el Switch de core existe una VLAN exclusiva para servidores y no existe alguno de ellos que se necesite conectar y dar servicio hacia Internet. Todo el tráfico hacia los servidores será controlado por rutas existentes en el Switch.

3.8.3.3 Diseño del Direccionamiento IP a aplicarse en Linserver UCNC y Routers de Frontera

Para independizar la red LAN de CIS se debe realizar una restructuración del direccionamiento IP de los equipos de frontera, como también se debe asignar las direcciones respectivas a las interfaces del servidor Linserver.

A continuación se detalla el esquema que se propone para el presente diseño de seguridad perimetral en lo que se refiere a direccionamiento IP para este Distrito.

Para la Zona 1, que corresponde a Internet, se tiene la dirección 190.152.145.222/29 que corresponde al router del proveedor y para el servidor LINSERVER UCNC la dirección 190.152.145.221/29.

Para la Zona 2, que corresponde al enlace de datos a través de Global Crossing, se asigna la dirección 172.30.120.4/26 para el router de Global y la dirección 172.30.120.1/26 para la interfaz correspondiente al servidor LINSERVER UCNC.

Para la Zona 3 que corresponde a la conexión de la red LAN de CIS, se asigna la dirección 172.30.24.109/24 que corresponderé a la puerta de enlace de la VLAN de servidores en el Switch Cisco 4507R y la dirección 172.30.24.22/24 para la interfaz correspondiente al servidor LINSERVER UCNC.

En un futuro se pretende crear en este Distrito una DMZ para la cual se recomienda asignar la dirección de red 172.30.120.64/26 para una buena distribución de los equipos que se administren en esta área.

3.8.3.4 Rutas a Implementarse en Linserver UCNC

Según el estudio realizado de la red de CIS se establece en la Tabla 3.3 las rutas que se deben crear en el servidor LINSERVER UCNC para que se integre en forma satisfactoria a la infraestructura existente en este Distrito.

RED DESTINO	GATEWAY	MASCARA	INTERFAZ	DESCRIPCIÓN
190.152.145.116	0.0.0.0	255.255.255.248	ETH1	Acceso Internet
0.0.0.0	190.152.145.222	0.0.0.0	ETH1	Acceso a Internet
172.30.120.0	0.0.0.0	255.255.255.192	ETH2	Acceso Perimetral
172.30.15.0	172.30.120.4	255.255.255.0	ETH2	Acceso a DMZ-MATRIZ
172.30.16.0	172.30.120.4	255.255.255.0	ETH2	Acceso Red LAN-MATRIZ
172.30.17.0	172.30.120.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.17.64	172.30.120.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.17.128	172.30.120.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.17.192	172.30.120.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.0	172.30.120.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.64	172.30.120.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.128	172.30.120.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.192	172.30.120.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.19.226.7	172.30.24.109	255.255.255.255	ETH3	Acceso a Petroecuador
172.19.230.0	172.30.24.109	255.255.255.0	ETH3	Acceso a Petroecuador
172.30.24.0	0.0.0.0	255.255.255.0	ETH3	Acceso a Red LAN-CIS
172.30.25.0	172.30.24.109	255.255.255.240	ETH3	Acceso a Red LAN-CIS
172.30.25.16	172.30.24.109	255.255.255.240	ETH3	Acceso a Red LAN-CIS
172.30.25.32	172.30.24.109	255.255.255.240	ETH3	Acceso a Red LAN-CIS
172.30.25.48	172.30.24.109	255.255.255.240	ETH3	Acceso a Red LAN-CIS
172.30.25.64	172.30.24.109	255.255.255.240	ETH3	Acceso a Red LAN-CIS
172.30.25.80	172.30.24.109	255.255.255.240	ETH3	Acceso a Red LAN-CIS
172.30.25.96	172.30.24.109	255.255.255.240	ETH3	Acceso a Red LAN-CIS
172.30.25.112	172.30.24.109	255.255.255.240	ETH3	Acceso a Red LAN-CIS
172.30.25.128	172.30.24.109	255.255.255.224	ETH3	Acceso a Red LAN-CIS
172.30.25.160	172.30.24.109	255.255.255.224	ETH3	Acceso a Red LAN-CIS

Tabla 3.5 Rutas a implementarse en el Servidor LINSERVER UCNC de CIS

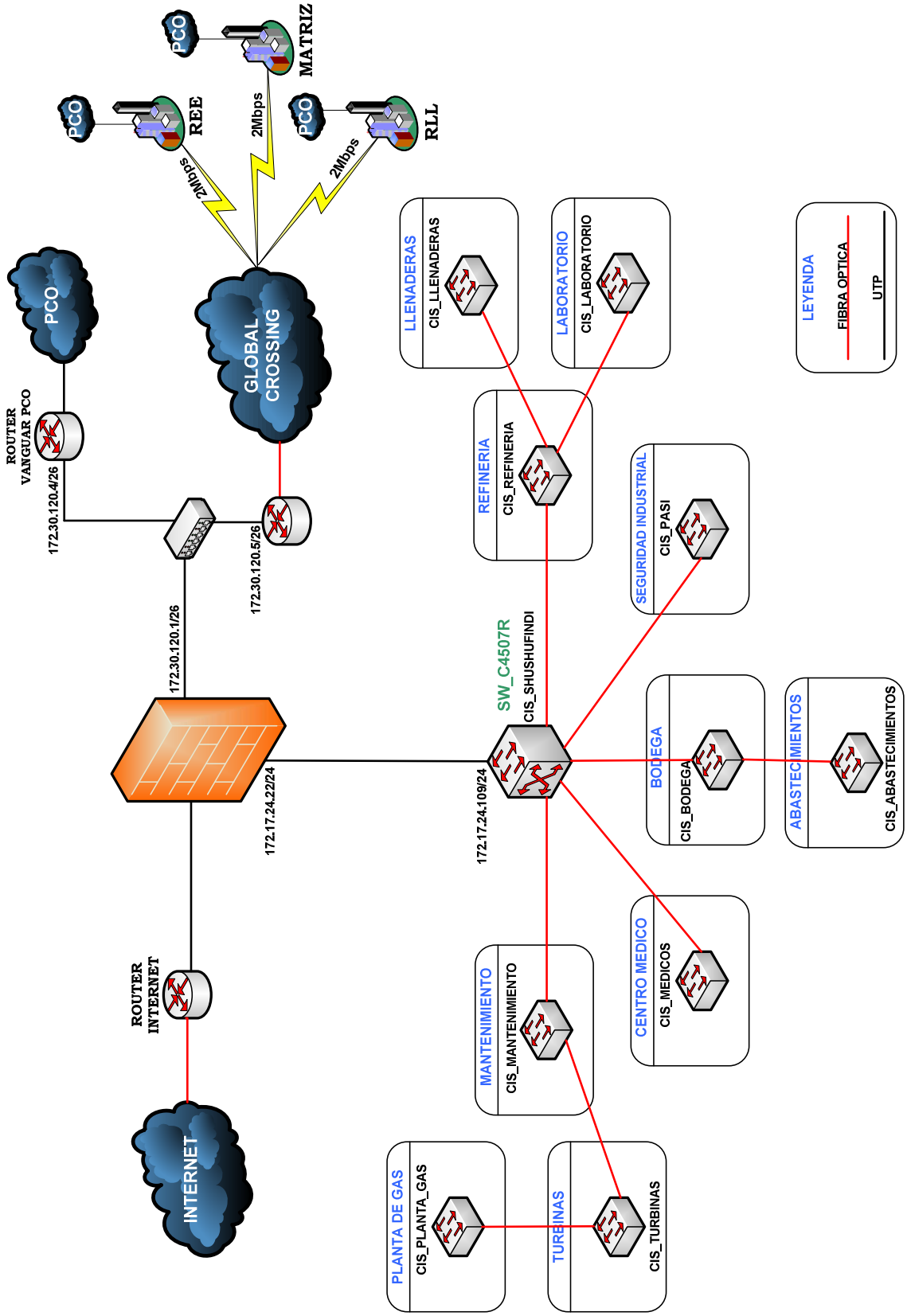


Figura 3.6 Esquema del Sistema de Seguridad Integral de Petroindustrial-CIS

3.8.4 DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL DE REFINERÍA LA LIBERTAD

3.8.4.1 Requerimientos del Diseño

Para realizar el Diseño del Sistema de Seguridad Perimetral en la Refinería La Libertad se requiere definir una nueva VLAN para seguridad perimetral, además nuevas rutas y políticas para re direccionar y controlar el tráfico hacia Matriz y hacia el proveedor de Internet. De igual forma el nuevo enlace con Global Crossing obliga a realizar una restructuración a nivel de la red WAN.

3.8.4.2 Soluciones para el Diseño

Se creará una nueva VLAN en el Switch de core, que se la denominará como Red Perimetral RLL la misma que se la ubicará en la red 172.30.119.0/26 y esta será completamente independiente y sin ninguna relación a las que se encuentran creadas.

Para el Diseño del Sistema de Seguridad Perimetral se va utilizar un Servidor LINSERVER UCNC como infraestructura de Core, de las mismas características que en Matriz.

Este Servidor estará administrado por personal de esta Unidad Operativa, el mismo que cuenta con las siguientes Zonas:

- Zona 1: G-Ethernet 1 - Internet
- Zona 2: G-Ethernet 2 - Red Wan REE
- Zona 3: G-Ethernet 3 - Red Lan REE
- Zona 4, 5 y 6: G-Ethernet 4, 5 y 6 – Libres para futuras necesidades

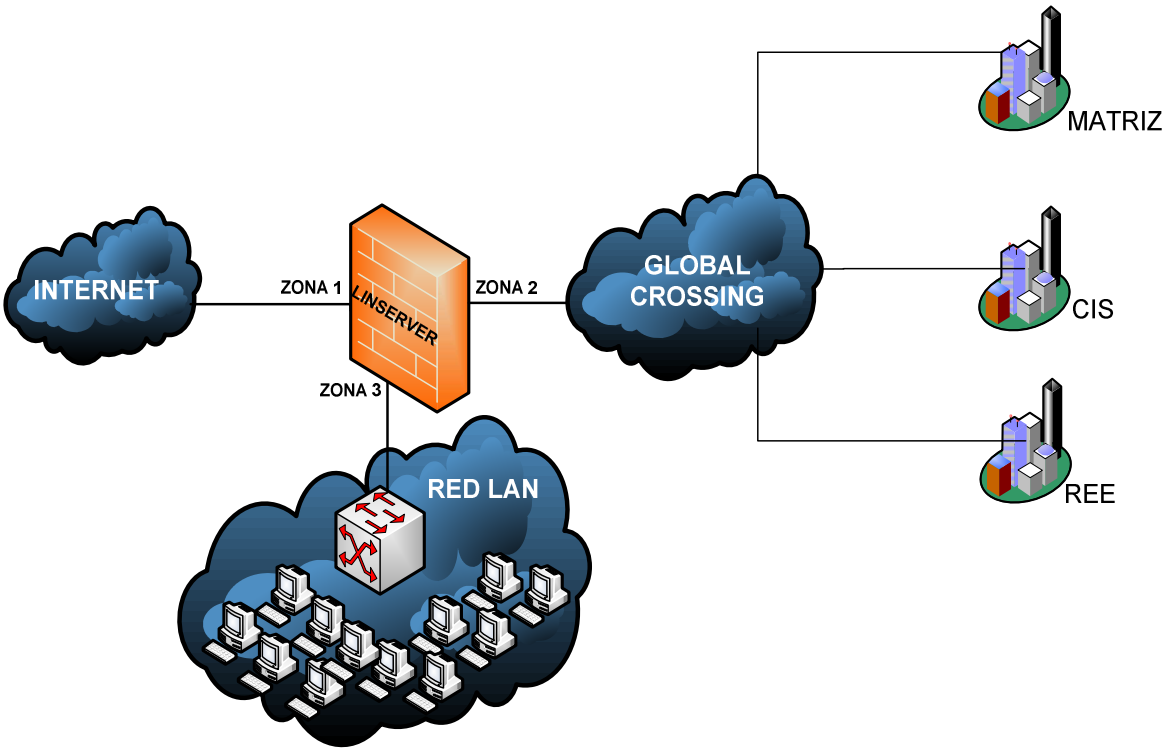


Figura 3.7 Definición de Zonas del Sistema de Seguridad Integral de Petroindustrial-RLL

En esta Refinería no se diseña una DMZ ya que en el Switch de core existe una VLAN exclusiva para servidores y además no existe alguno de ellos que se necesite conectar y dar servicio hacia Internet. Todo el tráfico hacia los servidores será controlado por rutas existentes en el Switch.

3.8.4.3 Definición de Direccionamiento IP a aplicarse en Linserver UCNC y Routers de Frontera

Para independizar la red LAN de RLL se debe realizar una restructuración del direccionamiento IP de los equipos de frontera como también se debe asignar las direcciones respectivas a las interfaces del servidor Linserver.

A continuación se detalla el esquema que se propone para el presente diseño de seguridad perimetral en lo que se refiere a direccionamiento IP para este Distrito.

Para la Zona 1, que corresponde a Internet, se tiene la dirección 190.95.224.30/30 que corresponde al router del proveedor y para el servidor Linserver UCNC la dirección 190.95.224.29/30.

Para la Zona 2, que corresponde al enlace de datos a través de Global Crossing, se asigna la dirección 172.30.119.4/26 para el router de Global y la dirección 172.30.119.1/26 para la interfaz correspondiente al servidor LINSERVER UCNC.

Para la Zona 3, que corresponde a la conexión de la red LAN de CIS, se asigna la dirección 172.30.28.233/24 que corresponderé a la puerta de enlace de la VLAN de servidores en el Switch Cisco 4507R y la dirección 172.30.28.254/24 para la interfaz correspondiente al servidor LINSERVER UCNC.

En un futuro se pretende crear en este Distrito una DMZ para la cual se recomienda asignar la dirección de red 172.30.119.64/26 para una buena distribución de los equipos que se administren en esta área.

3.8.4.4 Rutas a Implementarse en Linserver UCNC

Según el estudio realizado de la red de RLL se establece en la Tabla 3.4 las rutas que se deben crear en el servidor LINSERVER UCNC para que se integre en forma satisfactoria a la infraestructura existente en este Distrito.

RED DESTINO	GATEWAY	MASCARA	INTERFAZ	DESCRIPCIÓN
190.95.224.28	0.0.0.0	255.255.255.252	ETH1	Acceso Internet
0.0.0.0	190.95.224.30	0.0.0.0	ETH1	Acceso a Internet
172.30.119.0	0.0.0.0	255.255.255.192	ETH2	Acceso Perimetral
172.30.15.0	172.30.119.4	255.255.255.0	ETH2	Acceso a DMZ-MATRIZ
172.30.16.0	172.30.119.4	255.255.255.0	ETH2	Acceso Red LAN-MATRIZ
172.30.17.0	172.30.119.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.17.64	172.30.119.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.17.128	172.30.119.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.17.192	172.30.119.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.0	172.30.119.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.64	172.30.119.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.128	172.30.119.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.30.18.192	172.30.119.4	255.255.255.192	ETH2	Acceso Red LAN-MATRIZ
172.19.226.7	172.30.28.233	255.255.255.255	ETH3	Acceso a Petroecuador
172.19.230.0	172.30.28.233	255.255.255.0	ETH3	Acceso a Petroecuador
172.30.28.0	0.0.0.0	255.255.255.0	ETH3	Acceso a Red LAN-RLL
172.30.29.0	172.30.28.233	255.255.255.192	ETH3	Acceso a Red LAN-RLL
172.30.29.64	172.30.28.233	255.255.255.192	ETH3	Acceso a Red LAN-RLL
172.30.29.128	172.30.28.233	255.255.255.192	ETH3	Acceso a Red LAN-RLL
172.30.29.192	172.30.28.233	255.255.255.192	ETH3	Acceso a Red LAN-RLL
172.30.30.0	172.30.28.233	255.255.255.192	ETH3	Acceso a Red LAN-RLL
172.30.30.64	172.30.28.233	255.255.255.192	ETH3	Acceso a Red LAN-RLL
172.30.30.128	172.30.28.233	255.255.255.192	ETH3	Acceso a Red LAN-RLL
172.30.30.192	172.30.28.233	255.255.255.192	ETH3	Acceso a Red LAN-RLL
172.30.31.0	172.30.28.233	255.255.255.192	ETH3	Acceso a Red LAN-RLL
172.30.31.64	172.30.28.233	255.255.255.192	ETH3	Acceso a Red LAN-RLL
172.30.31.128	172.30.28.233	255.255.255.192	ETH3	Acceso a Red LAN-RLL

Tabla 3.6 Rutas a implementarse en el Servidor LINSERVER UCNC de RLL

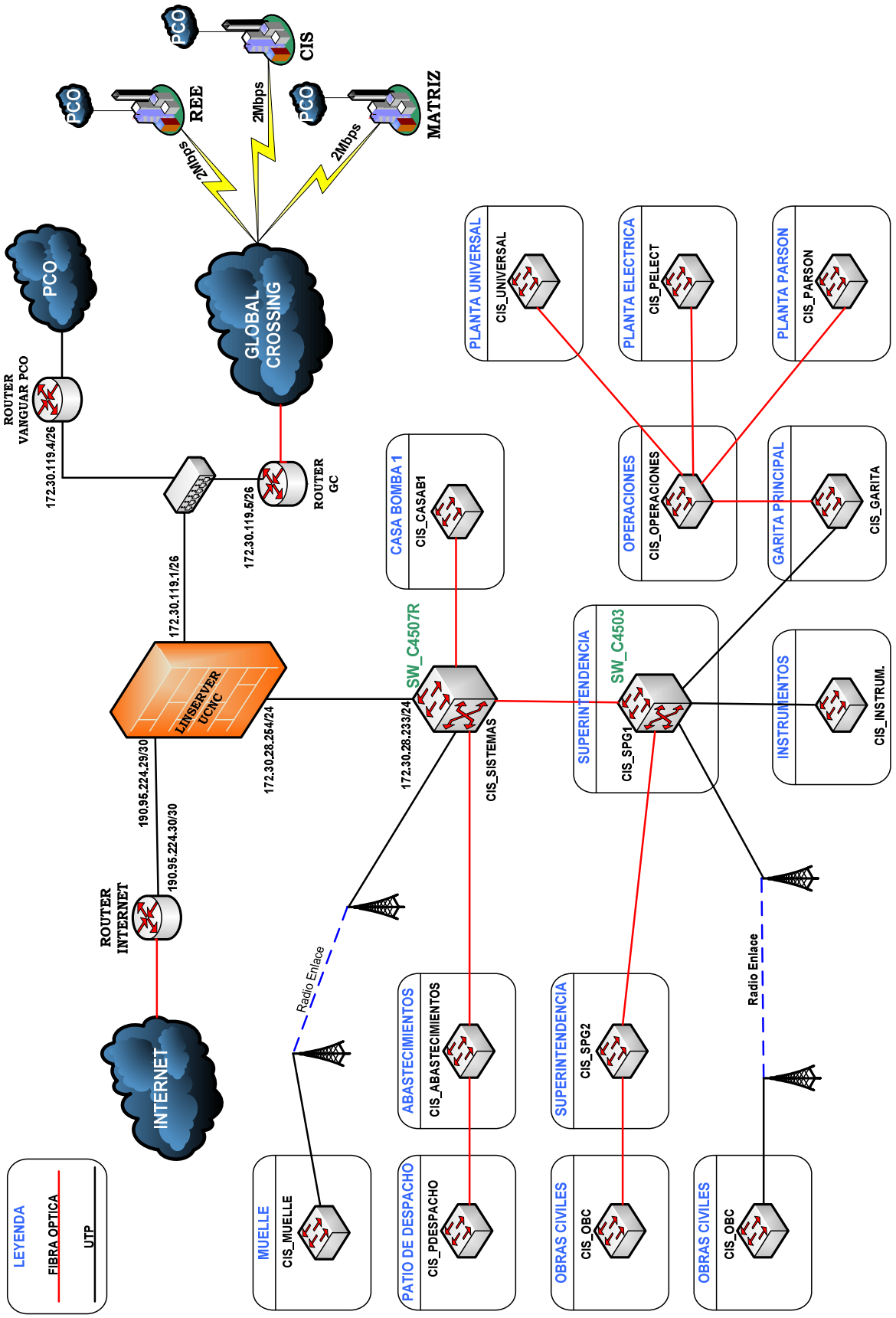


Figura 3.8 Esquema del Sistema de Seguridad Integral de Petroindustrial-RLL

Con esto se concluye el Diseño del Sistema de Seguridad operacional para mejorar la protección de las redes LAN y WAN de Petroindustrial, la cual es totalmente integrable a la infraestructura actual de la empresa y garantiza una optima funcionalidad y un nivel de seguridad, que seguirá fortificándose de acuerdo a las nuevas políticas que se crearán luego de una futura implementación

CAPÍTULO 4

DETERMINACIÓN DE COSTOS REFERENCIALES DEL SISTEMA DE SEGURIDAD

4.1 INTRODUCCIÓN

Una vez que se ha concluido con el Diseño del Sistema de Seguridad Operacional para la protección de las redes LAN y WAN de Petroindustrial, se presenta los costos referenciales. Tomando en cuenta que se trata de una empresa estatal, se realizó un presupuesto con dos alternativas de solución.

4.2 COSTOS REFERENCIALES DEL DISEÑO

4.2.1 COSTOS DE EQUIPOS JUNIPER SSG 550

En la Tabla 4.1 se puede observar los costos referenciales de los diferentes equipos necesarios para el presente diseño, como también del Software para Seguridad Perimetral y Administración de redes LAN y WAN.

COSTOS REFERENCIALES DE EQUIPOS JUNIPER SSG 550				
ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	SUBTOTAL
	GRUPO 1: SERVIDORES			
1	DL380 G5 XEON QUAD CORE E5430	4	11546,00	46184,00
2	Soporte en Servidores con Sistema Operativo	1	12000,00	12000,00
	GRUPO 1: SOFTWARE PARA SEGURIDAD PERIMETRAL Y ADMINISTRACION DE REDES LAN Y WAN			
3	SSG550 System, 1GB DRAM, 1AC Power Supply	4	9038,00	36152,00
4	1 Gigabyte RAM Memory Upgrade for the SSG 500 series	4	1722,00	6888,00
5	Módulo WebFilter SSG550	4	1980,00	7920,00
6	Módulo Deep Inspectin SSG550	4	904,00	3616,00
7	4 Port Fast Ethernet Enhanced PIM - Spare	4	1033,00	4132,00
8	Software de inventario de red IP	4	3864,00	15456,00
9	Optimizador de ancho de banda	4	5152,00	20608,00
10	Soporte y reporting de los equipos de Seguridad de red	1	33600,00	33600,00
			SUBTOTAL	**186556,00**
			I.V.A. 12%	**22386,72**
			VALOR TOTAL DE LA COTIZACIÓN INCLUIDO EL IVA	**208942,72**

Tabla 4.1 Costos Referenciales de Equipos y Software Juniper SSG 550

En la Tabla 4.2 se puede observar lo que costaría una futura implementación y en el ITEM 3 el precio de la capacitación e instalación de los Servidores y de los Equipos de Seguridad.

COSTOS REFERENCIALES DE EQUIPOS JUNIPER SSG 550				
ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	SUBTOTAL
	GRUPO 1: SERVIDORES			
1	DL380 G5 XEON QUAD CORE E5430	4	11546,00	46184,00
2	Soporte en Servidores con Sistema Operativo	1	12000,00	12000,00
3	Capacitación e Instalación de Servidores y de los Equipos de Seguridad	1	2500,00	2500,00
	GRUPO 1: SOFTWARE PARA SEGURIDAD PERIMETRAL Y ADMINISTRACION DE REDES LAN Y WAN			
4	SSG550 System, 1GB DRAM, 1AC Power Supply	4	9038,00	36152,00
5	1 Gigabyte RAM Memory Upgrade for the SSG 500 series	4	1722,00	6888,00
6	Módulo WebFilter SSG550	4	1980,00	7920,00
7	Módulo Deep Inspectin SSG550	4	904,00	3616,00
8	4 Port Fast Ethernet Enhanced PIM - Spare	4	1033,00	4132,00
9	Software de inventario de red IP	4	3864,00	15456,00
10	Optimizador de ancho de banda	4	5152,00	20608,00
11	Soporte y reporting de los equipos de Seguridad de red	1	33600,00	33600,00
			SUBTOTAL	**189056,00**
			I.V.A. 12%	**22686,72**
			VALOR TOTAL DE LA COTIZACIÓN INCLUIDO EL IVA	**211742,72**

Tabla 4.2 Costos Referenciales de Equipos, Software e Instalación

4.2.2 COSTOS DE EQUIPOS LINSERVER UCNC

A continuación se presenta los costos de otros dispositivos sugeridos en este diseño, tomando en cuenta que se recomienda el Servidor Linserver UCNC (Universal Corporate Networking Center). Se listan los precios en dos grupos el de Servidores y el de Software.

DETALLE VALORADO GRUPO 1				
ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	SUBTOTAL
1	Servidor HP Proliant DL380 G5 XEON QUAD CORE E 5430: INCLUYE	4	2905	11620,00
	1 Procesador Intel Xeon Quad Core E5430 2.66 GHz			
	2 GB installed 2x1 GB of 2-way interleaved PC2-5300 Fully Buffered DIMMs DDR2-667 (at 533MHz on processors witch 1066 MHz FSB) with Advanced ECC, mirrored and online spare memory capabilities.			
	2 HP Ethernet Interfaces 10/100/1000 Base T			
	RAID (Serial ATA-150/SAS) - PCI Express x8(Smart Array P400); IDE (IDE/ATA)			
	Cache Memory: 12MB L2 cache			
	Cache por Procesador: 12MB (2x6MB(6MB per core pair))			
	1 Power supply - hot - plug AC 120/230V (50/60Hz)			
2	1 Procesador Adicional Intel Xeon Quad Core E5430 2.66 GHz	4	875,00	3500,00
3	2 GB Aditional Kit 2x1 GB of 2-way interleaved PC2-5300 Fully Buffered DIMMs DDR2-667 (at 533MHz on processors witch 1066 MHz FSB) with Advanced ECC, mirrored and online spare memory capabilities.	4	218,00	872,00
4	HP Hard Disk: 146GB 10K SAS 2.5 Hot Plug Hard Drive	16	341,00	5456,00
5	1 Power supply - hot- plug / redundant	4	300,00	1200,00
6	HP Modular PDU: HP Low Voltage Modular Power Distribution Unit Zero-U/1U- power distribution strip.	4	390,00	1560,00
7	HP NC364T Pcle Tarjeta PCI Express de 4 Ethernet Interfaces 10/100/1000 Base T	8	700,00	5600,00
8	Instalación, configuración en cada Unidad Operativa de Petroindustrial	4	698,00	2792,00
9	Carepack DL38x 6horas. Call to Repair CTR3Y. Por 36 meses	4	950,00	3800,00
			SUBTOTAL	36400,00
			I.V.A. 12%	4368,00
			VALOR TOTAL DE LA COTIZACIÓN INCLUIDO EL IVA	40768,00

Tabla 4.3 Costos Referenciales de Dispositivos para el Servidor Linserver UCNC

DETALLE VALORADO GRUPO 2				
ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	SUBTOTAL
3	Linserver UCNC Firewall Licencia Unlimited Users	4	2478,00	9912,00
4	Linserver UCNC IPS Licencia Unlimited Users	4	3189,00	12756,00
5	Linserver UCNC IDS Licencia Unlimited Users	4	2200,00	8800,00
6	Linserver UCNC Monitoreo Licencia Unlimited Users	4	3567,00	14268,00
7	Linserver UCNC Proxificación Licencia Unlimited Users	4	1478,00	5912,00
8	Linserver UCNC Inspector de Contenido Licencia Unlimited Users	4	1970,00	7880,00
9	Linserver UCNC Operador de Ancho de Banda Licencia Unlimited Users	4	1209,00	4836,00
10	Linserver UCNC Inventario de HW IP Licencia Unlimited Users	4	2809,00	11236,00
			SUBTOTAL	75600,00
			I.V.A. 12%	9072,00
			VALOR TOTAL DE LA COTIZACIÓN INCLUIDO EL IVA	84672,00

Tabla 4.4 Costos Referenciales del Software para el Sistema de Seguridad Perimetral y Administración de redes LAN y WAN.

COSTOS REFERENCIALES DE EQUIPOS LINSERVER UCNC				
ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	SUBTOTAL
	GRUPO 1: SERVIDORES	4	9100	36400,00
1	HP Proliant DL380 G5 XEON QUAD CORE E5430			
2	Garantía extendida, soporte y mantenimiento por 36 meses. Tiempo de atención: Quito 6 horas, Shushufindi, Esmeraldas y Libertad 48 horas			
	GRUPO 2: SOFTWARE PARA SEGURIDAD PERIMETRAL Y ADMINISTRACION DE REDES LAN Y WAN LINSERVER UCNC (UNIVERSAL CORPORATE NETWORKING CENTER)	4	18900,00	75600,00
3	Linserver UCNC Firewall Licencia Unlimited Users			
4	Linserver UCNC IPS Licencia Unlimited Users			
5	Linserver UCNC IDS Licencia Unlimited Users			
6	Linserver UCNC Monitoreo Licencia Unlimited Users			
7	Linserver UCNC Proxificación Licencia Unlimited Users			
8	Linserver UCNC Inspector de Contenido Licencia Unlimited Users			
9	Linserver UCNC Inventario de HW IP Licencia Unlimited Users			
10	Linserver UCNC Operador de Ancho de Banda Licencia Unlimited Users			
			SUBTOTAL	**112000,00**
			I.V.A. 12%	**13440,00**
			VALOR TOTAL DE LA COTIZACIÓN INCLUIDO EL IVA	**125440,00**

Tabla 4.5 Costos Referenciales de Equipos y Software Linserver UCNC

En las siguientes Tablas se proporciona un detalle de precios para una futura implementación tomando en cuenta aspectos como instalación, configuración, soporte y capacitación para que el sistema de seguridad quede en condiciones adecuadas para cumplir las necesidades de la empresa.

DETALLE VALORADO GRUPO 1				
ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	SUBTOTAL
1	Servidor HP Proliant DL380 G5 XEON QUAD CORE E 5430: INCLUYE	4	2905	11620,00
	1 Procesador Intel Xeon Quad Core E5430 2.66 GHz			
	2 GB installed 2x1 GB of 2-way interleaved PC2-5300 Fully Buffered DIMMs DDR2-667 (at 533MHz on processors witch 1066 MHz FSB) with Advanced ECC, mirrored and online spare memory capabilities.			
	2 HP Ethernet Interfaces 10/100/1000 Base T			
	RAID (Serial ATA-150/SAS) - PCI Express x8(Smart Array P400); IDE (IDE/ATA)			
	Cache Memory: 12MB L2 cache			
	Cache por Procesador: 12MB (2x6MB(6MB per core pair))			
	1 Power supply - hot - plug AC 120/230V (50/60Hz)			
2	1 Procesador Adicional Intel Xeon Quad Core E5430 2.66 GHz	4	875,00	3500,00
3	2 GB Aditional Kit 2x1 GB of 2-way interleaved PC2-5300 Fully Buffered DIMMs DDR2-667 (at 533MHz on processors witch 1066 MHz FSB) with Advanced ECC, mirrored and online spare memory capabilities.	4	218,00	872,00
4	HP Hard Disk: 146GB 10K SAS 2.5 Hot Plug Hard Drive	16	341,00	5456,00
5	1 Power supply - hot- plug / redundant	4	300,00	1200,00
6	HP Modular PDU: HP Low Voltage Modular Power Distribution Unit Zero-U/1U- power distribution strip.	4	390,00	1560,00
7	HP NC364T Pcle Tarjeta PCI Express de 4 Ethernet Interfaces 10/100/1000 Base T	8	700,00	5600,00
8	Instalación, configuración en cada Unidad Operativa de Petroindustrial	4	698,00	2792,00
9	Carepack DL38x 6horas. Call to Repair CTR3Y. Por 36 meses	4	950,00	3800,00
			SUBTOTAL	**36400,00**
			I.V.A. 12%	**4368,00**
			VALOR TOTAL DE LA COTIZACIÓN INCLUIDO EL IVA	**40768,00**

Tabla 4.6 Costos Referenciales de Dispositivos para el Servidor Linserver UCNC

DETALLE VALORADO GRUPO 2				
ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	SUBTOTAL
1	Servicios de Instalación	4	4087	16348,00
2	Servicios de Configuración	4	8560,00	34240,00
3	Linserver UCNC Firewall Licencia Unlimited Users	4	2478,00	9912,00
4	Linserver UCNC IPS Licencia Unlimited Users	4	3189,00	12756,00
5	Linserver UCNC IDS Licencia Unlimited Users	4	2200,00	8800,00
6	Linserver UCNC Monitoreo Licencia Unlimited Users	4	3567,00	14268,00
7	Linserver UCNC Proxificación Licencia Unlimited Users	4	1478,00	5912,00
8	Linserver UCNC Inspector de Contenido Licencia Unlimited Users	4	1970,00	7880,00
9	Linserver UCNC Operador de Ancho de Banda Licencia Unlimited Users	4	1209,00	4836,00
10	Linserver UCNC Inventario de HW IP Licencia Unlimited Users	4	2809,00	11236,00
11	Soporte Mantenimiento 12 meses	4	6309,40	25237,60
12	Capacitación Linserver UCNC	1	1920,00	1920,00
			SUBTOTAL	153345,60
			I.V.A. 12%	18401,47
			VALOR TOTAL DE LA COTIZACIÓN INCLUIDO EL IVA	171747,07

Tabla 4.7 Costos Referenciales del Software para el Sistema de Seguridad Perimetral y Administración de redes LAN y WAN y Servicios de implementación.

COSTOS REFERENCIALES DE EQUIPOS LINSERVER UCNC				
ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	SUBTOTAL
	GRUPO 1: SERVIDORES	4	9100	36400,00
1	HP Proliant DL380 G5 XEON QUAD CORE E5430			
2	Garantía extendida, soporte y mantenimiento por 36 meses. Tiempo de atención: Quito 6 horas, Shushufindi, Esmeraldas y Libertad 48 horas			
	GRUPO 2: SOFTWARE PARA SEGURIDAD PERIMETRAL Y ADMINISTRACION DE REDES LAN Y WAN LINSERVER UCNC (UNIVERSAL CORPORATE NETWORKING CENTER)	4	38336,40	153345,60
3	Servidores de Instalación			
4	Servidores de Configuración			
5	Linserver UCNC Firewall Licencia Unlimited Users			
6	Linserver UCNC IPS Licencia Unlimited Users			
7	Linserver UCNC IDS Licencia Unlimited Users			
8	Linserver UCNC Monitoreo Licencia Unlimited Users			
9	Linserver UCNC Proxificación Licencia Unlimited Users			
10	Linserver UCNC Inspector de Contenido Licencia Unlimited Users			
11	Linserver UCNC Inventario de HW IP Licencia Unlimited Users			
12	Linserver UCNC Operador de Ancho de Banda Licencia Unlimited Users			
13	Soporte Mantenimiento 12 meses			
14	Capacitación Linserver UCNC			
			SUBTOTAL	189745,60
			I.V.A. 12%	22769,47
			VALOR TOTAL DE LA COTIZACIÓN INCLUIDO EL IVA	212515,07

Tabla 4.8 Costos Referenciales de Equipos, Software Linserver UCNC y Servicios de Implementación

A pesar que la segunda opción tiene una cotización mayor, se la recomienda por motivos de funcionalidad y beneficios que garantizará un mejor rendimiento del sistema de seguridad operacional.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

Luego de realizado este trabajo, de los resultados obtenidos es posible extraer las conclusiones siguientes:

5.1 CONCLUSIONES

- Petroindustrial, como una empresa de industrialización del petróleo de propiedad del Estado Ecuatoriano, que aporta productivamente al desarrollo del país, tiene la obligación de poseer los mejores equipos en todos los ámbitos sean humanos o de carácter tecnológico. Por esta razón, se ha visto la necesidad de diseñar un sistema de seguridad integral que brinde la protección adecuada a las redes de comunicación hacia las diferentes áreas productivas para garantizar la transferencia segura de información.

- Petroindustrial posee una infraestructura de red LAN y WAN que tienen un alto grado de complejidad, ya que como toda red actual, se encuentra en constante crecimiento y requiere de nuevas actualizaciones tecnológicas para satisfacer las necesidades de los usuarios, razón por la cual los proyectos realizados deben ser innovadores para garantizar el desarrollo de la misma.

- Puesto que en la actualidad hay una demanda creciente de acceso a Internet, las redes están expuestas a diferentes peligros como: Virus, Gusanos, Caballos de Troya, los mismos que pueden mermar la confiabilidad y el rendimiento de la empresa, de aquí la importancia de tener un sistema que sea capaz de monitorear y detectar todo este tráfico malicioso que perjudicará la información de Petroindustrial.

- Hoy en día las amenazas para las redes de datos son mucho más sofisticadas, buscando redes vulnerables para causar ataques que pueden ser muy peligrosos para la integridad de la información de las empresas. Un buen método para combatirlas es instalar un sistema de hardware y software de seguridad que controle este problema con ayuda de políticas que proporcionen un conjunto de requisitos definidos por los administradores, que garanticen la seguridad de la red.

- En la actualidad existen Tecnologías de Seguridad unificadas como UTM (Unified Threat Management) que brinda un alto grado de seguridad para la protección de las redes informáticas mediante la incorporación de varias técnicas y componentes de seguridad, entre ellos, Firewalls, VPNs, IDS, IPS, Controladores de Ancho de Banda entre los más importantes.

- A lo largo de este trabajo se ha podido comprender la importancia de asegurar la información mediante un conjunto de recursos destinados a lograr que los activos de una organización permanezcan confidenciales, exhiban integridad y siempre estén disponibles para todos los usuarios.

- Hay que estar consientes que no existe un esquema de seguridad que cubra en su totalidad los posibles riesgos; sin embargo, hay que estar preparados y dispuestos a reaccionar con rapidez ya que las amenazas cambian constantemente.

- El sistema de seguridad diseñado cuenta con un cortafuegos capaz de filtrar tráfico a nivel de capa de enlace, (capa 2), de red (capa 3) y de transporte (capa 4) a través de iptables y a nivel de capa de aplicación gracias a la tecnología proxy. También es posible implementar mecanismos de priorización de tráfico que permita controlar el ancho de banda para brindar calidad de servicio.

- Se puede concluir que las expectativas personales fueron totalmente satisfechas, pues se tuvo la oportunidad de aprender nuevos conceptos, y se trabajó sobre temas vigentes y se pudo aplicar la teoría a un caso práctico.

- Los costos de los equipos a utilizarse cuentan mucho en el momento de tomar una decisión ya que se debe tomar en cuenta la posición económica que tenga la empresa, y hacer una evaluación en virtud de escoger la mejor opción para diseñar un sistema de seguridad que garantice la tranquilidad de los usuarios.

5.2 RECOMENDACIONES

De la experiencia obtenida durante la ejecución de este trabajo es posible extraer las recomendaciones siguientes:

- Se recomienda realizar conferencias para concientizar a los trabajadores de la empresa sobre la importancia de implementar un sistema de seguridad para la información y así prevenir incidentes y estar preparados para los retos tecnológicos que se presentan continuamente.

- Se recomienda desarrollar e implementar políticas de seguridad que apoyen y permitan obtener el máximo provecho de las bondades que brinda el sistema de seguridad diseñado.

- La política restrictiva que se implementa en el firewall debe ser muy bien comprendida, ya que de este aspecto depende la protección de la red de datos

de la empresa y la implementación de nuevos servicio que a futuro requerirá la empresa para poder habilitar en el firewall.

- Es recomendable investigar los puertos que utilizan las diferentes aplicaciones asociadas a la capa de transporte, antes de aplicar una restricción en el firewall para garantizar el correcto funcionamiento de la misma.

- Se recomienda realizar una reestructuración de la red, en particular las VLANs existentes en Petroindustrial, ya que muchas de ellas no soportarán el crecimiento y cambio continuo que sufre esta empresa.

- Para realizar el diseño de seguridad, se debe analizar minuciosamente la red actual de la empresa, es decir su infraestructura, sus sistemas operativos, conocer los puertos utilizados por cada aplicación, saber las configuraciones de los switches o routers existentes, para de esta manera tener una visión clara para que el diseño sea confiable y garantice el correcto enrutamiento de la información con los nuevos dispositivos añadidos.

- Para realizar políticas de seguridad, se debe hacer una auditoria previa en todas las áreas operativas de la empresa, con esto, a más de reunir la información necesaria, se involucra a todos los empleados en este importante proceso de cambio y lograr así una migración con mayor facilidad y rapidez.

- Al tener un equipo de seguridad con tecnología UTM en cada distrito, el cual proporciona muchas aplicaciones de seguridad, se recomienda crear una política de uso que establezca que la Matriz de Petroindustrial tenga el control total de dichos equipos, y los administradores de cada distrito solo el que le pertenece. Con esto se logrará tener una mejor administración de la red y se facilitará la solución de problemas o la habilitación de una nueva aplicación a nivel de firewall o proxy.

REFERENCIAS BIBLIOGRÁFICAS

[1] MAIWALD Eric. Fundamentos de Seguridad de Redes. Segunda Edición McGranHill.

[2] CHAPMAN David. Firewalls PIX de Cisco Secure. Segunda Edición. ELECE Industria Gráfica S.L.

[3] KAEO Merike. Diseño de Seguridad en Redes. Segunda Edición. Mater Offset S.L.

[4] VILLALÓN Huerta Antonio. Seguridad en Unix y Redes. Versión 1.2 Octubre 2000.

[5] ANDREW S. Tanenbaum. Redes de Computadoras. Cuarta Edición. Pearson Prentice Hall.

[6] WACK John, CUTLER Ken, POLE Jamie. Guidelines on Firewalls and Firewall Policy. National Institute of Standards and Technology Special Publication. Enero, 2002.

[7] BACE Rebecca. Intrusion Detection, Macmillan Technical Publishing, 2000.

[8] HERRERA Jordi, GARCÍA Joaquín, PERRAMÓN Javier. Aspectos Avanzados en Seguridad de Redes. Primera Edición. Eureca Media, SL

[9] LUCENA José. Criptografía y Seguridad en Computadores. Tercera Edición. Versión 2.0.1. Marzo de 2003.

[10] STALLING Willam. Cryptography and network security: Principles and Practice. Segunda Edición. Prentice Hall

[11] CCNA Discovery 4.0 Networking para el hogar y pequeñas empresas.

[12] http://www.petroindustrial.com.ec/frontEnd/main.php

[13] http://www.netxg.com/Products/Cisco/C6500Series/WS-C6509-E.html

[14] http://www.consein.com/images/PDF/symantec/SymantecEnterpriseEdition.pdf

[15] http://www.nec.com.

ANEXO

Lin Server UCNC

Lin Server UCNC

Universal Corporate Networking Center

LinSERVER Universal Corporate Networking Center es un producto creado para reemplazar todo el equipamiento de software y de hardware que para el MIDDLEWARE posee una organización. Y cuyo objetivo principal es eliminar el licenciamiento de productos para el funcionamiento de una red corporativa.

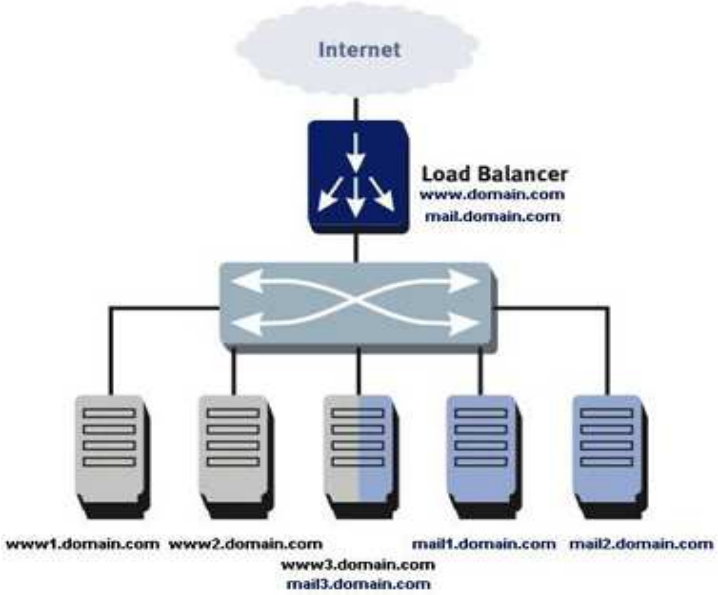
Esta solución es la más completa del mercado e incluye tanto software como hardware para MIDDLEWARE, se brinda una solución global e integrada que incluye un servicio y soporte en varios niveles.

Esta plataforma incluye la migración del sistema de correo a uno más moderno y mucho más sofisticado que incluye el uso del LDAP, capas de seguridad, capas de filtrado y que incluye políticas de administración de correo electrónico personalizadas y de mayor flexibilidad entregando propiedades a todo el conjunto de usuarios de manera fácil y sencilla como a su vez de manera puntual a un usuario, a grupos de usuarios definidos por el administrador. Incluye además servicio de antivirus y antispam que garantiza 100% de tráfico de correo libre de virus y de spam. Esto solamente como una parte menor de los servicios que se entregan como parte de la plataforma de networking corporativo. Puesto que este es un producto que comprende y abarca todo lo que es una solución de red: Firewall, IDS, IPS, DHCP local o remoto, DNS, servidor de Dominio, políticas de seguridad de red local, servidor web, servidor de túneles privados por Internet, voz sobre IP, manejador de cámaras de video, y todo lo que una red corporativa pueda requerir.

Lo más importante es que este producto es modular y puede instalarse completo como de manera separada módulo por módulo, por ejemplo puede adecuarse a servidores de Correo como Exchange o Lotus Domino, sin interferir en su configuración original.

BONDADES QUE BRINDA EL PRODUCTO

Servidor de Load Balancing

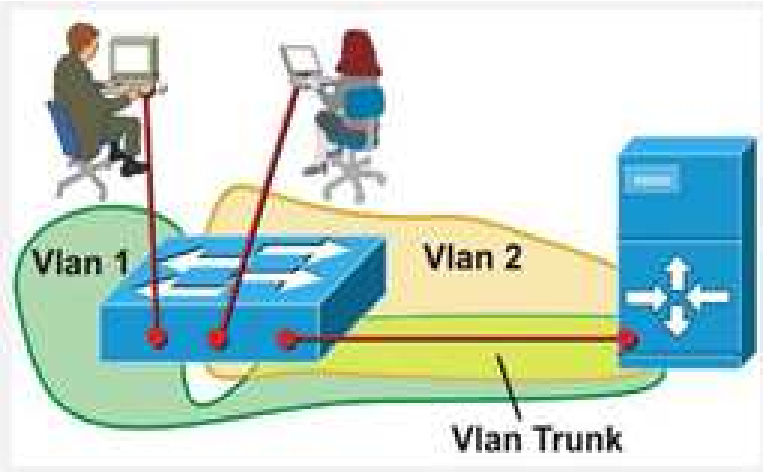


LinSERVER UCNC puede balancear el tráfico de una red que viaja sobre TCP/IP logrando balancear aplicativos, servidores de aplicación, carga hacia routers y switch's. Acoplandose a VLAN's estructuradas, o en su defecto formando VLAN's con tráfico controlado y balanceado. Se puede balancear carga y distribuir carga en varios servidores tanto para aplicativos como para tráfico.

Virtualización de Servidores

LinSERVER UCNC genera un servidor de Virtualización para Servidores tanto en Windows con Linux o Unix, una poderosa herramienta para aprovechar al máximo el equipamiento de Hardware que posee una compañía. Permite correr en un mismo equipo varios servidores de plataformas de sistemas operativos diferentes y hasta no compatibles como Linux y Windows.

Engine para el manejo de router's y Switch's



LinSERVER UCNC genera conexión para el manejo y administración de Router's y Switch, permitiendo una administración centralizada desde la herramienta Web 100% Gráfica. Permite establecer VLAN's con control de tráfico y permisos adicionando a este servicio como a todos la integración con el directorio Activo. Maneja Interfaces: Ethernet, 802.1 q VLAN, PPP 802.3ad Link Aggregation.

Servidor SMS (Short Messange Service)

LinSERVER posee un gestor de manejo de mensajes SMS, conectado a su appliance incorpora un teléfono celular que puede enviar y recibir mensajes SMS desde y hacia cualquier teléfono celular. El mecanismo sofisticado de LinSERVER permite:

Recibir alertas desde el servidor de monitoreo hacia los administradores en su teléfono celular en cualquier lugar o momento.

Recibir mensajes SMS que incluyan comandos de administración desde un teléfono registrado, desde cualquier ubicación geográfica del Ecuador incluso fuera de él en cualquier momento.

Procesar cualquier alerta desde el módulo de administración y monitoreo.

Interface de Dispositivos Biométricos

LinSERVER posee una interface con dispositivos biométricos que permite enlazar la información de los mismos y efectuar alertas en tiempo real.

Servidor de Monitoreo

En el caso de poseer servidores de Oracle Data Base Server u Oracle Application Server la solución cuenta con un módulo desarrollado para proveer monitoreo en tiempo real de los servidores que permiten alertar de cualquier funcionamiento anómalo, y reportarlo al administrador.

Permite generar estadísticas de todo lo que monitoree, en tiempo real e histórico.

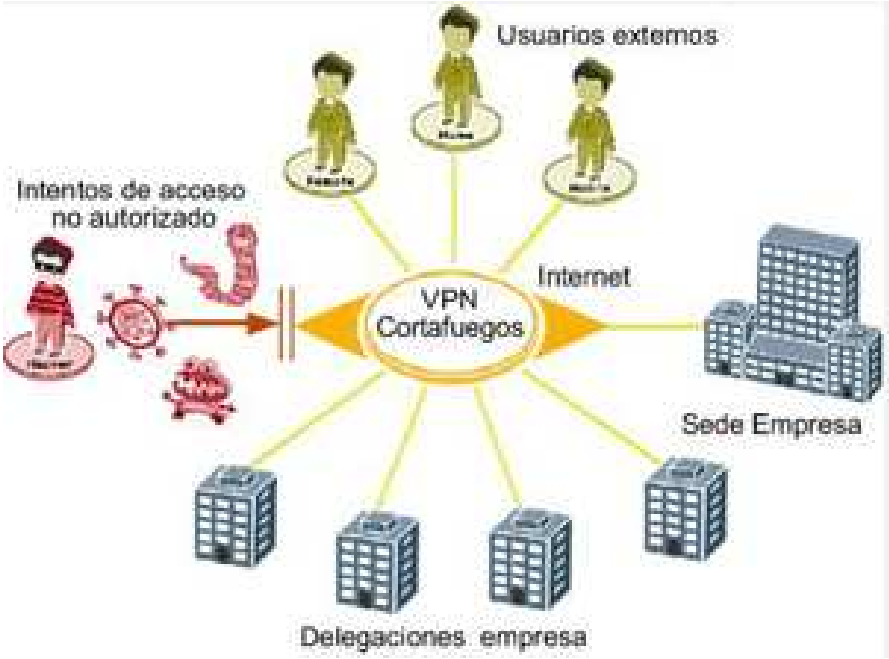
El servidor de Monitoreo ofrece al **CLIENTE**, un análisis completo de los servicios de la red, como son: Ancho de Banda por canal y monitoreo al proveedor, servicios Web, Mail, POP, DHCP, Bases de Datos, control de inventarios entre otros, actuando con alarmas en tiempo real en el momento que se quede fuera de servicio cada uno de ellos.

Permite guardar información del status de los computadores.

Permite personalizar alertas, usuarios, y accesos.

Permite analizar el tipo de tráfico que atraviesa en cada segmento de red, facilitando tareas de búsqueda de posibles errores, así como de ataques.

Establecimiento de VPN y Túneles Privados

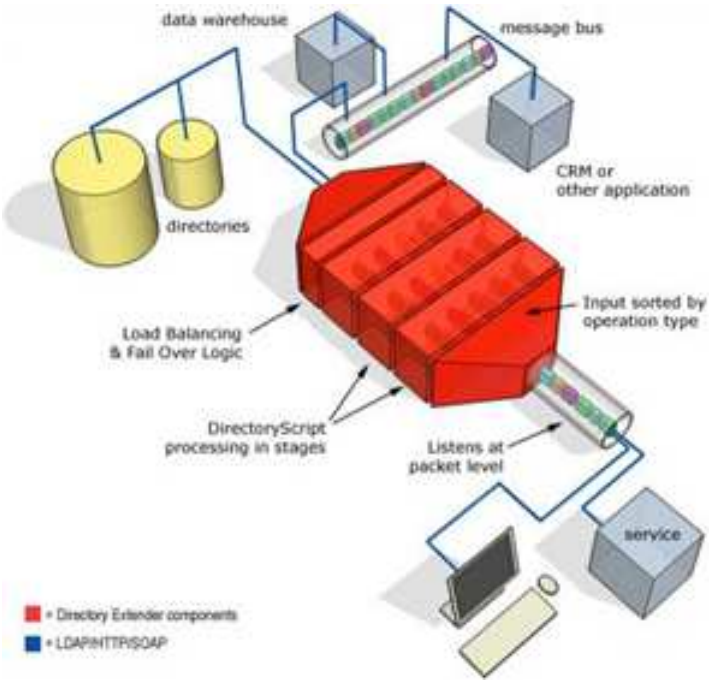


Se puede establecer VPN con cualquier cliente en el Internet poniendo a disposición recurso de la red local de manera segura Base de Datos accesos específicos de manera segura. Se puede establecer túneles privados y seguros con cualquier otra red, necesitando solamente poseer un enlace al menos 64 kbps.

Acceso Remoto Seguro

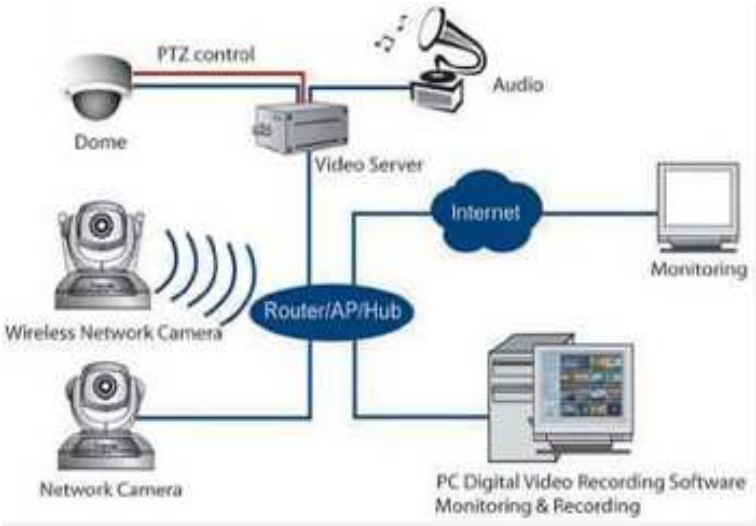
El servidor estará listo para poder acceder a él desde cualquier lugar del mundo a través de una consola bajo el protocolo SSH, llevando su información cifrada de un lugar a otro, monitorear, configurar y administrar el servidor. Podrá transferir, de igual forma, archivos de cualquier tamaño y para cualquier fin.

Inventarios de la Red



Gracias a los modernos sistemas de Open LDAP se puede mostrar un completo inventario de equipos, dispositivos y usuarios en tiempo real.

Video Digital Almacenamiento y Publicación

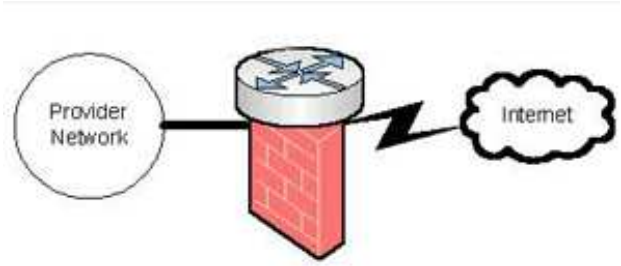


Los ejecutivos de la empresa con la debida seguridad pueden controlar lo que sus empleados hacen sin que ellos perciban que están siendo controlados todo el tiempo y sin necesidad de transportarse a su oficina para realizarlo.

Permite grabar y reproducir eventos programados, mostrarlos en tiempo real o almacenarlos para una posterior lectura según fechas.

La aplicación le permite la grabación del video capturado por cámaras de vigilancia y permite revisar día por día, hora por hora, cualquier evento extraño, como robos o daños causados a equipos, e identificar al sospechoso.

Servidor Firewall



El servidor de firewall garantiza en un 99% que los ataques que se sufran de manera externa serán contenidos y repelidos; pero lo más importante alertará al administrador de estos ataques, para tomar acciones de monitoreo.

Se implementarán reglas de filtrado de paquetes diseñadas, exclusivamente para el **CLIENTE**, de acuerdo a la nueva topología de seguridad.

Se podrá hacer redirección de puertos a servidores internos para balancear la carga dependiendo el servicio.

Se mantendrá un control total sobre los protocolos y puertos que se estén ejecutando sobre la red del **CLIENTE.**

Se manejará la política, por default, DROP tanto en INPUT, OUTPUT y FORWARD hacia las diferentes subredes.

Soporta una velocidad de procesamiento de paquetes de hasta 155 Mbps.

Permitirá dar acceso exclusivo por servicio, protocolo, aplicación a todos los usuarios

Servidor WEB

Carga del sitio Web corporativo en este servidor.

Se implementará un servidor Web seguro para proyectar al **CLIENTE** a aplicaciones presentes o futuras que necesiten acceso desde el INTERNET y hacia la misma, convergiendo en una INTRANET, para facilitar los servicios que presente.

El tráfico será cifrado en ambas vías.

Soporta aplicaciones PHP y JSP dependiendo de la necesidad del cliente, y sobre todo sin tener un costo económico adicional por licenciamiento

Se instalará una consola centralizada basada en Web para poder administrar, en cada servicio, Proxy, Firewall, VPN entre otras.

Servidor Mail

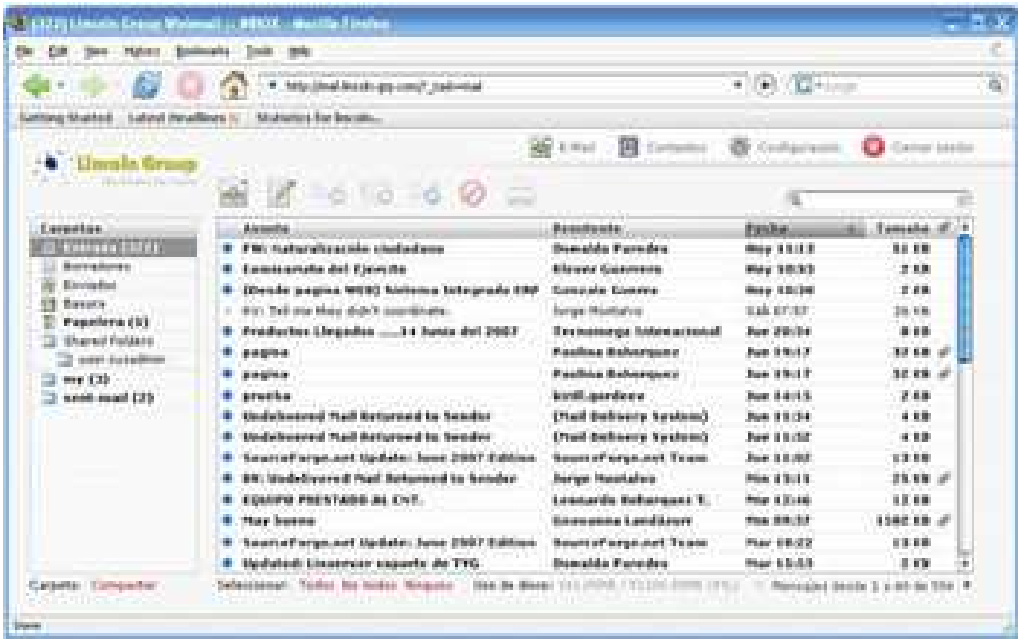
Debido a los problemas que se encuentran actualmente en el INTERNET sobre los correos no deseados, virus, límite de espacio en disco, spam, etc., se implementará un servidor SMTP e IMAP basado en Cyrus con capacidad de procesamiento sobre los 100 mil correos diarios, límite de espacio controlado para usuarios, límite de envío de correos, manejo de las colas remotas y/o locales.

Control de archivos por extensiones y contenido. Evitando que ciertas personas, grupos de usuarios o toda la base de usuarios; cualquiera que sea el caso tengan restricciones de envío de archivos de música, video, ejecutables de Windows, etc.

Servidor Antispam, Antispoof y Antirelay

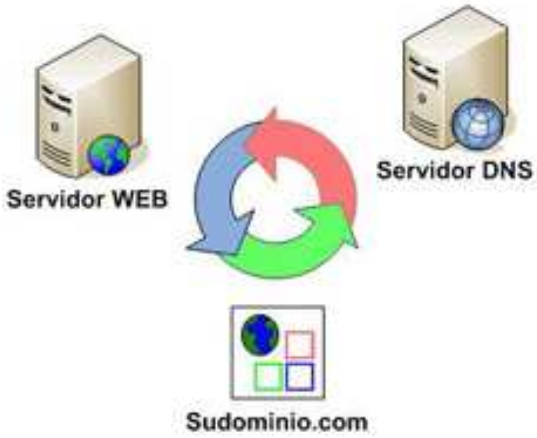
Bloqueo de direcciones usurpadas hacia la empresa, así como una correcta configuración para evitar problemas de Relay no autorizado y evitar estar en listas negras RBL y dejar de recibir correo. Hoy en día es común este tipo de ataques que llegan a molestar a los usuarios, por lo que el servidor lleva un filtrado de correo no deseado (SPAM), llegando a un 99% de efectividad gracias a los métodos matemáticos y heurístico empleados para este tipo de filtrado.

Servidor Webmail



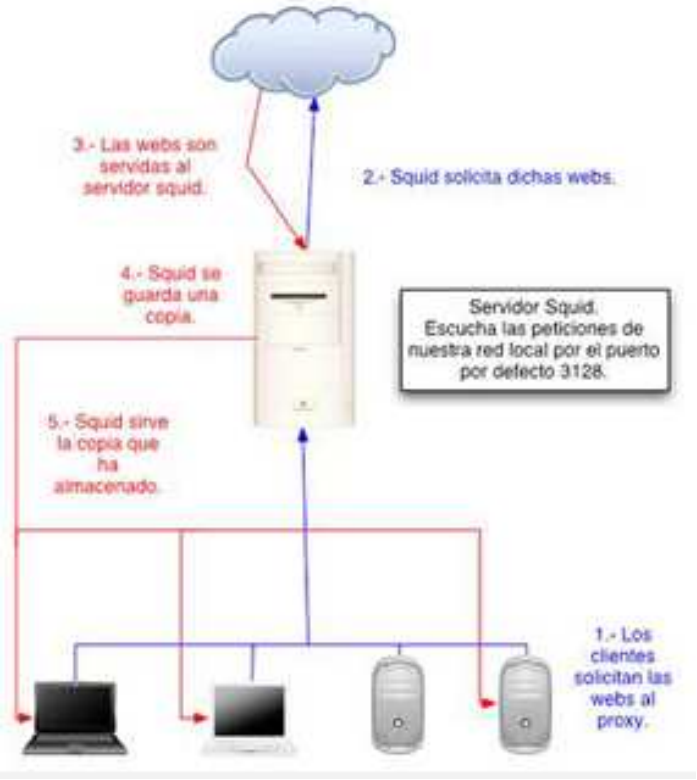
El personal del **CLIENTE** podrá revisar su correo de manera segura (cifrada) desde cualquier parte del mundo a través de una interfaz Web, permitiendo fácil movilidad del personal. Esto de una manera muy rápida y liviana.

Cache DNS



Para evitar consumo innecesario de ancho de banda cuando se realizan consultas DNS, se instalará un cache local de DNS, usando de mejor manera dicho canal.

Cache de páginas Web-Proxy



Para poder realizar control en la navegación de los usuarios hacia el INTERNET ya sea desde la red local o desde otras sucursales, evitando descargas excesivas, descargas duplicadas, navegación fuera de horas, etc., se implementará un servidor Proxy, el cual permitirá de igual modo optimizar el ancho de banda y realizar una navegación más rápida. Se podrá realizar el control del uso de Ancho de Banda por cada usuario o grupo de usuarios, asignándoles a c/u su respectiva velocidad.

Se obtendrán reportes diarios, semanales, mensuales y anuales de la navegación por usuario para poder bloquear accesos no autorizados.
El sistema Proxy viene con un sistema de base de datos de páginas no permitidas en un ámbito mundial, la misma que se actualiza automáticamente facilitando al administrador en su trabajo.

Control de Navegación por Usuarios

Se puede controlar la navegación por los siguientes ítems:

- Horarios.
- Direccionamiento IP.
- Direcciones MAC.
- Acceso y Bloqueo a páginas Permitidas y/o Prohibidas.
- Número de conexiones.
- ACLs.
- Bloqueo de descargas de archivos puntuales (mp3, mov, etc.). Esto permite controlar que el ancho de banda sea usado para los fines que son destinados. Evita descargas de música, archivos de video, etc.
- Validación por Claves.
- Entre otros.

En este ítem se debe tener en cuenta las reglas y políticas de navegación pueden ser usadas de manera que se combinen las características es decir por ejemplo: En horario de 8h00-20h00 los usuarios del grupo operador 1, no pueden realizar descargas de ningún tipo, fuera de él pueden realizar descargas a 2kbps, excepto de archivos de música y videos.

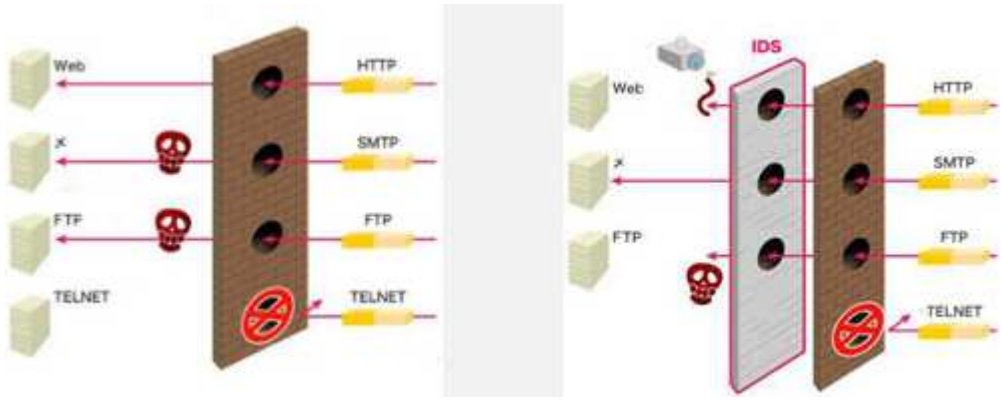
Reportes de Navegación

Topsites
Sites y Usuarios
Bajados

NUM	USERID	CONEXION	BYTES	%BYTES	ENTRADA	CACHE	SALIDA	TIEMPO UTILIZADO	MILISEC	%HORA
1	ADQUISICIONESN.cntt.local	1.93K	327.21M	38.23%	0.05%	99.95%	00:00:00		0	0.00%
2	192.168.34.120	1.92K	91.46M	10.69%	0.32%	99.68%	00:00:00		0	0.00%
3	192.168.34.186	872	57.24M	6.69%	1.05%	98.95%	00:00:00		0	0.00%
4	INFORMATICA11.cntt.local	7.52K	37.09M	4.33%	2.15%	97.85%	00:00:00		0	0.00%
5	192.168.34.106	5.04K	35.03M	4.09%	3.91%	96.09%	00:00:00		0	0.00%
6	ADMINISTRATIVO5.cntt.local	4.70K	34.87M	4.07%	0.00%	100.00%	00:00:00		0	0.00%
7	archivos6.cntt.local	447	22.88M	2.67%	0.29%	99.71%	00:00:00		0	0.00%
8	DEVELOPER1.cntt.local	1.52K	22.73M	2.66%	0.47%	99.53%	00:00:00		0	0.00%
9	CONTRALORIA.cntt.local	2.63K	22.03M	2.57%	0.31%	99.69%	00:00:00		0	0.00%
10	192.168.34.151	4.90K	18.32M	2.14%	1.13%	98.87%	00:00:00		0	0.00%
11	cfinanciero1.cntt.local	155	17.29M	2.02%	0.15%	99.85%	00:00:00		0	0.00%
12	192.168.34.80	84	17.16M	2.00%	0.23%	99.77%	00:00:00		0	0.00%
13	OPNACIONALES3.cntt.local	791	16.60M	1.94%	3.98%	96.02%	00:00:00		0	0.00%
14	informatica10.cntt.local	903	16.45M	1.92%	0.00%	100.00%	00:00:00		0	0.00%
15	192.168.34.152	1.41K	15.65M	1.83%	1.43%	98.57%	00:00:00		0	0.00%
16	rhumanos1.cntt.local	852	12.34M	1.44%	2.71%	97.29%	00:00:00		0	0.00%
17	192.168.34.106	2.54K	11.04M	1.29%	1.25%	98.75%	00:00:00		0	0.00%
18	TINTERNACIONAL1.cntt.local	4.49K	9.76M	1.14%	0.73%	99.27%	00:00:00		0	0.00%
19	archivos8.cntt.local	497	7.60M	0.88%	7.73%	92.27%	00:00:00		0	0.00%

Una vez implementado los controles evidentes, se pueden producir excepciones a las reglas debido a un abuso de confianza con el personal, niveles de acceso, entre otros, el servidor contará con reportes de la navegación para continuar el bloqueo pero de manera específica, sacar reportes diarios, semanales y mensuales para estadísticas, etc.

Sistema Automático Detección, Prevención Intrusos (IDS/IPS)



El sistema automático de detección de intrusos sirve para detectar ataques de cualquier segmento de red en tiempo real, mostrando estadísticas completas de los mismos, así como alertas.

Permite personalizar el acceso por usuarios

Permite que el sistema tome decisiones en tiempo real para bloquear cualquier tipo de ataque que se haya detectado.

Políticas Corporativas de Seguridad LAN (Dominio de Red)

El servidor permite manejar un dominio de red seguro y confiable bajo los mismos criterios que los productos de Microsoft Windows 2000 y 2003 Server lo hacen, salvo que de manera gratuita y mucho más ligera. Esto permite usar el mismo usuario y clave en el mail y en el dominio de red.

Permite crear todas las políticas de seguridad interna como:

Grupos de Trabajo por Departamento.

Asociar un IP determinado a cada máquina de la red.

Identificando por MAC Address a las máquinas de la red.

Eliminar los archivos compartidos de las máquinas de la red.

Utilizar un File Server de Directorios en el Servidor con control de usuarios y permisos. Ejemplo: Directorio Contabilidad.

Accesos a máquinas de la red con permisos y seguridad de Auditoría.

Monitorear desde la matriz cualquier máquina de la red, incluso en las sucursales.

Manejar remotamente cualquier máquina de la red, incluso en las sucursales.

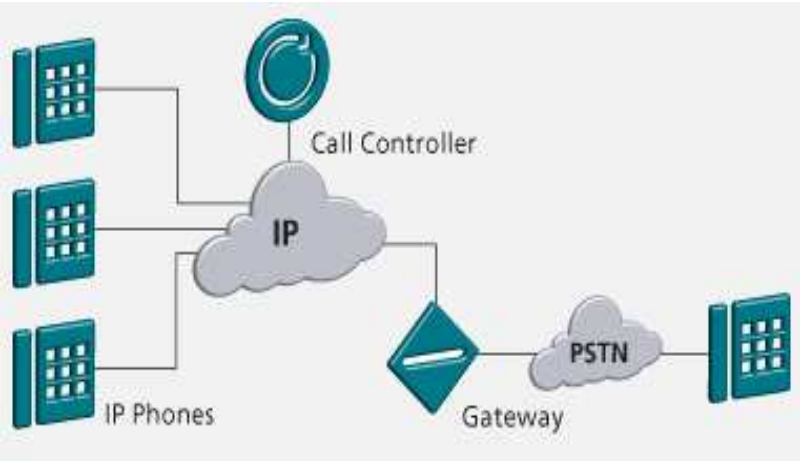
Alertar al administrador si existe violaciones de seguridad de un funcionario en específico a las políticas de calidad.

Guardar configuraciones predeterminadas para los usuarios del dominio en el servidor.

File Server, Shared Files, Volumenes

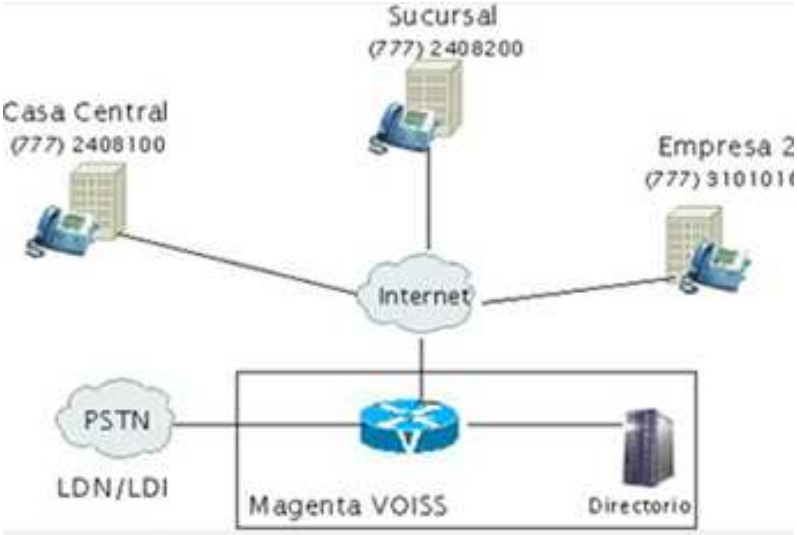
Manejo seguro de volúmenes y archivos compartidos en la red. El servidor puede disponer espacio en disco accesible por los usuarios de la red tanto remotamente como de manera local incluyendo permisos de lectura, escritura, etc., sobre los archivos por usuario.

Voz sobre IP



Voz sobre el protocolo de Internet que permite el enrutamiento de conversaciones de voz sobre el Internet, lo que le permitirá realizar llamadas a muy bajo costo lo que le permitiría la principal ventaja de bajar sus costos operativos.

Manejo de Centrales Telefónicas



A través de **LINSERVER UNIVERSAL CORPORATE NETWORKING CENTER** se puede realizar el manejo digital y centralizado de una central telefónica digital. Este servicio permite administra la central de manera remota o local y de manera segura todos los servicios que dispone la central.

Consola Web Enable de Administración

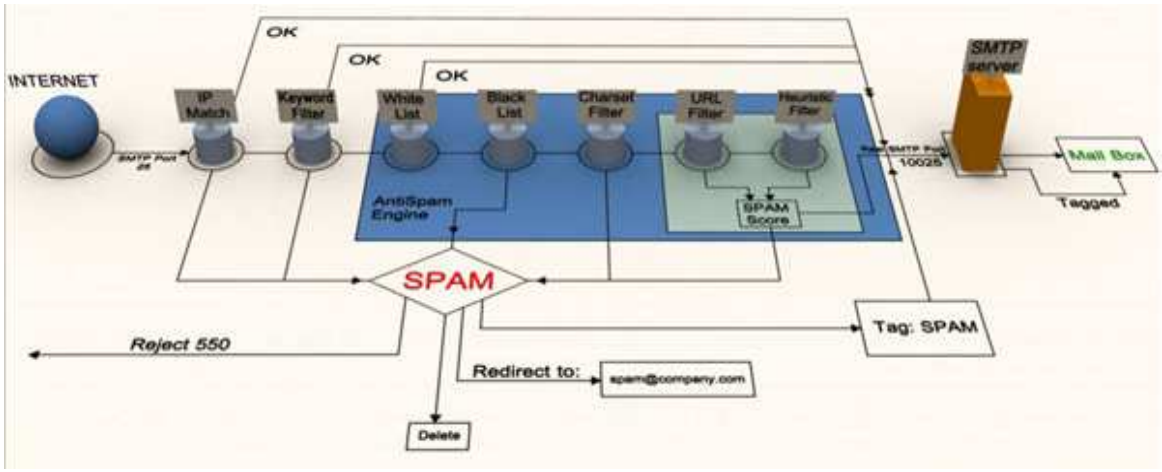
LINSERVER UNIVERSAL CORPORATE NETWORKING CENTER es un producto desarrollado para ser administrado por un usuario sin conocimientos de computación; la idea se basa en un centro de administración web con pantallas gráficas y amigables para desarrollar tareas de administración básica y avanzada. Crear usuarios nuevos, dar permisos de navegación de Internet, establecer cuotas de correo, crear grupos de usuarios en el dominio de red local, establecer permisos de acceso sobre un directorio, crear políticas de uso de los recursos de red, alias de correo electrónico, direcciones de reenvío de correo, monitorear equipos de la red, establecer túneles de comunicación virtual entre puntos remotos, monitoreo de servidores de comunicación, de Bases de Datos, etc., manejo y administración de impresoras de red, asignación automática de IP's dentro de la red entre las más comunes tareas que no requieren el más mínimo conocimiento técnico.

Antivirus

A través de **LINSERVER UNIVERSAL CORPORATE NETWORKING CENTER,** Usted adquiere una solución completa la misma que como parte del costo trae instalado y licenciado un Antivirus para su servidor de correo que lo protege de manera eficiente de todos aquellos archivos o correos que se envíen desde y hacia el servidor de correo que contengan algún tipo de virus o de señal maliciosa

La licencia del Antivirus está incluida en el precio de la solución, sin límite de usuarios, misma que con el pago del mantenimiento no tendrá en el futuro pago de costos de adicionales por renovación. La garantía en el escaneo de los correos de nuestro antivirus es del 99% de seguridad.

Antispam

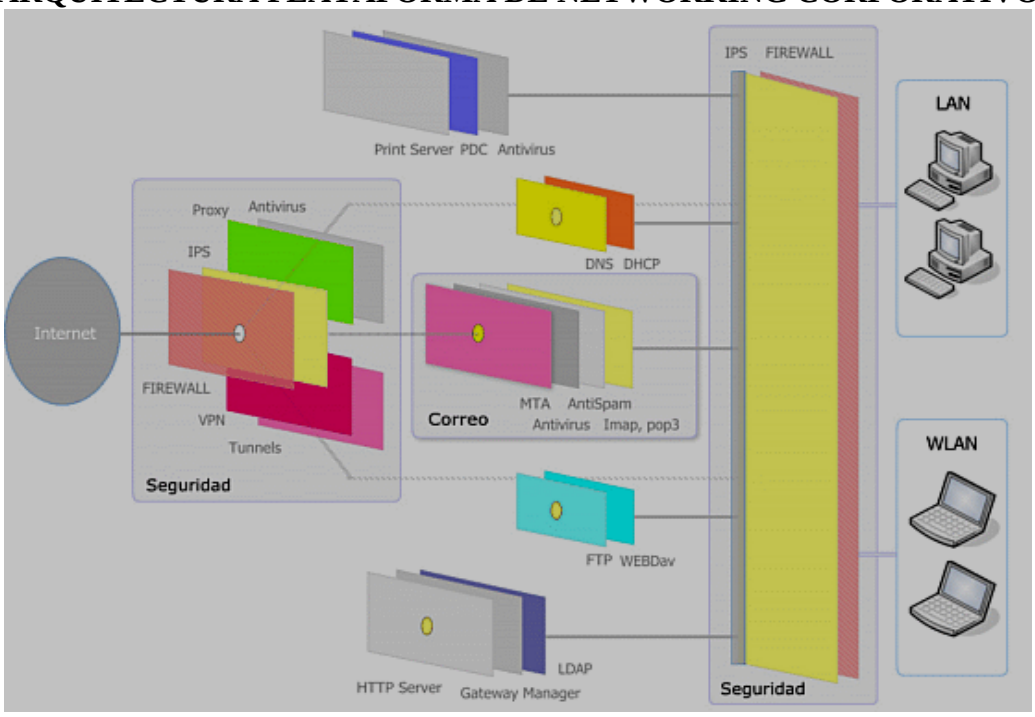


LINSERVER UNIVERSAL CORPORATE NETWORKING CENTER, posee instalado y licenciado un poderoso Antispam dentro de la solución el mismo que bloquea el ingreso de todos los correos que son Spam que llegan al servidor.

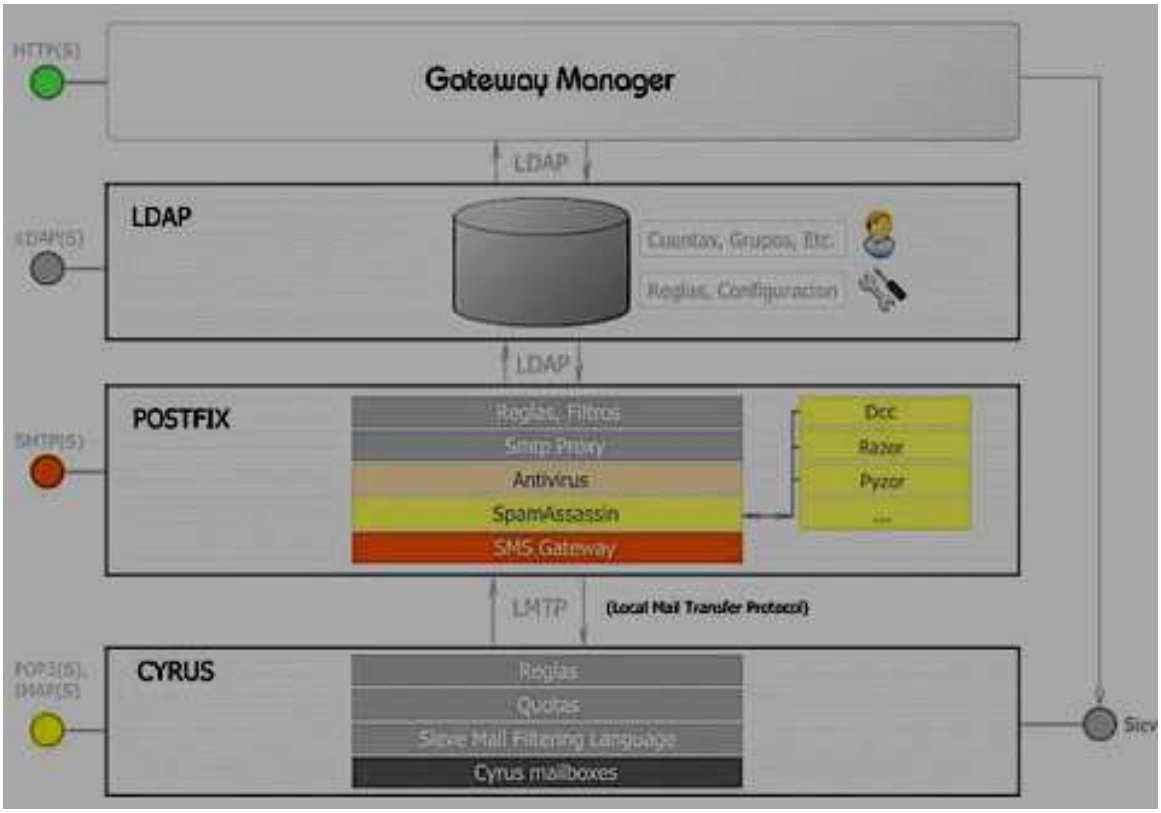
La licencia del Antispam se encuentra incluida dentro de la solución ofertada, sin límite de usuarios, y sin costos de recargo adicionales por renovación o actualización de versiones.

La garantía de que el servidor de correo no filtre un mail de Spam a una cuenta del mismo es del 99%.

ARQUITECTURA PLATAFORMA DE NETWORKING CORPORATIVO



ARQUITECTURA MAIL SERVER


HTTP(S)
Gateway Manager
LDAP
LDAP(S)
LDAP
Cuentas, Grupos, Etc.
Reglas, Configuracion
LDAP
SMTP(S)
POSTFIX
Reglas, Filtros
Smtp Proxy
Antivirus
SpamAssassin
SMS Gateway
Dcc
Razor
Pyzor
...
LMTP
(Local Mail Transfer Protocol)
POP3(S),
IMAP(S)
CYRUS
Reglas
Quotas
Sieve Mail Filtering Language
Cyrus mailboxes