UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

"SEGURIDAD PERIMETRAL Y SEGMENTACIÓN LÓGICA EN LA RED DE DATOS DEL INSTITUTO TECNOLÓGICO SUPERIOR JOSÉ CHIRIBOGA GRIJALVA DE LA CIUDAD DE IBARRA"

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTORA: NORA ANGÉLICA PUERRES TREJO

DIRECTOR: ING. EDGAR MAYA

IBARRA-ECUADOR

2017

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1.- IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DEL CONTACTO	
Cédula de Identidad	0401453022
Apellidos y Nombres	Puerres Trejo Nora Angélica
Dirección	Urbanización Obando Luna, Calle Armando Hidrobo
E-mail	napuerrest@utn.edu.ec
Teléfono Fijo	062 -2977679
Teléfono Móvil	0992129668
DATOS DE LA OBRA	
Título	"SEGURIDAD PERIMETRAL Y SEGMENTACIÓN LÓGICA EN LA RED DE DATOS DEL INSTITUTO TECNOLÓGICO SUPERIOR JOSÉ CHIRIBOGA GRIJALVA DE LA CIUDAD DE IBARRA."

Autor	Puerres Trejo Nora Angélica
Fecha	Martes 20 de junio del 2017
Programa	Pregrado
Título por el que se aspira:	Ingeniería en Electrónica y Redes de Comunicación
Director	Ing. Edgar Maya

2.- AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Y SEGMENTACIÓN LÓGICA EN LA RED DE DATOS DEL INSTITUTO

Yo, NORA ANGÉLICA PUERRES TREJO, con cédula de identidad Nro. 040145303-2, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior artículo 144.

3.- CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad Técnica del Norte en caso de reclamación por parte de terceros.

Ibarra, 20 de junio del 2017

.....

Nora Angélica Puerres Trejo

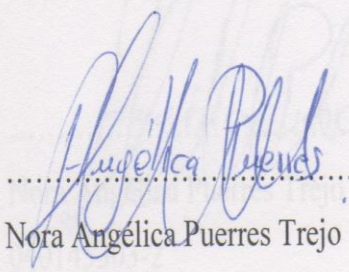
040145303-2

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, NORA ANGÉLICA PUERRES TREJO, con cédula de identidad Nro. 040145303-2, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de grado denominado: "SEGURIDAD PERIMETRAL Y SEGMENTACIÓN LÓGICA EN LA RED DE DATOS DEL INSTITUTO TECNOLÓGICO SUPERIOR JOSÉ CHIRIBOGA GRIJALVA DE LA CIUDAD DE IBARRA.", que ha sido desarrollado para optar el título de Ingeniería en Electrónica y Redes de Comunicación, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos concedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, 20 de junio del 2017



.....

Nora Angélica Puerres Trejo

040145303-2

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Nora Angélica Puerres Trejo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte

.....

Nora Angélica Puerres Trejo
040145303-2

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico que la Tesis "SEGURIDAD PERIMETRAL Y SEGMENTACIÓN LÓGICA EN LA RED DE DATOS DEL INSTITUTO TECNOLÓGICO SUPERIOR JOSÉ CHIRIBOGA GRIJALVA DE LA CIUDAD DE IBARRA." ha sido realizada en su totalidad por la señorita: NORA ANGÉLICA PUERRES TREJO portadora de la cédula de identidad numero: 040145303-2

.....

Ing. Edgar Maya

Director de Tesis

AGRADECIMIENTO

Nunca dejes a Dios por fuera de tus proyectos, es parte de la clave del éxito

Anónimo

Mi agradecimiento con mi alma entera a mis padres: Elías Puerres e Inés Trejo por su amor incondicional, y por regalarme la mejor herencia de todas, mi educación.

A mi director de tesis el Mg. Edgar Maya director de tesis, por su paciencia y conocimiento para alcanzar esta meta académica.

Al Instituto Tecnológico Superior José Chiriboga Grijalva, por la apertura necesaria para desarrollar el tema de titulación, en especial al Ingeniero Jorge Acosta Director de Sistemas del instituto y al Ingeniero Hugo Narváez administrador de la red.

Gracias infinitamente.

DEDICATORIA

Las decisiones de Dios son misteriosas, pero siempre son a nuestro favor.

Anónimo

Este proyecto de tesis se lo dedico a mi padre Elías por ser mi fuente de inspiración diaria. De lucha y trabajo, a mi madre Inés por ser una guerrera de vida por despertar cada día y vencer al dragón.

A mi hermana Lilia Puerres, por ser un ejemplo de superación, a la luz de mis ojos mi alegría mis sobrinas, Doménica y Bianca.

Con amor Nora.

CONTENIDO

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE ii
CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE iv
DECLARACIÓN v
CERTIFICACIÓN vi
AGRADECIMIENTO vii
DEDICATORIA viii
CONTENIDO ix
RESUMEN xvii
ABSTRACT xviii
CAPITULO I i
1 Presentación 1
1.1 Problema. 1
1.2 Objetivos. 3
1.3 Alcance. 4
1.4 Justificación 5
1.4 Contexto de la Institución 7
CAPITULO II 9
2. Fundamentos teóricos de seguridad de redes y seguridad perimetral 9
2.1 Redes de Datos 9
2.2 Dispositivos de la Red de Datos. 19
2.3 Seguridad perimetral 25
2.4 Componentes de la seguridad perimetral. 25
2.5 Sistema de Detección y Prevención de intrusos. 30
2.6 Fundamentos de seguridad en redes 31
2.7 Segmentación de redes. 34
2.8 Red de área local virtual (VLANs). 35
2.9 Técnicas y métodos de investigación para la evaluación del riesgo. 37
CAPÍTULO III 40
3. Evaluación de la situación actual de la red de datos 40
3.1 Instituto Tecnológico Superior “José Chiriboga Grijalva”. 40

3.2 Situación actual de la red de datos del Instituto Tecnológico Superior "José Chiriboga Grijalva". 44
3.3 Descripción de la topología de red del Instituto Tecnológico Superior "José Chiriboga Grijalva" 47
3.4 Descripción de la topología de red. 49
3.5 Especificaciones técnicas de los equipos de Networking. 53
CAPÍTULO IV 62
4 Análisis de riesgos en base a la metodología NIST SP 800 - 30 62
4.1 Importancia del Análisis del riesgo. 62
4.2 Pasos de la metodología de evaluación del riesgo según la Guía NIST SP 800 - 30 64
4.3 Desarrollo de la metodología de evaluación del riesgo según la Guía NIST SP 800 - 30 para la red de datos del Tecnológico ITCA. 69
4.4 Evaluación y control del riesgo 83
4.5 Determinación de amenazas y de las acciones de la amenaza 87
4.6 Resultado de la evaluación del riesgo 90
4.7 Acciones de mitigación del riesgo 93
4.8 Conclusiones finales de metodología de evaluación del riesgo según la Guía NIST SP 800 - 30 para la red de datos del Tecnológico ITCA. 124
CAPITULO V 127
5 Diseño e implementación del sistema de seguridad perimetral en la red del instituto 127
5.1 Análisis de los tipos de firewall. 127
5.2 Políticas de seguridad en la red. 130
5.3 Descripción y selección del software para el desarrollo del diseño del sistema de seguridad Perimetral. 131
5.5 Distribución lógica de la red del Tecnológico ITCA 135
5.6 Diseño del sistema de Seguridad Perimetral. 138
5.7 Configuración de los equipos del sistema de seguridad perimetral para la red de datos del tecnológico ITCA. 139
5.8 Implementación real del firewall Pfsense en la red del Tecnológico ITCA 159
5.9 Implementación real del servidor de dominio de nombres y gateway en la red del Tecnológico ITCA 161

5.10 sistema de prevención de intrusos (IPS). 166
CAPITULO VI..... 170
6 Pruebas de verificación y funcionamiento del sistema de seguridad perimetral. 170
6.1 Pruebas del servicio Squid 170
6.2 Ataque de envenenamiento a la red, mediante ataque hombre en el medio, utilizando kali-linux 173
CAPITULO VII..... 185
7 Conclusiones y recomendaciones..... 185
7.1 Análisis económico 185
7.2 Conclusiones 191
7.3 Recomendaciones..... 194
7.4 Bibliografía..... 196

ÍNDICE DE TABLAS

Tabla 1. Direccionamiento IP versión 4 12
Tabla 2. Resumen de protocolos más utilizados 19
Tabla 3. Número de personal del ITCA 42
Tabla 4. Número de estudiantes ITCA 42
Tabla 5. Direccionamiento IPs Públicas 50
Tabla 6. Distribución de Switch Rack 1 51
Tabla 7. Distribución de Switch Rack 2 51
Tabla 8. Distribución de Switch Rack 2 52
Tabla 9. Distribución del direccionamiento IP de los servidores 53
Tabla 10. Especificaciones técnicas del Router 1900 54
Tabla 11. Especificaciones técnicas del Router 881 55
Tabla 12. Especificaciones técnicas del switch 2950 56
Tabla 13. Especificaciones técnicas del Switch SG300-28 57
Tabla 14. Especificaciones técnicas del Switch SG200-26 58
Tabla 15. Escala de valoración del factor Confidencialidad, Integridad y disponibilidad de los activos de información 71
Tabla 16. Rangos de Importancia de los activos de información. 72
Tabla 17. Caracterización de los Routers de comunicación. 73
Tabla 18. Caracterización de los switch de comunicación 73
Tabla 19. Caracterización de los servidores de la red 75
Tabla 20. Caracterización de los host de usuarios 76
Tabla 21. Caracterización de los host de administrativos 77
Tabla 22. Estado de la probabilidad de amenazas 79
Tabla 23. Definición de la magnitud del impacto 80
Tabla 24. Matriz del nivel de riesgo 81
Tabla 25. Cálculo de Nivel de Importancia para el activo equipos y redes de comunicación 83
Tabla 26. Cálculo de Nivel de Importancia para el activo servidores de la red. 85
Tabla 27. Cálculo de Nivel de Importancia para el activo host de usuarios 86
Tabla 28. Cálculo de Nivel de Importancia para el activo host de administrativos 86
Tabla 29. Cálculo de Nivel de Importancia para el activo recurso humano 87
Tabla 30. Determinación de amenazas e impacto 88

Tabla 31. Evaluación de amenazas/vulnerabilidades 90
Tabla 34. Controles mitigadores para el activo equipos de redes y comunicación. 94
Tabla 35. Controles mitigadores para el activo servidores de la red 100
Tabla 36. Controles mitigadores para el activo host de usuario. 106
Tabla 37. Controles mitigadores para el activo host de administrativos 112
Tabla 38. Controles mitigadores para el activo Recurso humano. 118
Tabla 39. Servicios de Pfsense 134
Tabla 40. Distribución de las Vlans para la segmentación lógica 136
Tabla 41. Distribución de las IP de la Vlan 2 137
Tabla 42. Direccionamiento del diseño de red 139
Tabla 43. Resumen de la configuración de las Vlans 141
Tabla 44. Direccionamiento de la implementación firewall Pfsense 159
Tabla 45. Costo de la infraestructura existente en el tecnológico ITCA 186
Tabla 46. Comparación de los servidores HP Proliant 187
Tabla 47 herramientas necesarias para la instalación de infraestructura 188
Tabla 48 costo estimado de ingeniería e instalación 189
Tabla 49 detalle total del costo estimado.....189

ÍNDICE DE FIGURAS

Figura 1. Ubicación Instituto Tecnológico Superior “José Chiriboga Grijalva”.....8
Figura 2. Estructura de la dirección física o MAC.....10
Figura 3. Procesos de resolución de direcciones para una red local.....14
Figura 4. Procesos de resolución de direcciones para una red remota 16
Figura 5. Conexión de un Hub.....20
Figura 6. Interconexión de dos segmentos de red mediante un Bridge.....21
Figura 7. Interconexión de dispositivos finales mediante un switch. 21
Figura 8. Interconexión de redes hacia la red de Internet mediante un Router capa tres. 22
Figura 9. Interconexión de dispositivos finales mediante un modem 23
Figura 10. Topología de una red típica donde se visualiza la zona de perímetro de red.26
Figura 11. Topología de una red típica donde aísla la zona DMZ del resto de la red. 27
Figura 12. Topología de una red típica donde se visualiza la zona wireless.....27
Figura 13. Topología de una red típica se visualiza la red de área local LAN.....28
Figura 14. Vista del Instituto Técnico Superior “José Chiriboga Grijalva”.....41
Figura 15. Organigrama Estructural General 43
Figura 16. Topología física del Instituto Tecnológico Superior “José Chiriboga Grijalva” 45
Figura 17. Topología lógica del Instituto Tecnológico Superior “José Chiriboga Grijalva” 46
Figura 18. Ubicación del data center en el Instituto Tecnológico Superior “José Chiriboga Grijalva” 47
Figura 19. Router CISCO 1900.....54
Figura 20. Router CISCO Serie 881.....55
Figura 21. Switch cisco 2950 56
Figura 22. Switch CISCO SG300-28 57
Figura 23. Switch CISCO SG200-26 58
Figura 24. Central Telefónica CISCO 560 60
Figura 25. Video Vigilancia HIK VISION.....61
Figura 26. Metodología del análisis de riesgo.....65
Figura 27. Topología del diseño del firewall.....138
Figura 28. Configuración de la red WAN 142

Figura 29. Configuración de la red DMZ 142
Figura 30. Configuración de la red LAN 143
Figura 31.configuración de la Vlan 5 acceso a internet. 143
Figura 32.asignación de la Vlan 5 hacia la red LAN 144
Figura 33. Asignación a las interfaces con la Vlan 5 144
Figura 34.selección de la interfaz LAN 145
Figura 35. Cambio de la interfaz LAN por la Vlan 5 146
Figura 36. Asignación de las tarjetas de las redes 147
Figura 37.configuración de una regla NAT 148
Figura 38. Habitación de puertos para el NAT 149
Figura 39. Habilitación de proxy Squid 150
Figura 40.descarga de la lista negra 151
Figura 41.Bloqueo de páginas no deseadas 151
Figura 42. Bloqueo por dominio de las redes sociales 152
Figura 43. Bloqueo de las descargas 153
Figura 44.creación de la lista de acceso ACL 154
Figura 45. Bloqueo de la páginas de redes sociales. 155
Figura 46. Bloqueo de la páginas para descargas 155
Figura 47. Bloqueo de la páginas pornográficas 156
Figura 48. Inicialización del servicio proxy Squid 157
Figura 49. Reglas del firewall para la red WAN 158
Figura 50. Reglas del firewall para la red LAN 158
Figura 51. Reglas del firewall para la red DMZ 159
Figura 52. Configuración de interfaz LAN 160
Figura 53. Configuración de interfaz WAN 160
Figura 54. Configuración de interfaz DMZ 161
Figura 55. Servidor DNS para el firewall real 162
Figura 56. Habilitación del NAT en Firewall real 163
Figura 57. Reglas del firewall para la red WAN 164
Figura 58. Reglas del firewall para la red LAN 164
Figura 59. Reglas del firewall para la red LAN 165
Figura 60.saturación del servidor firewall Pfsense implantado 166
Figura 61.instalación del software Snort 167
Figura 62. Creación de la lista de direcciones IP en Snort. 167

Figura 63. Servicio de Snort no inicializado 168
Figura 64. Servicio de Snort inicializado 168
Figura 65. Reglas de Snort seleccionadas 169
Figura 66. Reglas de Snort seleccionadas (continuación) 169
Figura 67.acceso exitoso a Google 171
Figura 68. Restricción a la página de Facebook 171
Figura 69. Restricción a la página de vide youtube 172
Figura 70. Restricción a la página pornografica 172
Figura 71. Restricción a la página de descargar softonic 173
Figura 72 muestra la ejecución del comando de ettercap en Kali Linux 174
Figura 73 selecciona la opción para empezar con la escucha 174
Figura 74 Selección de la tarjeta de red 175
Figura 75 Selección del host para escanear 175
Figura 76 Selección del host para escanear 176
Figura 77 lista de los host escaneados 176
Figura 78 Selección del host y la dirección IP 177
Figura 79 Firewall Pfsense como objetivo 2 177
Figura 80. Objetivo 2 Pfsense 178
Figura 81 Activación del sniffer remoto 178
Figura 82 Activación del envenenamiento 179
Figura 83 Activación de drifnet para la interfaz 179
Figura 84 . Alertas generadas por Snort donde no ha sido posible el envenenamiento 180
Figura 85 Resumen de Snort donde no ha sido posible el envenenamiento 180
Figura 86 . Selección del archivo slowloris para realizar el ataque 181
Figura 87 se inicializa el envio de peticiones mediante slowloris 182
Figura 88 Envio de paquetes mediante slowloris 182
Figura 89 Envio de paquetes mediante slowloris 183
Figura 90 Firewall Pfsense es accesible después del ataque 183
Figura 91 Alertas generadas por Snort IPS 184
Figura 92 Resumen de las alertas generadas por el ataque DOS 184

RESUMEN

El proyecto de titulación se basa en el diseño e implementación de un Sistema de Seguridad Perimetral para la red de datos del Instituto Tecnológico Superior "José Chiriboga Grijalva " de la ciudad de Ibarra, con el objetivo primordial de mejorar la seguridad de la información en la institución educativa .

Como inicio del desarrollo del Sistema de Seguridad Perimetral, se realiza el levantamiento de la información de los activos informáticos físicos y lógicos de la institución con el objetivo primordial de evidenciar directamente la situación actual de red de datos , de esta manera se obtendrá las vulnerabilidades y amenazas, a las que se encuentra sometida la red lógica , con este antecedente se realiza el estudio del análisis de riesgo donde se utilizara la Guía del Instituto Nacional de estándares y tecnología NIST SP 800-30, y describir puntualmente los niveles actuales de seguridad de la información.

La parte de implementación del sistema de Seguridad Perimetral consta básicamente de la configuración del firewall en software libre, donde se definen las políticas de acceso o restricción que permita una defensa ante los ataques que puedan suscitarse en la red de datos, además la implementación y configuración del IPS y finalmente la creación de VLANs necesarias y que se ajusten a las necesidades de la red para un correcto funcionamiento de la segmentación lógica.

ABSTRACT

The degree project is based on the design and implementation of a Perimeter Security System for the data network of the Higher Technological Institute “José Chiriboga Grijalva” of the Ibarra city, with the primary objective of improving the information’s security in the educational institution.

As the beginning of the Perimeter Security System development, the information gathering from the physical and logical computer assets of the institution is done, whit the primary objective of directly showing the current data network situation, so the vulnerabilities and threats, to which the logical network is subjected, will be obtained, with this antecedent the study of the risk analysis ,where the National Institute of Standards and Technology Guide, publication especial NIST SP 800-30 is used, is done; and to accurately describe current levels of information security.

The part of the Perimeter Security System implementation basically consists in the firewall configuration in free software, where the access or restriction policies that allow a defense against attacks that may arise in the data network are defined, also the implementation and configuration of the IPS and finally the creation of necessary VLANs that conform to the needs of the network for a correct operation of the logical segmentation.

CAPÍTULO I

1 Presentación

En este capítulo se presenta el modelo de anteproyecto aprobado, el cual contiene la propuesta realizada para la implementación del plan de titulación.

1.1 Problema.

Con la evolución de las redes de datos en los últimos años, se puede evidenciar un crecimiento en el flujo de la información y en los servicios que estas brindan, puesto que son de carácter fundamental y necesario para cualquier tipo de proceso sea este de tipo comercial, gubernamental o educativo. Al encontrarse en estos grandes entornos se involucran el uso de equipos de cómputo u otros dispositivos que permita acceder a las redes de datos, que se encuentran susceptibles a cualquier tipo de ataque sea este de sustracción, falsificación o modificación de la información, denegación de servicios en las instituciones lo que conllevaría a pérdida de información y en algunos casos, perdidas económicas.

El desarrollo y crecimiento del Instituto Tecnológico Superior José Chiriboga Grijalva ITCA, han permitido que su infraestructura tecnológica, crezca en gran medida, la misma que cuenta con una capacidad de acceso a Internet de 16 Mbps y una red de datos con direccionamiento IPv4 clase B, estructurada a través de un Cableado Estructurado tanto de Fibra Óptica Furukawa 10gigabit dúplex optical, como también Cable UTP Categoría

6, los cuales se rigen en las normativas: EIA/TIA-568B. A su vez su Data Center se encuentra constituido por equipos Cisco tales como un Router HP A-MSR 900 perteneciente a TELCONET, un Router Cisco 881, un Switch Cisco 2950 capa 3, seis Switch SG200-26 y ochp Switch SG300-28, también contiene una Central 500 FXO de Voz IP, como también una Central HIK VISION de Cámaras IP además de ocho Servidores los cuales contienen grandes cantidades de información de suma importancia. A su vez cuenta con seis sistemas administrativos, una plataforma virtual en Moodle, cinco laboratorios informáticos y un espacio dedicado para libre acceso a consultas académicas para los estudiantes.

Actualmente el Instituto ITCA cuenta con una infraestructura de red funcional, pero no posee un buen sistema de seguridad para dicha red, por lo que se encuentra vulnerable ante ataques informáticos, de manera interna y externa; carece de una buena segmentación lógica que permita generar un mayor control de los accesos permitidos y denegados a determinada información, por lo cual el departamento de tecnología de la Institución ha visto urgente la implementación de un sistema de seguridad que proteja su red de datos.

Ante el crecimiento inminente de la red de datos del Instituto Tecnológico Superior José Chiriboga Grijalva, aumenta también la necesidad de mantener dicha red bajo ciertos parámetros de seguridad, que se ajusten a los requerimientos sugeridos por parte de las autoridades del Instituto, pero sobre todo a lo que la propia red requiera, para que su funcionamiento pueda desarrollarse de manera eficiente sin sufrir efectos de ataques informáticos, e implementar un sistema de seguridad a nivel perimetral para solucionar los problemas de vulnerabilidad de la red.

1.2 Objetivos.

1.2.1 Objetivo General.

Mejorar el esquema de Seguridad Perimetral en la red de datos del Instituto Tecnológico Superior José Chiriboga Grijalva para de esta manera solucionar los problemas incidentes de la seguridad.

Objetivos Específicos.

- Realizar la base teórica de todos los objetos que participan de la seguridad de redes, seguridad perimetral y direccionamiento lógico para la aplicación del proyecto en el Instituto Tecnológico Superior José Chiriboga Grijalva.

- Analizar la situación actual de la red de datos del instituto, para verificar el tipo de segmentación lógica que la infraestructura al momento la red necesita de acuerdo a sus requerimientos.

- Realizar el estudio de amenazas y vulnerabilidades que presenta la red de datos mediante la guía de gestión de riesgos, establecido en la metodología de (National Institute of Estandards and Tecnology Special Publication) NIST SP 800 -30.

- Diseñar el esquema de seguridad mediante un Firewall e IPS (sistema de prevención de intrusos), definiendo las políticas de seguridad y segmentación

lógica de la red con los datos resultantes, en el estudio de la norma NIST-SP 800-30.

- Implementar el sistema de Seguridad Perimetral el cual protegerá los equipos físicos además la creación de VLANs que se ajusten a los requerimientos necesarios de la red de datos del instituto.

- Verificar la funcionalidad del Sistema de Seguridad Perimetral, mediante pruebas de simulación de ataques en la red de datos del instituto.

- Realizar el análisis costo beneficio, conclusiones y recomendaciones obtenidas en desarrollo del plan de tesis.

1.3 Alcance.

El presente proyecto de titulación se basa en el bloqueo de las amenazas que se puedan presentar en la red de datos del Instituto Tecnológico Superior José Chiriboga Grijalva mediante la implementación de un Firewall basado en software libre además de la ejecución de políticas de seguridad y segmentación en base a la construcción de VLANs para la segmentación de la red.

En primera instancia se presenta los fundamentos teóricos, de seguridad de redes y las características para la implementación de la Seguridad Perimetral y la creación de VLANs en la red de datos del instituto.

Se realizará el levantamiento de la información, para evaluar la situación actual de la red de datos del Instituto Tecnológico Superior José Chiriboga Grijalva, de esta manera se obtendrá las vulnerabilidades y amenazas, a las que se encuentra sometida la red física y lógica de la red, esto se lo realizará en base a la metodología de análisis y gestión de riesgos NISTP SP 800-30 que comprende la caracterización de los sistemas, identificación de amenazas y vulnerabilidades y finalmente análisis y control de las mismas.

La parte de implementación del sistema de Seguridad Perimetral consta básicamente de la configuración del firewall, donde se definen las políticas de acceso o restricción que permita una defensa ante los ataques que puedan suscitarse en la red de datos, además la implementación y configuración del IPS y finalmente la creación de VLANs necesarias y que se ajusten a las necesidades de la red para un correcto funcionamiento de la segmentación lógica.

Después de realizar la parte de implementación del sistema de Seguridad Perimetral en la red de datos del Instituto Tecnológico Superior José Chiriboga Grijalva, se realiza un ataque simulado en la red de datos, dónde se verificará la funcionalidad de mismo.

Finalmente se presenta las conclusiones y recomendaciones obtenidas a lo largo del plan de titulación.

1.4 Justificación

Actualmente la red de datos del el Instituto Tecnológico Superior José Chiriboga Grijalva, soporta gran cantidad de información, proveniente de los sistemas y plataformas

que ahí se manejan. Estos sistemas contienen información de suma importancia como son los reportes de calificaciones, pagos generados al personal, facturación, videos provenientes de las cámaras de vigilancia, consultas diarias por parte de los alumnos, entre otros, y al no contar con un sistema de seguridad adecuado la red se encuentra vulnerable ante ataques informáticos con el fin de ocasionar daño a la red.

La implementación de la Seguridad Perimetral para la red de datos del Instituto, garantiza la protección de la red de posibles ataques, obteniendo una red más segura y confiable a nivel interno y externo, además como una base fundamental para la administración de la misma.

Su segmentación y direccionamiento, está enfocado en los requerimientos actuales de la red y las políticas, que en el Instituto y sus autoridades plantean, esto se manejan, en lo que respecta a jerarquías de departamentos para el acceso, delimitando a los diferentes tipos de tráfico que en la red se cursará, ya que, no todos los departamentos tienen los mismos privilegios de acceso total a los datos.

Por esta razón, este proyecto es base fundamental para el crecimiento y desarrollo de la red de datos del Instituto, puesto que, una red que carezca de seguridad es muy difícil implementar otros servicios y aplicaciones que hagan que una red funcione de manera eficiente y eficaz.

La seguridad perimetral propuesta en este proyecto puede ser implementado en el Instituto Tecnológico Superior José Chiriboga Grijalva, ya que su infraestructura de red se encuentra desarrollada y estructurada bajo las siguientes normativas: EIA/TIA-568b.1

cableado para edificios comerciales, EIA/TIA-569 rutas y espacios para cableado estructurado, Además sus equipos dentro de su Data Center admiten el tipo de configuraciones de seguridad como lo indican sus hojas de datos, en las cuales se especifican principalmente los protocolos y tecnologías que soportan.

1.4 Contexto de la Institución

1.5.1 Instituto Tecnológico Superior "José Chiriboga Grijalva"

En la página web del Instituto Tecnológico Superior "José Chiriboga Grijalva" se encuentran descritos los pilares fundamentales de la institución los cuales se indican a continuación.

1.5.2 Misión

El Instituto Tecnológico Superior "José Chiriboga Grijalva", forma profesionales de nivel tecnológico con valores éticos, calidad en el perfeccionamiento de habilidades y destrezas en el saber y hacer, con espíritu emprendedor, que generen soluciones a los problemas y necesidades de la zona uno del país, entorno al desarrollo de la matriz productiva en las áreas de: Educación, Servicios personales, Educación comercial y administración, industria y producción, informática y protección del medio ambiente.

1.5.3 Visión

El Instituto Tecnológico Superior "José Chiriboga Grijalva" en los próximos cinco años será una Institución del Sistema de Educación Superior con reconocimiento y

prestigio en la formación de profesionales de nivel tecnológico, liderando los cambios que requiere la sociedad, fundamentada en los códigos propios de la modernidad, el trabajo en equipo, la sustentabilidad y la práctica de valores.

1.5.4 Ubicación

El Instituto Tecnológico Superior “José Chiriboga Grijalva” se encuentra ubicado en la ciudad Ibarra, entre las calles El Oro y 13 de Abril, como se muestra en la Figura 1.

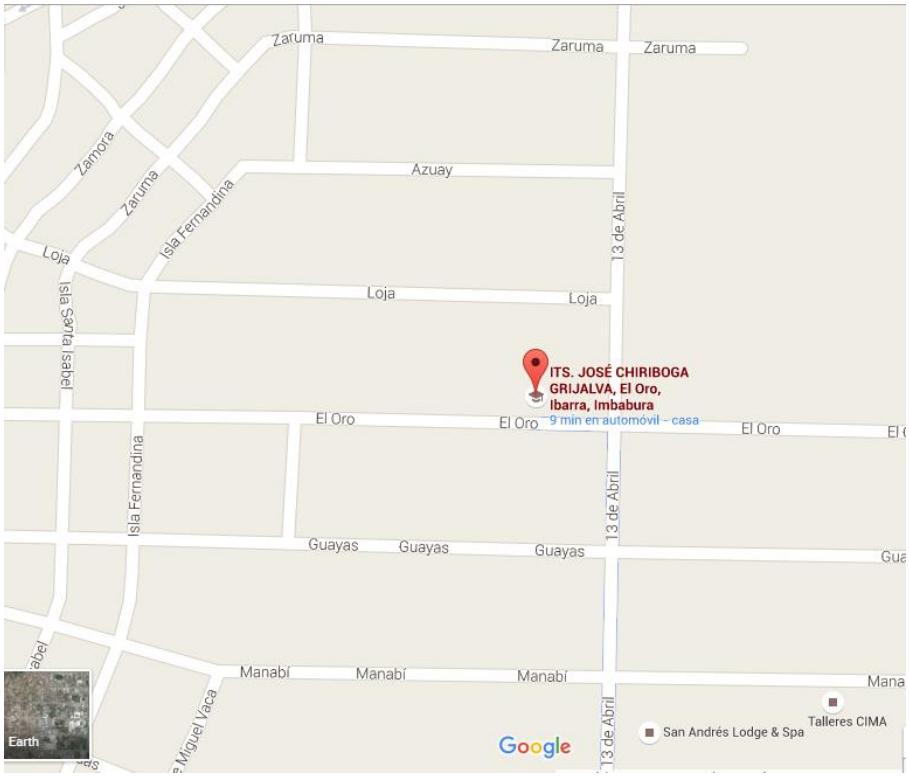


Figura 1. Ubicación Instituto Tecnológico Superior “José Chiriboga Grijalva”

Fuente: Recuperado de https://www.google.com.ec/maps/place/ITS.+JOS%C3%89+CHIRIBOGA+GRIJALVA,+El+Oro,+Ibarra,+Imbabura/@0.3723578,-78.1238652,17z/data=!3m1!4b1!4m5!3m4!1s0x8e2a3b50a373556f:0xa2dcbeffddd2167d!8m2!3d0.3723524!4d-78.1216765

CAPÍTULO II

2. Fundamentos teóricos de seguridad de redes y seguridad perimetral

En este capítulo se analiza los fundamentos teóricos correspondientes a los sistemas de seguridad en redes, características principales de la seguridad perimetral, también los aspectos de prevención de intrusos (IPS) y segmentación de la redes de datos.

2.1 Redes de Datos.

Desde el punto de vista de la computación, una red de datos es un conjunto de computadoras independientes interconectadas física y lógicamente para facilitar el intercambio y procesamiento de la información.

En la actualidad las redes de datos son una indiscutible necesidad en cualquier sector, por lo que cada día se mantendrán en una constante evolución, alcanzando nuevas fronteras, brindan comunicación inmediata casi en cualquier parte de la tierra, esto gracias a la versatilidad de la misma, emplean diferentes medios que se utilizan para su transmisión. Las redes de datos se clasifican con base en su forma de transmisión en redes cableadas e inalámbricas, dentro de éstas existen clasificaciones tomando en cuenta su topología, alcance, medio de transmisión y velocidad. . (Baltazar José, Campuzano Juan, 2011)

2.1.1 Dirección MAC o dirección física

La dirección Mac por sus siglas en ingles “control de acceso al medio” es un identificador único de 48 bits asignada a cada interfaz de red , que identifican a un host en la red universal, también conocida como dirección física que opera en la capa 2 del modelo OSI, permitiendo la comunicación entre dos host conectados directamente. Se conforma de manera especial, seis grupos de dos caracteres hexadecimales, cada uno separado por dos puntos de la siguiente forma: los primeros 24 bits configurados por el IEEE que identifican al fabricante, y los siguientes 24 bits identifican la tarjeta del fabricante, como se indica en la Figura 2.

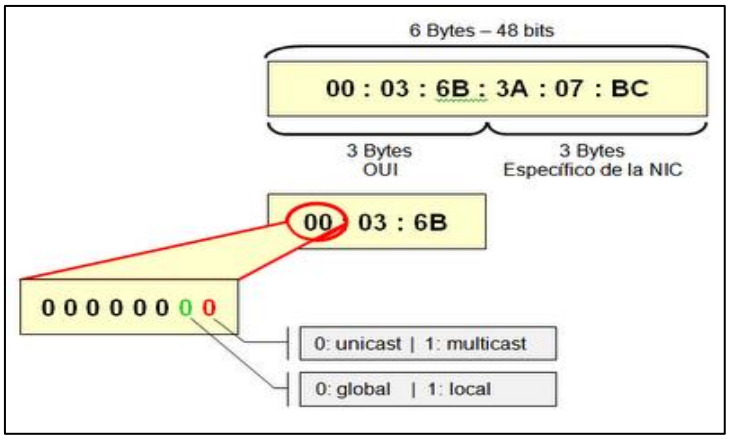


Figura 2. Estructura de la dirección física o MAC

Fuente: Recuperado de: http://librosnetworking.blogspot.com

2.1.2 Dirección IP.

IP es un acrónimo para describir el Protocolo de Internet, que al formar un conjunto de cuatro números, desde 0 hasta 255 separados por puntos identifican de manera lógica

y jerárquica un dispositivo final dentro de una red, para el envío y recepción de información.

La dirección IPv4 es representada por 32 bits, dicha dirección comúnmente es representada utilizando notación decimal, se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal máximo de cada octeto es 255, reservando este número para envió broadcast. (Baltazar José, Campuzano Juan, 2011)

2.1.3 Rango y clases de direcciones IP.

La dirección IP es una etiqueta numérica que identifica de manera lógica una interfaz de red o un host en particular, existen cinco tipos de clases de direcciones para identificar y localizar un dispositivo final dentro de una red, utilizando el Protocolo de Internet la tabla 1 muestra la distribución del direccionamiento IP versión 4.

- **Clase A:** Esta clase está destinada para redes muy grandes, tales como las de una gran compañía internacional. La clase A comprende redes desde 1.0.0.0 hasta 127.0.0.0. El valor del primer octeto es el que determina el tipo de clase y los tres últimos octetos son usados para identificar cada anfitrión. Esto significa que hay 126 redes de la clase A con la ecuación (2^24 -2) aproximadamente 16, 777,214 host.

- **Clase B:** La clase B se utiliza para las redes de tamaño mediano, como por ejemplo es el caso de un campus grande de una universidad. La clase B comprende

las redes desde 128.0.0.0 hasta 191.255.0.0; el número de red está en los dos primeros octetos. Esta clase permite 16.320 redes con 65.024 host cada una.

- **Clase C:** Las direcciones de la clase C se utilizan comúnmente para los negocios pequeños a mediados de tamaño siendo esta clase de direcciones, las más utilizadas. Las redes de clase C van desde 192.0.0.0 hasta 223.255.255.0, con el número de red contenido en los tres primeros octetos. Esta clase permite cerca de 2 millones de redes con más de 254 host.

- **Clase D y F:** Las direcciones que están en el rango de 224.0.0.0 hasta 254.0.0.0 son experimentales o están reservadas para uso con propósitos especiales y no especifican ninguna red.

Tabla 1. Direccionamiento IP versión 4

Clase	Desde	Hasta	Cantidad de redes	Cantidad de host	Direcciones para uso privado	Aplicación
A	0.0.0.0	127.255.255.255	128	16.777.214	10.0.0.0 – 10.255.255.255	**Redes grandes**
B	128.0.0.0	192.255.255.255	16.384	65.534	172.16.0.0 – 172.31.255.255	**Redes medianas**
C	192.0.0.0	223.255.255.255	2.097.152	254	192.168.0.0 – 192.168.255.255	**Redes pequeñas**
D	224.0.0.0	239.255.255.255	No aplica	No aplica	No aplica	**Multicast**
E	240.0.0.0	255.255.255.255	No aplica	No aplica	No aplica	**Investigación**

Fuente: Recuperado de https://www.rfc-es.org/rfc/rfc1918-es.txt

2.1.4 Protocolo de Resolución de Direcciones (ARP)

El Protocolo de resolución de direcciones (ARP, Address Resolution Protocol) es un estándar TCP/IP necesario que está definido en RFC 826, responsable de la comunicación

en la capa de enlace de datos del modelo OSI, asocia la dirección física (MAC), con una dirección IP determinada. Este protocolo se utiliza en los dispositivos de red local.

Las direcciones de control de acceso a medios se obtienen mediante una solicitud de difusión de red en forma de la pregunta "¿Cuál es la dirección de control de acceso al medio (MAC) de un dispositivo configurado con la dirección IP adjunta?". Cuando responde a una solicitud ARP, el remitente de la respuesta ARP y el solicitante de ARP original registran sus direcciones IP y de control de acceso a medios respectivos como una entrada en una tabla local, llamada la caché de ARP, para su uso posterior como referencia. (Microsoft Develoer network, 2005)

Otro protocolo es el RARP (Reverse Address Resolution Protocol –Protocolo de resolución de dirección de retorno) que funciona de manera inversa, para este caso debe existir un servidor que mantiene una base de datos de correspondencia de direcciones MAC a direcciones IP.

2.1.4.1 ARP de Control de Acceso al medio para tráfico local.

La Figura 3 muestra cómo resuelve ARP las direcciones IP en direcciones de hardware de hosts que se encuentran en la misma red local.

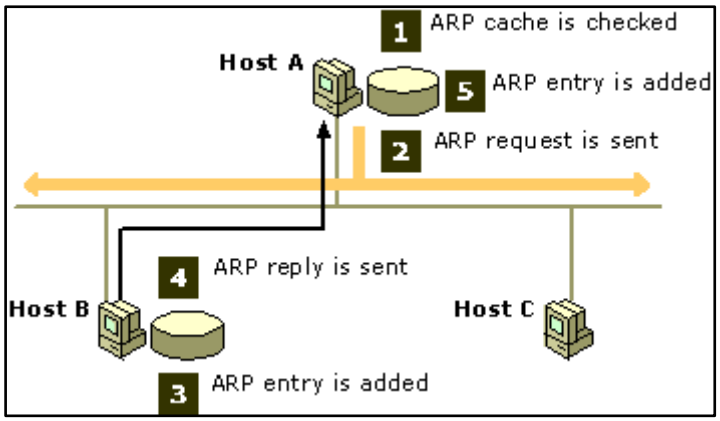


Figura 3. Procesos de resolución de direcciones para una red local

Fuente: Recuperado de https://msdn.microsoft.com

En este ejemplo, dos hosts TCP/IP, los hosts A y B, se encuentran en la misma red física. El host A tiene asignada la dirección IP 10.0.0.99 y el host B la dirección IP 10.0.0.100, ccuando el host A intenta comunicarse con el host B, los siguientes pasos permiten resolver la dirección asignada por el software al host B (10.0.0.100) en la dirección de control de acceso a medios asignada por el hardware al host B.

- Según el contenido de la tabla de enrutamiento del host A, IP determina que la dirección IP de reenvío que se va a utilizar para llegar al host B es 10.0.0.100. Después, el host A busca en su propia caché de ARP local una dirección de hardware coincidente para el host B.

- Si el host A no encuentra ninguna asignación en su caché, entonces, difunde una trama de solicitud ARP a todos los hosts de la red local con la pregunta "¿Cuál es la dirección de hardware para 10.0.0.100?" Las direcciones de hardware y software del origen, el host A, se incluyen en la solicitud ARP. Cada host de la red local recibe la solicitud ARP y comprueba si coincide con su propia dirección IP. Si el host no encuentra una coincidencia, descarta la solicitud ARP.

- El host B determina que la dirección IP especificada en la solicitud ARP coincide con su propia dirección IP y agrega una asignación de direcciones de hardware y software para el host A a su caché de ARP local.

- El host B envía directamente un mensaje de respuesta de ARP que contiene su dirección de hardware al host A.

- Cuando el host A recibe el mensaje de respuesta de ARP del host B, actualiza su caché de ARP con una asignación de direcciones de hardware y software para el host B.

Una vez determinada la dirección de control de acceso a medios del host B, el host A puede enviar al host B tráfico IP que se dirigirá a la dirección de control de acceso a medios del host B.

2.1.4.2 ***ARP de Control de Acceso al medio para tráfico remoto.***

ARP también se utiliza para reenviar datagramas IP a enrutadores locales de destinos que no se encuentran en la red local. En estos casos, ARP resuelve la dirección de control de acceso a medios de la interfaz de un enrutador en la red local. (Microsoft Develoer network, 2005)

La Figura 4 muestra cómo resuelve ARP las direcciones IP en direcciones de hardware de dos hosts que se encuentran en redes físicas diferentes conectadas por un enrutador común. (Microsoft Develoer network, 2005)

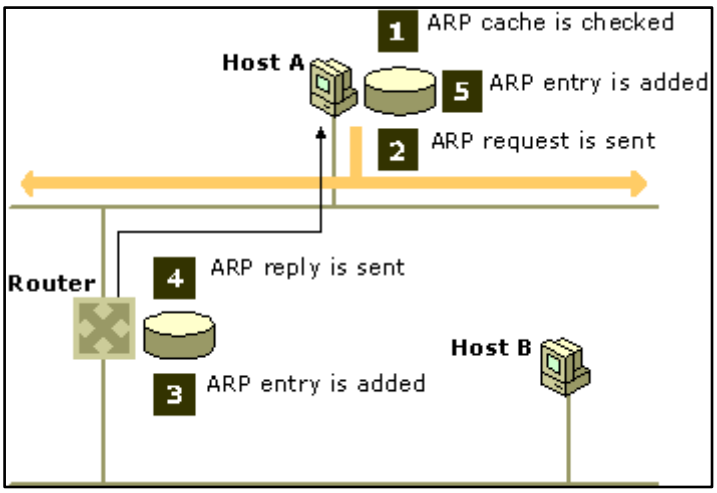


Figura 4. Procesos de resolución de direcciones para una red remota

Fuente: Recuperado de https://msdn.microsoft.com

En este ejemplo, el host A tiene asignada la dirección IP 10.0.0.99 y el host B la dirección IP 192.168.0.99. La interfaz del enrutador del host A se encuentra en la misma red física que el host A y utiliza la dirección IP 10.0.0.1. La interfaz del enrutador del host B se encuentra en la misma red física que el host B y utiliza la dirección IP 192.168.0.1.

Cuando el host A intenta comunicarse con el host B, los siguientes pasos permiten resolver la dirección asignada por el software a la interfaz del enrutador 1 (10.0.0.1) en la dirección de control de acceso a medios asignada por el hardware:

- Según el contenido de la tabla de enrutamiento del host A, IP determina que la dirección IP de reenvío que se va a utilizar para llegar al host B es 10.0.0.1, la dirección IP de la puerta de enlace predeterminada. Después, el host A busca en

su propia caché de ARP local una dirección de hardware coincidente para 10.0.0.1.

- Si el host A no encuentra ninguna asignación en la caché, difunde una trama de solicitud ARP a todos los hosts de la red local con la pregunta "¿Cuál es la dirección de hardware para 10.0.0.1?" Las direcciones de hardware y software del origen, el host A, se incluyen en la solicitud ARP.

- Cada host de la red local recibe la solicitud ARP y comprueba si coincide con su propia dirección IP. Si el host no encuentra una coincidencia, descarta la solicitud ARP.

- El enrutador determina que la dirección IP especificada en la solicitud ARP coincide con su propia dirección IP y agrega una asignación de direcciones de hardware y software para el host A a su caché de ARP local.

- Después, el enrutador envía directamente un mensaje de respuesta de ARP que contiene su dirección de hardware al host A.

- Cuando el host A recibe el mensaje de respuesta de ARP del enrutador, actualiza su caché de ARP con una asignación de direcciones de hardware y software para 10.0.0.1.

Una vez determinada la dirección de control de acceso a medios de la interfaz del enrutador del host A, el host A puede enviar a la interfaz del enrutador del host A, tráfico

IP que se dirigirá a la dirección de control de acceso a medios de esa interfaz. Posteriormente, el enrutador reenvía el tráfico al host B mediante el mismo proceso ARP que se describe en esta sección.

2.1.5 Puertos lógicos de red.

Son lugares de conexión lógica necesarios para que los programas puedan comunicarse con el exterior. La diferencia es que se enlazan virtualmente con los programas para compartir información y concretamente, utilizan el protocolo de Internet IP simultáneamente, es decir, es el medio por el cual un programa cliente, se comunica con un programa en específico, un host dentro de la red enlazados virtualmente, o dicho de otra manera, son puntos de acceso entre host para el uso de servicios y flujo de datos entre ellos.(Aguilar, 2012)

Los números de puertos lógicos de red van desde el 0 hasta 65536, que son gestionados por la IANA (Autoridad de Asignación de Números de Internet) y asegura la unicidad global de tres tipos de identificadores utilizados en internet:

- Puertos bien conocidos, definidos del puerto 1 al 1023, utilizados para servicios bien conocidos como web, correo electrónico, telnet, etcétera.
- Direcciones de protocolo de internet (direcciones IP).
- Nombres de dominio de Internet.

En la Tabla 2 se muestran los puertos lógicos más utilizados en las redes de datos

Tabla 2. Resumen de protocolos más utilizados

Numero de puerto	Servicio	Descripción
1	TCP	Multiplexor de servicios de puertos TCP
5	RJE	Entrada de trabajo remota
7	ECHO	Servicio de echo
9	DISCHARD	Servicio para evaluación de conexiones
19	MSP	Protocolo de envío de mensajes
20	FTP (datos)	Puerto de dialogo para la trasferencia de datos
21	FTP (control)	Puerto de dialogo para compartir de datos
22	SSH	Servicio de shell seguro
23	TELNET	Acceso remoto
25	SMTP	Protocolo de trasferencia simple de correo electrónico
42	NAMESERVER	Servicio de nombres de internet
53	DNS	Traducción de nombres de dominio
69	TFTP	
80	HTTP	Protocolo de trasferencia hipertexto de internet
110	POP3	Correo electrónico offline
8080	Proxy web	Forma segura de navegar por internet

Fuente: Recuperado de http://www.internetmania.net/int0/int133.htm

2.2 Dispositivos de la Red de Datos.

Los dispositivos dentro de una red son elementos físicos que básicamente permiten la conectividad entre segmentos para lograr compartir recursos. Dentro de las funciones de las redes podemos mencionar las siguientes: comparten información, comparten hardware, software y centralizan la administración y soporte de redes.

Para lograr un buen rendimiento dentro de una red de datos, es necesario contar con varios dispositivos de red para realizar las conexiones necesarias y unir la red con otras

redes y así, brindar un sistema más seguro y eficiente, a continuación se mencionan los varios de ellos.

2.2.1 Hub.

Es un dispositivo básico, repetidor multipuerto que corresponde a la capa uno del modelo OSI, donde se concentran un número limitado de host, crea una conexión central trasmitiendo paquetes que reciben desde cualquiera de sus puertos hacia todos los demás. Los Hubs han dejado de ser utilizados por su alto nivel de colisiones. En la Figura 5 se observa el modo de conexión de este dispositivo. (Sanchez; Ivan, 2014)

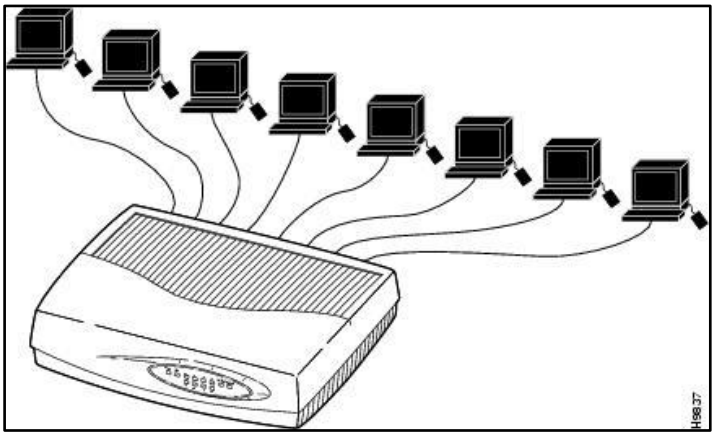


Figura 5. Conexión de un Hub

Fuente: Recuperado de http://www.cisco.com

2.2.2 Bridge o Puente de red.

Son dispositivos de capa dos del modelo OSI que tienen la misma funcionalidad de los repetidores, pero a diferencia de ellos, pueden dividir la red para aislar una parte de ella además permite la conexión entre equipos sin necesidad de routers, como se muestra en la Figura 6. (Sanchez; Ivan, 2014)

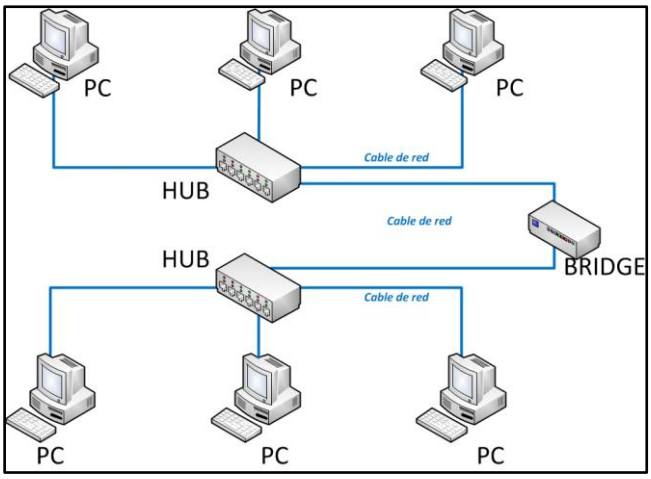


Figura 6. Interconexión de dos segmentos de red mediante un Bridge

Fuente: Recuperado de https://joseba18.files.wordpress.com/2011/12/bridge.png

2.2.3 Switch o Conmutador.

Son dispositivos de capa dos del modelo OSI, diseñados para resolver problemas de rendimiento dentro de un segmento de red debido a los anchos de banda y tráfico. Este dispositivo acelera la salida de paquetes reduciendo el tiempo de espera ya que basa su envío de paquetes en base a las direcciones MAC en la Figura 7 se observa la imagen de un Switch que conecta varios dispositivos finales o host.

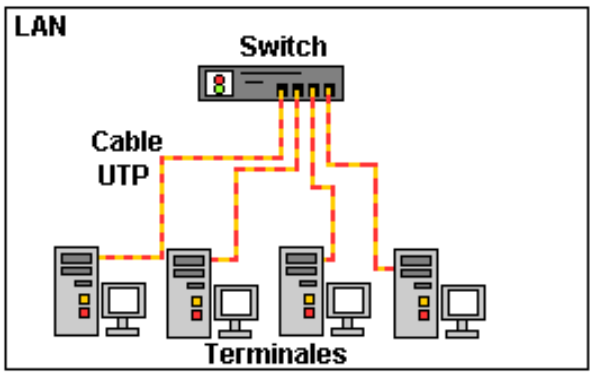


Figura 7. Interconexión de dispositivos finales mediante un switch.

Fuente: Recuperado de http://www.informaticamoderna.com/Switch.htm

2.2.4 Ruteadores o Router .

Este dispositivo que proporciona conectividad, y permite interconectar segmentos de red en una sola de manera inteligente, operan en la capa dos y tres de modelo OSI dependiendo de su capacidad. Su función principal es la de enviar o encaminar paquetes de datos de una red a otra, es decir puede conectar subredes amplias con la posibilidad de determinar el camino más corto rápido y de menos costo, en base a su dirección MAC, desde el origen hacia el destino, como se muestra en la Figura 8.

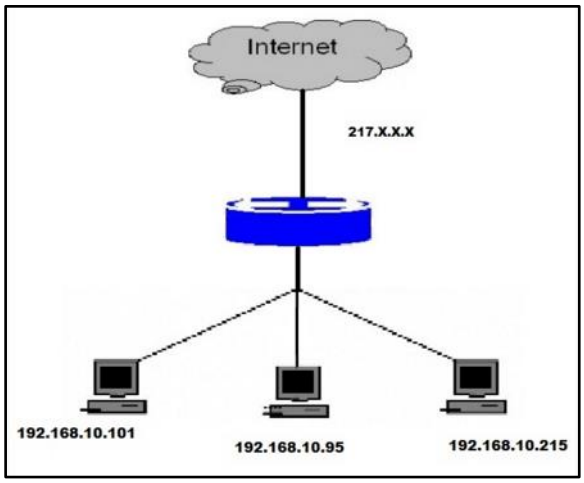


Figura 8. Interconexión de redes hacia la red de Internet mediante un Router capa tres.

Fuente: Recuperado de https://blogs.manageengine.com

2.2.5 Modem o demulador.

Es un dispositivo externo que nos permite convertir señales o pulsaciones en señales de información para ser transmitidas por las líneas telefónicas, esta señal se llama portadora y las funciones las realiza, con una señal llamada moduladora y con este dispositivo es posible la comunicación hacia el ISP, como se muestra en la Figura 9.

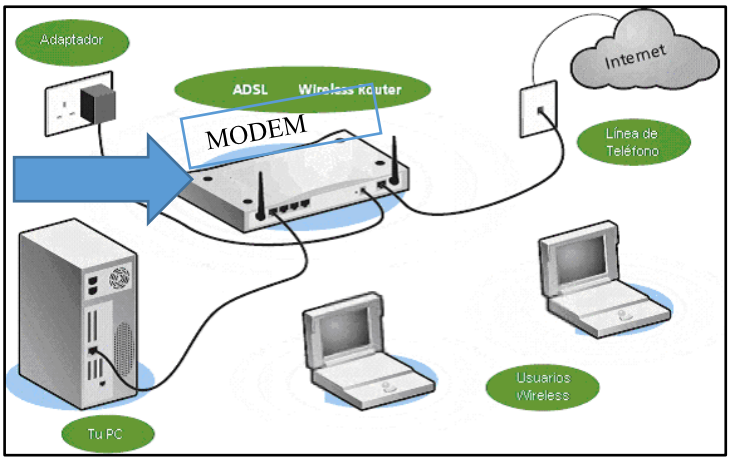


Figura 9. Interconexión de dispositivos finales mediante un modem

Fuente: Recuperado de http://www.configurarequipos.com

2.2.6 Servidor

Es un elemento principal que forma parte importante de la red, y provee de servicios en forma de programas, de aplicaciones finales en ejecución (software). Se denomina servidor dedicado a todo aquel que ofrece todos los recursos para atender solicitudes de los host clientes. (educativo, 2014)

Existen varios tipos de servidores que brindan distintas aplicaciones para los usuarios finales dentro. Según el portal educativo se detallan los siguientes:

- **Servidor web:** Este servidor provee de contenidos estáticos a los navegadores. Este trasfiere los archivos por medio de la red al navegador del usuario. Los archivos pueden ser imágenes, escrituras, documentos HTML y cualquier otro material web.

- **Servidores de correo FTP (File Transfer Protocol):** Protocolo de trasferencia de archivos, permite realizar todas las operaciones relacionadas con la trasferencia de datos entre diferentes servidores y ordenadores.

- **Servidor de acceso remoto:** Estos servidores permiten la administración de una determinada red de forma remota. De esta forma, se puede negar o permitir el acceso a ciertos sitios web, etc.

- **Servidor telnet:** Estos son los que admiten al usuario a entrar en una computadora huésped y hacer cualquier tipo de actividad como si estuviera trabajando directamente en esa computadora.

- **Servidores de archivos:** Estos servidores son los encargados de almacenar distintas clases de archivos para después enviárselas a otros clientes en la red.

- **Servidor de base de datos:** Estos servidores son los que ofrecen servicios de bases de datos a computadoras o programas.

- **Servidor dedicado:** este tipo de servidores dedican toda su capacidad y rendimiento a la administración de recursos dentro de la red, es decir atienden las solicitudes que son directamente de clientes.

- **Servidor no dedicado:** son aquellos que no dedican toda su capacidad y rendimiento a las solicitudes de clientes, toman el rol de procesa solicitudes de usuario local.

2.3 Seguridad perimetral

La seguridad perimetral es una rama de la seguridad informática que se ocupa de vigilar el perímetro o "borde" de la red, es decir, es una defensa ante las amenazas externas que intentan filtrarse. Se puede hacer una analogía con una muralla fortificada cuyo objetivo es restringir el paso a los enemigos, eso es básicamente lo que busca la seguridad perimetral, limitar los accesos solamente los paquetes confiables que circulan por la red y restringir aquellos que pueden hacer daño. (MAYORGA, 2008)

2.3.1 Objetivos de la seguridad perimetral.

Dentro de los objetivos de la seguridad perimetral se puede mencionar los siguientes:

- Proteger el perímetro de la red privada de datos ante las amenazas externas permitiendo sólo cierto tipo de tráfico en distintos segmentos de la red.

- Filtrar eficientemente todo tipo de acceso solicitado hacia la red privada, el tráfico entrante será dirigido a los sistemas adecuados dentro de la intranet.

- Reaccionar ante las amenazas antes de que estas puedan acceder a la red privada.

2.4 Componentes de la seguridad perimetral.

Los componentes esenciales que pueden existir en el perímetro de la red se detallan a continuación.

2.4.1 Perímetro de la red.

Llamado también zona de frontera ya que aísla la red externa con la red interna donde se encuentran los host y los servidores de aplicación. Es considerada como la zona menos segura del sistema además de ser un punto con el mayor tráfico a monitorizar, como se muestra en la Figura 10.

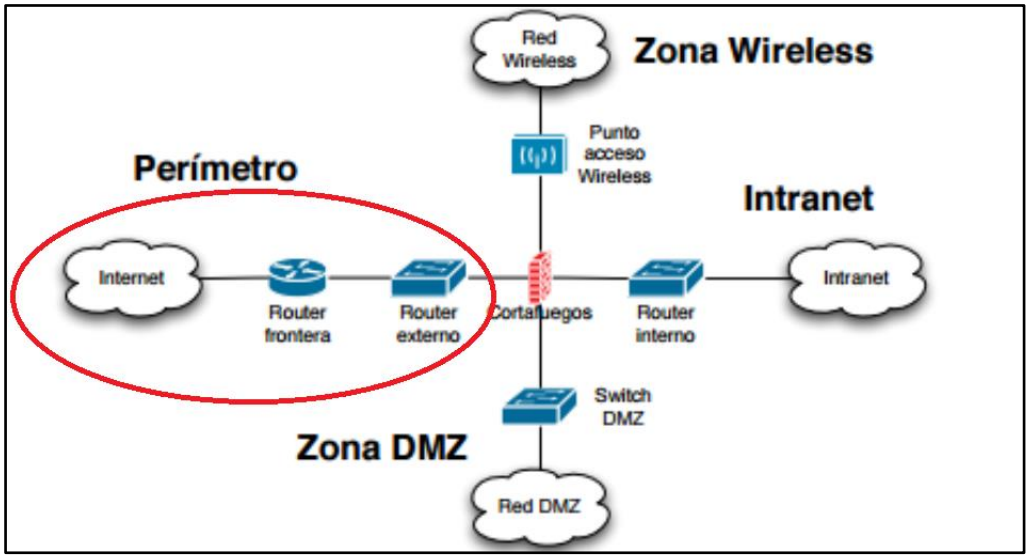


Figura 10. Topología de una red típica donde se visualiza la zona de perímetro de red

Fuente: Recuperado de http://www.ia.urjc.es

2.4.2 Zona desmitalirizada DMZ.

También es conocida por su acrónimo DMZ (zona desmitalirizada), red de perímetro, donde se ubica a una subred semipública dentro de la red en general. Es una zona segura de la subred donde se ubican los servidores que suministran acceso hacia la red pública, se colocan en un segmento separado, de esta manera se asegura que la red privada permanezca protegida, puesto que no necesitará involucrarse con otros segmentos de la red interna, como indica la Figura 11.

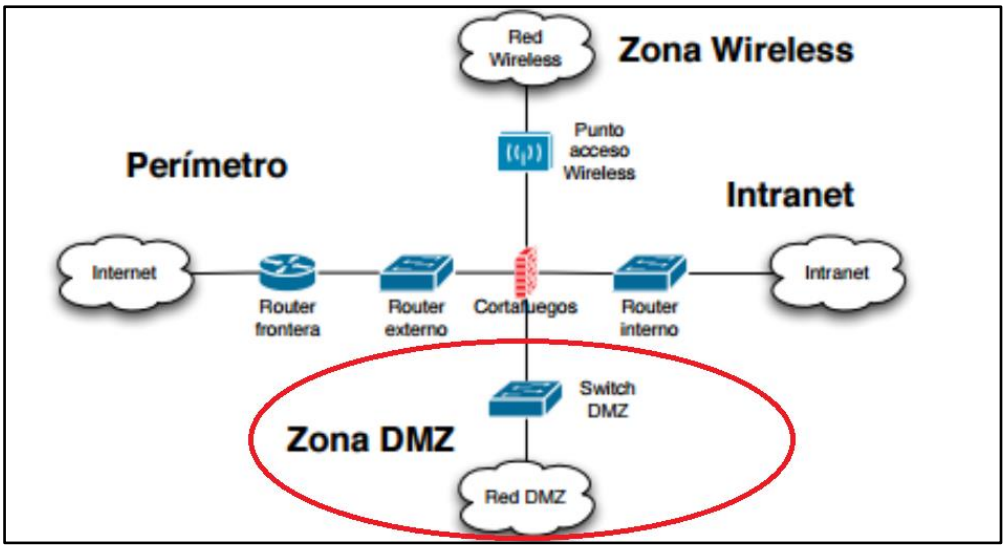


Figura 11. Topología de una red típica donde aísla la zona DMZ del resto de la red.

Fuente: Recuperado de http://www.ia.urjc.es/cms/

2.4.3 Zona de acceso inalámbrico (wireless)

Tecnología inalámbrica que permite conectar a equipos de usuarios finales con el soporte de un punto de acceso, brindado algún tipo de servicio. Es la zona susceptible y considerada como insegura tomando en cuenta la ubicación de la misma, como se muestra en la Figura 12.

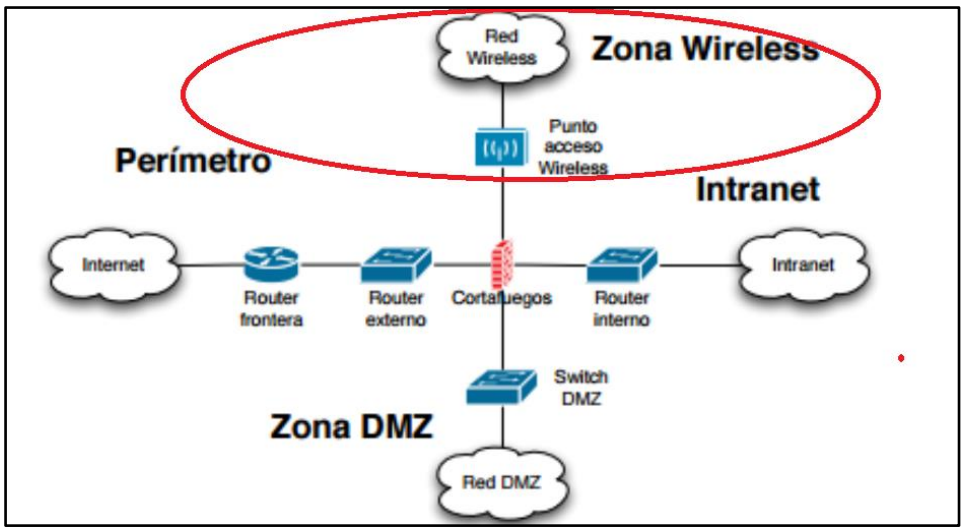


Figura 12. Topología de una red típica donde se visualiza la zona wireless

Fuente: Recuperado de http://www.ia.urjc.es

2.4.4 Zona de red de área local (LAN).

Es la red de área local donde se ha ubicado la intranet que en la mayoría de casos se ha creado utilizando normas, protocolos y una administración local de internet con la finalidad de compartir recursos con dispositivos físicamente adyacentes. Además Es la zona donde se dispone toda la información más crítica de la organización, como indica la Figura 13.

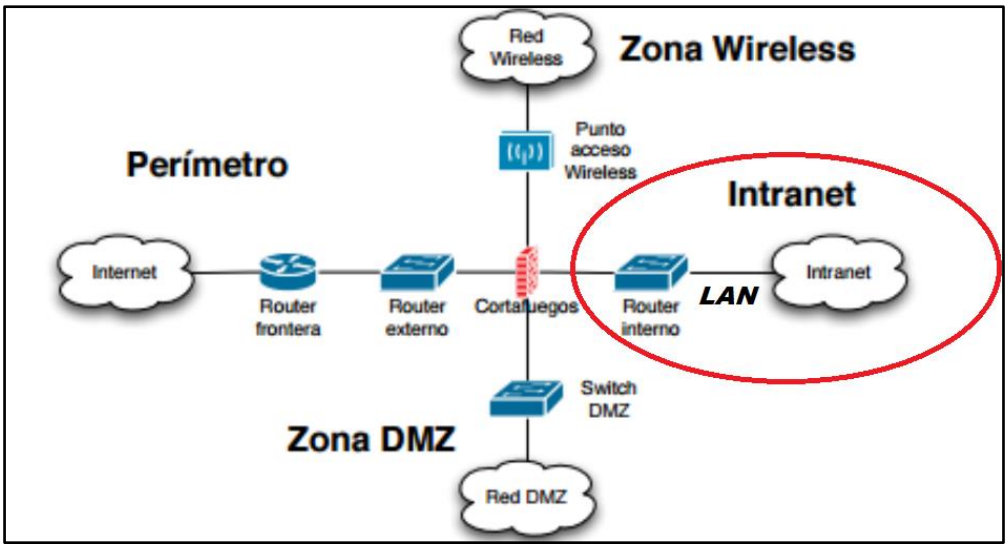


Figura 13. Topología de una red típica se visualiza la red de área local LAN

Fuente: Recuperado de http://www.ia.urjc.es

2.4.5 Firewall o corta fuegos

Firewall es un sistema de software o hardware, que impide el acceso no autorizado a la red de datos contra intrusiones provenientes de intrusos la mayoría procedentes de Internet, filtra los paquetes de datos que se intercambian a través de internet. Un sistema basado en un firewall básicamente debe cumplir con un conjunto de reglas, tales como las que se indican a continuación.

- Autoriza una conexión (permitir).
- Bloquea una conexión (denegar).
- Rechazar un pedido de conexión (negar).

En conjunto de reglas permiten crear una política de seguridad dependiendo de las necesidades de la red, por lo general las políticas de seguridad permiten:

- Permitir las comunicaciones autorizadas explícitamente y todo lo que no es autorizado está explícitamente prohibido.
- Impide cualquier comunicación que fuese explícitamente prohibida

2.4.6 Router de perímetro

Llamado también Router de borde situado entre la red interna y la red externa estos se encargan de dirigir el tráfico, lo direccionan hacía, desde y dentro de la red son los últimos ruteadores que están justo antes de una red no confiable, como el Internet. Debido a que todo el tráfico de Internet de una organización pasa por estos ruteadores, se lo utiliza como un primer y último filtro, por eso se los considera críticos para la defensa. (MAYORGA, 2008)

2.4.7 NAT (Network Address Traslation)

La mayoría de firewalls existentes ofrecen el servicio de NAT, que consiste en enmascarar o disfrazar la dirección IP de los hosts protegidos o que están detrás del

firewall a una dirección IP pública, por ejemplo, una red corporativa con 30 hosts con diferentes IP privadas dentro de la red interna, saldrán a navegar por Internet con una sola dirección IP pública. (MAYORGA, 2008)

2.5 Sistema de Detección y Prevención de intrusos.

2.5.1 IDS (Intrusion Detection System).

Es un sistema de detección de intrusos, es decir realiza la detección de acceso no autorizado, este tipo de mecanismo monitorea y genera un tipo de alarma si en el tráfico de la red se ha detectado amenazas.

Se utilizan tres tipos de sensores se mencionan a continuación, se ubican en puntos estratégicos de la red, esta es la clave para logar determinar una política de seguridad.

- *NIDS (Network-Based Intrusion Detection System):* Es un IDS basado en red que controla el tráfico en busca de actividades sospechosas.

- *HIDS (Host-Based Intrusion-Detection System):* Es un IDS que protege un solo host, por lo tanto el procesamiento del CPU es mucho menor a un NIDS.

- *DIDS (Network-Based Intrusion Prevention System):* Es un IDS que funciona en una arquitectura cliente servidor, está compuesto por varios NIDS que actúan como sensores centralizando la información de posibles ataques en una unidad central que almacena los datos en una base de datos. (MAYORGA, 2008)

2.5.2 IPS (Intrusion Prevention System)

Sistema de prevención de intrusos es un sistema integrado de prevención y protección en tiempo real a partir de la identificación de patrones de amenazas hacia un ataque en el tráfico de la red.

- *HIPS (Host Based Intrusion Prevencion System):* es una aplicación de prevención de intrusiones que se especifica en un solo host y previene diferentes ataques en la red de datos.

- *NIPS (Network Based Intrusion Prevencion System):* Son sistemas de prevención de intrusos a nivel de red, los cuales buscan todos los ataques que se produzcan hacia la red y los bloquea.

- *WIPS (Wireless Intrusion Prevencion System):* Wireless IPS, su funcionamiento es idéntico al de las NIPS con la diferencia que éstas controlan la seguridad de una red inalámbrica, cuando encuentra un usuario maligno lo bloquea para que no realice daños a la red. (TORRES, 2014)

2.6 Fundamentos de seguridad en redes

2.6.1 Seguridad en redes.

Se define a la seguridad en redes como el método de aplicación donde se protege la integridad y privacidad de la infraestructura de red donde esta se encuentra.

2.6.2 Requisitos de la seguridad en redes.

2.6.2.1 Disponibilidad

Se refiere al proceso de mantener los sistemas de red funcionando eficientemente para satisfacer requisitos, garantiza que los usuarios tengan acceso tanto a la información como servicios además debe de ser capaz de recuperarse rápidamente en caso de fallo.

2.6.2.2 Confidencialidad

Hace mención a la protección de los datos y a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información que se almacena, la pérdida de confidencialidad puede ser el resultante de problemas de tipo legal además de la credibilidad.

2.6.2.3 Integridad

Es la habilidad de proteger y asegurar que la información, datos o trasmisiones que se estén manejando no pueda ser modificada por personas no autorizadas.

2.6.2.4 Autenticidad

Se refiere a la legitimidad y credibilidad que permite asegurar el origen de la información, de modo que se puede demostrar que es quien dice ser.

2.6.2.5 Control de Acceso

Proceso en el cual se controla y verifica el acceso a los sistemas o recursos de la red, además del tipo de información puede recibir.

2.6.2.6 Vulnerabilidad.

Se refiere el punto o aspecto de la red que pueden ser más susceptible a amenazas.

2.6.2.7 Amenaza.

Se conoce como amenaza a la posibilidad de interferencia con el correcto funcionamiento de los recursos de la red, produciendo algún tipo de daño en los elementos de la red.

2.6.2.8 Tipos de Amenazas.

Las amenazas pueden clasificarse en dos tipos:

- Intencionales, en caso de que premeditadamente se intente producir un daño (por ejemplo el robo de información , la propagación de código malicioso , Hackers o las técnicas de ingeniería social).

- No intencionales, en donde se producen acciones u omisiones que si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de la información y pueden producir un daño (por ejemplo las amenazas relacionadas con fenómenos naturales, negligencia, etcétera)

2.7 Segmentación de redes.

La segmentación de redes es el proceso por el cual se agrupan o dividen lógicamente los activos, recursos y aplicaciones de red, proporcionando una mejora en la seguridad y proteger de forma dinámica la infraestructura de la red de datos de una organización.

2.7.1 Características de la segmentación.

- Los usuarios finales se conecta a un segmento de red el más cercano físicamente, los dispositivos que unen estos segmentos generalmente son hubs o switchs.

- Cada una de las VLANs es un dominio de broadcast.

- Dentro de la red, se encontraran varias VLANs, las que sean necesarias, compartiendo la misma Infraestructura.

- Cada una de las VLANs dentro de un red LAN es independiente

- Los usuarios o estaciones finales se agrupan en VLANs, según el administrador de la red crea conveniente.

- El Router es el encargado de la comunicación entre las VALNs

- La segmentación por VLANs es un método eficaz de proporcionar seguridad a la red.

2.8 Red de área local virtual (VLANs).

Una VLAN es una agrupación lógica de dispositivos o servicios de red, en base a las funciones departamentos, equipos de trabajo o aplicaciones sin considerar la localización física o conexiones de red. (MOLINA, 2012)

2.8.1 Dominio de colisión.

Se denomina dominio de colisión a el conjunto de dispositivos que se están físicamente conectados al mismo medio de comunicación, y es el área de red donde los dispositivos acceden al mismo tiempo, lo que resulta y originan las tramas múltiples que se produzcan las colisiones.

2.8.2 Dominio de Broadcast.

Dominio de broadcast es el conjunto de dispositivos que reciben tramas de broadcast que cualquiera de los dispositivos conectados a la red. Cuando un switch recibe una trama de broadcast este la reenvía a cada uno de sus puertos excepto al puerto entrante en el que el switch recibió la trama.

2.8.3 Tipos de VLANs.

2.8.3.1 VLANs de datos.

Es una VLAN configurada para trasportar tráfico generado por los usuarios se usan para dividir la red en grupos de usuarios o dispositivos.

2.8.3.2 VLAN predeterminada.

Todos los puertos de switch se vuelven parte de un segmento la VLAN también es conocida como VLAN 1.

2.8.3.3 VLAN nativa.

Es una condición usada con interfaces que son configuradas como Vlan de enlaces troncales. Cuando un puerto de switch ha sido configurado como un enlace troncal este, es etiquetado son su respectivo identificador de numero de Vlan. Las tramas de todas las Vlans son trasportadas por un enlace en modo troncal, por medio del protocolo 802.1Q.

2.8.3.4 VLAN de administración.

Una Vlan de administración en cualquier Vlan que se configura para acceder a las capacidades de administración de un switch. La VLAN 1 es la Vlan de administración predeterminada.

2.9 Técnicas y métodos de investigación para la evaluación del riesgo.

2.9.1 Método Cualitativo.

Se trata de determinar la severidad del Riesgo, agrupándolos en algunas categorías, de acuerdo a los criterios: alta, media y baja.

2.9.2 Método Cuantitativo.

Clasifican su importancia en función de cálculos de costos, importancia etc., estimados en función de su consecuencia y de su Probabilidad.

2.9.3 Técnicas de recolección de la información.

Cualquiera de las siguientes técnicas o combinación de las mismas se puede utilizar para recolectar información relevante sobre los límites operacionales de un sistema de TI

2.9.3.1 Cuestionarios.

El personal responsable por el análisis de riesgos puede desarrollar cuestionarios para colectar información sobre las amenazas, preocupaciones, clasificación y categorización de la información y los riesgos, las vulnerabilidades, los controles administrativos y operacionales planeados o utilizados por el sistema de TI. Estos cuestionarios se deben distribuir entre el personal técnico y no técnico relacionado con el sistema de TI.

2.9.3.2 Las visitas en sitio.

También permiten observar y recoger información sobre la seguridad física y operacional del ambiente de procesamiento del sistema de TI. Si esta información no existe, la sensitividad y criticidad de los activos de información se puede determinar a través de la medición del nivel de protección requerido para mantener la confidencialidad, integridad y disponibilidad de los datos y del sistema de TI. La persona más indicada para establecer estos niveles es el propietario de los datos y sistemas, por tanto es necesario entrevistarlos.

2.9.3.3 Revisión de documentos.

Los documentos de políticas (leyes, directivas, documentación del sistema tales como manuales de usuario y de administración, diseño del sistema y requerimientos funcionales y la documentación relacionada con la seguridad tales como informes de auditoría, análisis y evaluaciones de riesgos realizadas, resultados de pruebas de vulnerabilidad a los sistemas, los planes de seguridad del sistema), proveen excelente información acerca de los controles usados y planeados para el sistema de TI. El análisis de impacto a la misión de la entidad y la valoración de la criticidad de los activos (niveles de criticidad) proveen información relacionada con la sensibilidad y criticidad de los datos y sistemas.

2.9.3.4 Uso de herramientas de escaneo automatizadas.

Es una técnica proactiva para la recolección eficiente de información del sistema. Un caso son las herramientas de mapeo de redes que pueden identificar servicios en

ejecución en un grupo de servidores y proveen una vía rápida para la construcción de perfiles individuales de los sistemas objetivos.

CAPÍTULO III

3. Evaluación de la situación actual de la red de datos

Se evalúa la situación actual con la que se encuentra la red de Datos del Instituto Tecnológico Superior “José Chiriboga Grijalva”, mediante un estudio de la seguridad lógica y física de la red, además como parte importante se realiza una evaluación de los equipos de tecnología con los que cuenta la infraestructura de red.

3.1 Instituto Tecnológico Superior “José Chiriboga Grijalva”.

El Ministerio de Educación y Cultura mediante Acuerdo Ministerial Nº 3669 de fecha 5 de agosto de 1992, autoriza la transformación y funcionamiento del Instituto "José Chiriboga Grijalva" de la ciudad de Ibarra, provincia de Imbabura, con la finalidad de que otorgue los títulos de: Técnico Superior y el Título de Tecnólogo. (ITCA, 2015)

Instituto Tecnológico Superior “José Chiriboga Grijalva” con su acrónimo ITCA se encarga de formar profesionales en distintas carreras de nivel tecnológico, teniendo presente los valores y el perfeccionamiento de habilidades y destrezas, con la objetivo de generar soluciones a los problemas y necesidades del país.

3.1.1 Descripción física del Instituto Tecnológico Superior "José Chiriboga Grijalva"

El instituto de estudios superiores se encuentra ubicado en la provincia de Imbabura, cantón Ibarra ubicado específicamente en las calles El Oro y 13 de abril, figura 13, dentro de las carreras que oferta como educación se encuentran las siguientes: Administración de empresas, Mercadotecnia, Administración de centros infantiles, Informática, Secretariado Ejecutivo, Gestión turística mención en gastronomía y diseño, modas y pasarela. En la Figura 14 se muestra el campus del Instituto.

Figura 14. Vista del Instituto Técnico Superior "José Chiriboga Grijalva"

Fuente: Recuperado de http://portalins.tecnologicoitca.edu.ec

3.1.2 Personal del Instituto Tecnológico Superior "José Chiriboga Grijalva"

El instituto dentro de su planta educativa cuenta con veinte empleados de la parte administrativa y docentes de tiempo completo y de contrato igual a cuarenta y dos docentes, como muestra la Tabla 3, además posee un número total de estudiantes de mil ciento treinta y ocho actualmente matriculados, como se indica en la Tabla 4.

Tabla 3. Número de personal del ITCA

Cargo desempeñado ITCA	Número de empleados ITCA
Empleados administrativos y servicio	**20**
Docentes tiempo completo	**30**
Docentes a contrato	**12**
Total	**62**

Fuente: ITCA

Tabla 4. Número de estudiantes ITCA

Programas Académicos	Número de alumnos
Carrera de Administración de Empresas	**353**
Carrera de Administración de Centros Infantiles	**191**
Carrera de Secretariado Ejecutivo	**49**
Carrera de Informática	**38**
Carrera de Mercadotecnia	**39**
Carrera de Desarrollo Integral del Niño	**252**
Carrera de Diseño, Moda y Pasarela	**54**
Carrera de Gestión Turística, mención Gastronomía	**162**
Total	**1138**

Fuente: ITCA

3.1.3 Organigrama institucional del Instituto Tecnológico Superior "José Chiriboga Grijalva"

La Figura 15 muestra el organigrama institucional que maneja el ITCA.

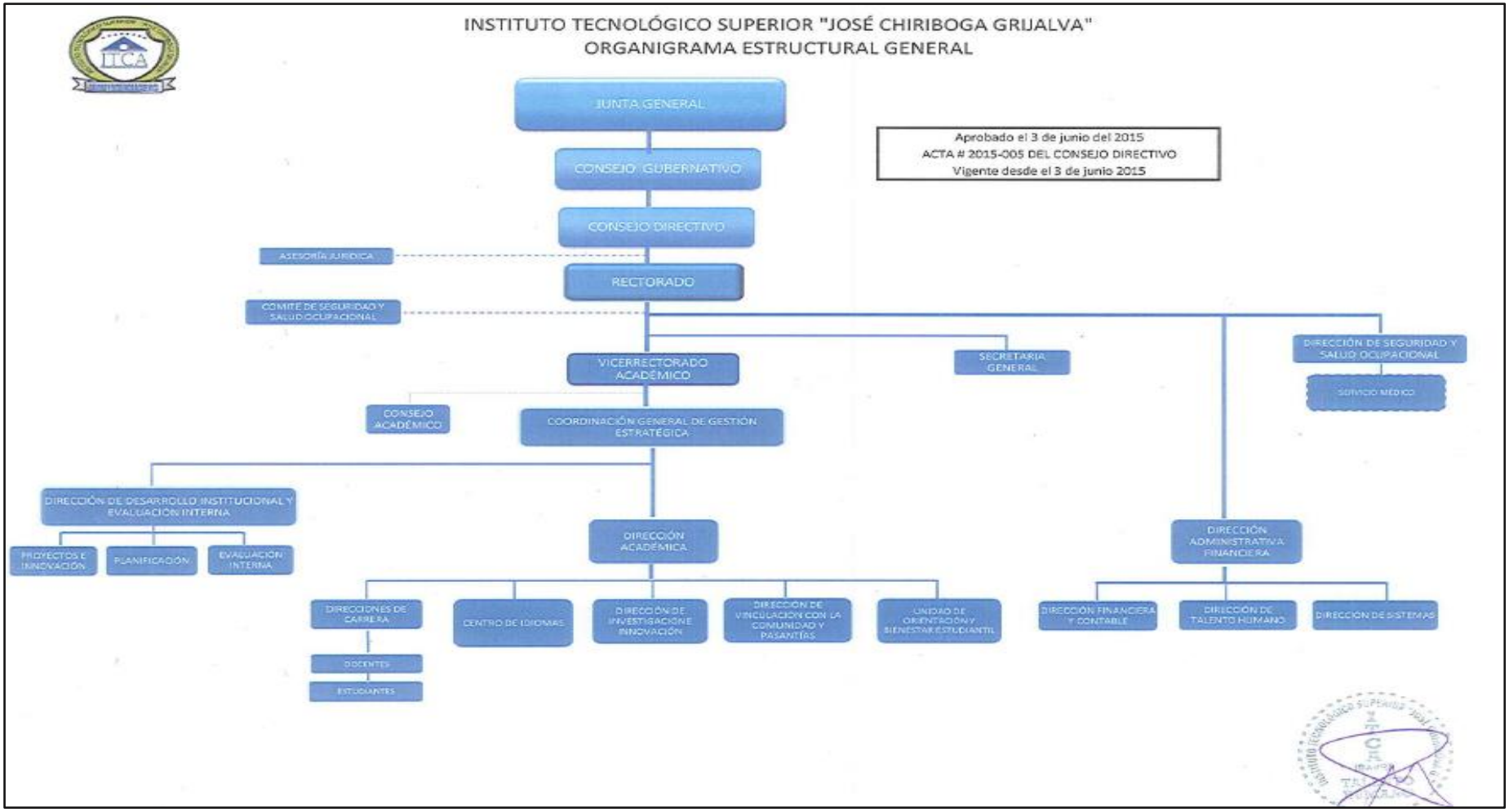


Figura 15. Organigrama Estructural General

Fuente: Recuperado de http://portalins.tecnologicoitca.edu.ec

3.2 Situación actual de la red de datos del Instituto Tecnológico Superior "José Chiriboga Grijalva".

Tomando en cuenta que la institución educativa en los últimos cinco años ha realizado un importante cambio de espacio físico, por hoy cuenta con un nuevo edificio y con esto la capacidad ha aumentado, de tener en sus instalaciones mayor número de alumnos, docentes y personal administrativo. Por ende este tipo de usuarios necesitan a diario los servicios de la red de datos del instituto como: acceso a las aulas virtuales, ingreso de notas, correo institucional, facturación etc., con la finalidad de compartir recursos.

3.2.1 Topología de red.

La topología de red del Instituto Tecnológico Superior "José Chiriboga Grijalva" se encuentra dividida en dos entornos, la topología física y la topología lógica.

3.2.1.1 Topología física.

En esta topología se evidencia el lugar físico donde se encuentran los equipos de usuarios finales, los dispositivos de red y el cableado que conforman la red de datos del instituto, como se muestra en la Figura 16.

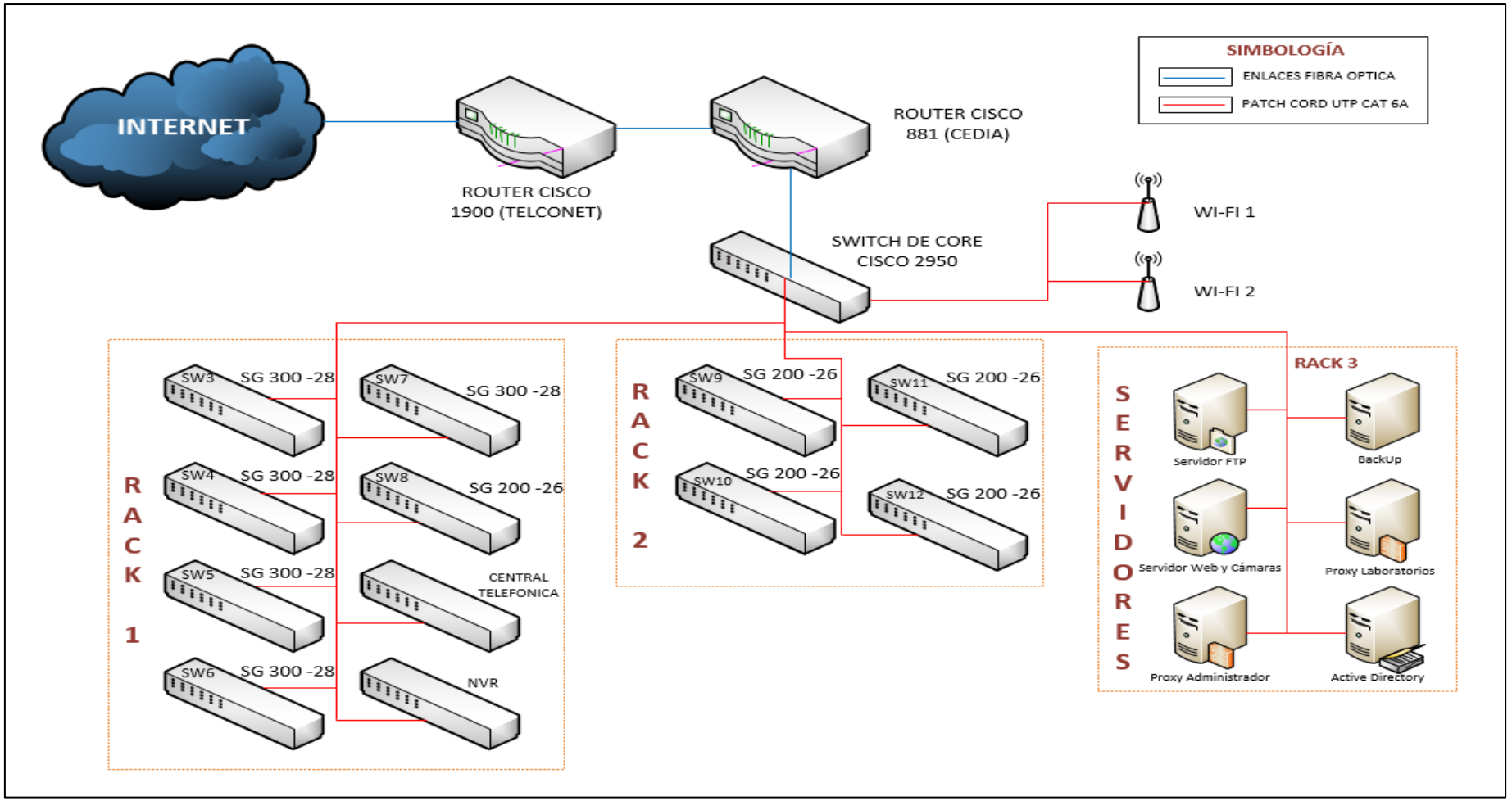


Figura 16. Topología física del Instituto Tecnológico Superior "José Chiriboga Grijalva"

Fuente: Dirección de tecnología de la información ITCA

3.2.1.2 Topología lógica.

Dentro de esta topología se visualiza la forma de cómo se comunican los servicios y usuarios de capa de acceso con la infraestructura de red dentro de la topología física, como indica la Figura 17.

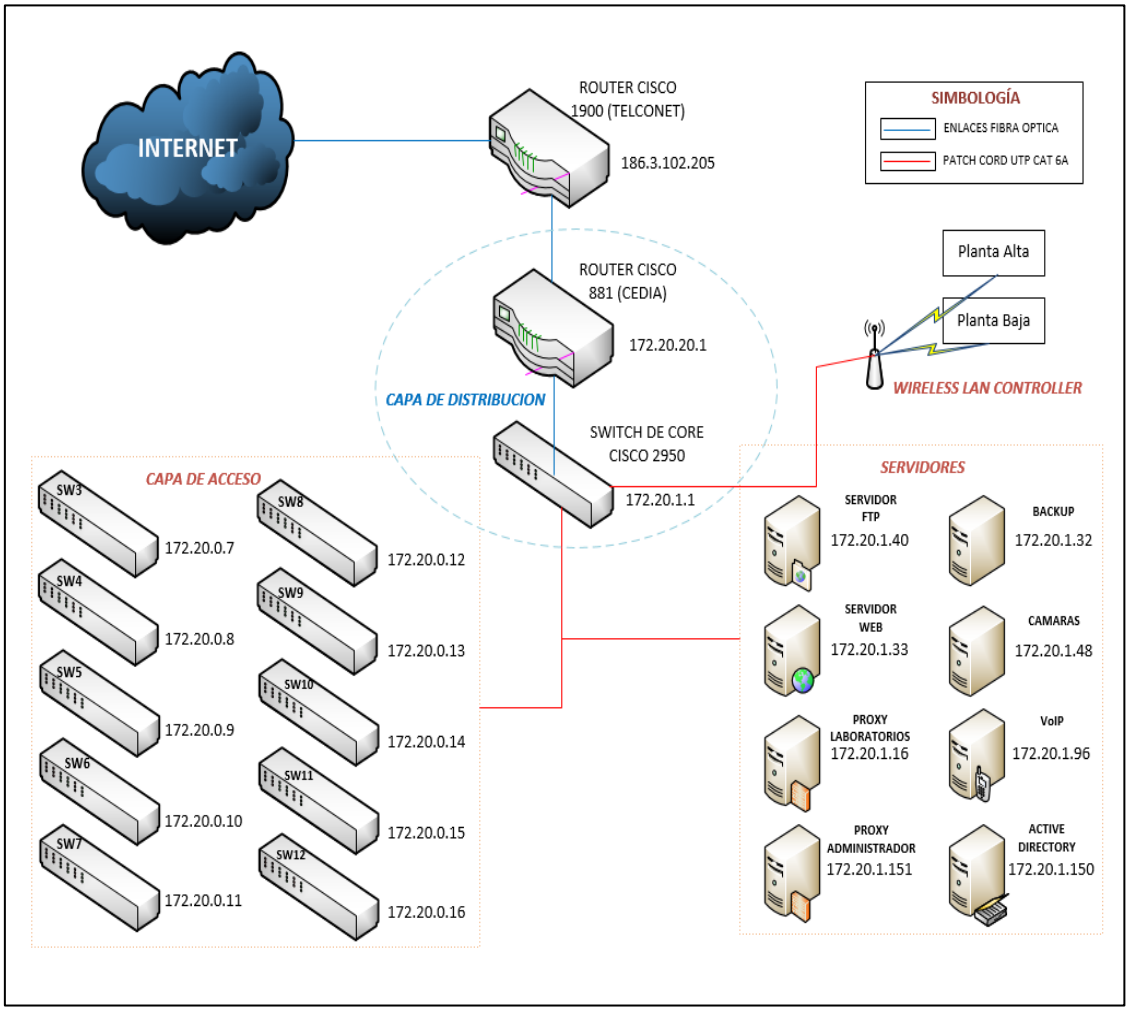


Figura 17. Topología lógica del Instituto Tecnológico Superior "José Chiriboga Grijalva"

Fuente: Dirección de tecnología de la información ITCA

3.3 Descripción de la topología de red del Instituto Tecnológico Superior "José Chiriboga Grijalva"

3.3.1 Componentes del Data Center.

3.3.1.1 Espacio físico.

El Data Center se encuentra ubicado en la planta baja del instituto, específicamente en al área de acceso a los laboratorios, cuenta con un espacio físico propio para este tipo de instalaciones aproximadamente con un área de 15m2, nivel de Tier 1 Véase la Figura 18.

Figura 18. Ubicación del data center en el Instituto Tecnológico Superior "José Chiriboga Grijalva"

Fuente: Dirección de tecnología de la información ITCA

3.3.1.2 Piso falso

El piso falso es el sistema que permite elevar 30 centímetros del piso fijo, para la instalación del aire acondicionado, y cableado eléctrico, garantiza la circulación del aire para el enfriamiento y climatización.

3.3.1.3 Cableado

El sistema de cableado es la estructura física donde se evidencia los cables dentro del centro de datos, permite la comunicación de todos los sistemas y servidores de manera local y remota.

El Cableado estructurado se desarrolla por un cordón de Fibra Óptica Furukawa cor-mm-dp-18-cog mm 50 om3 10 gigabit dúplex optical, de acuerdo a la norma ANSI/TIA/EIA- 568-C.3, para el uso interno de la instalación principal del cuarto de comunicaciones del instituto.

Así también Cable UTP Categoría 6A, los cuales se distribuyen desde su Data Center constituido por equipos Cisco tales como un Router HP A-MSR 900 que encabeza la topología de red perteneciente a TELCONET.

3.3.1.4 Sistema eléctrico.

Tiene que ver con el suministro de energía eléctrica para todo el centro de datos, en ese sistema incluye los paneles, conductores y algunos tipos de receptores, voltajes de operación que varían de un lugar a otro.

3.3.1.5 Sistema de climatización.

El centro de datos cuenta con un sistema de enfriamiento que permite mantener a los equipos en correcto funcionamiento.se encuentra dirigido hacia dentro del piso falso, hacia arriba en el centro de datos y dentro de los racks de equipos por los agujeros perforados del piso falso.

3.4 Descripción de la topología de red.

De acuerdo a la topología lógica de la red de datos del Instituto, se evidencia, que no se encuentra con un modelo jerárquico de capas correctamente establecido convirtiendo esta infraestructura en una red plana y de tal manera en una red no segura.

3.4.1 Capa de CORE o núcleo.

El proveedor de servicio de internet está dado por TELCONET a través de un Router CISCO 1900 con un rango de dirección IP pública, clase B que va desde la 186.3.102.202 hasta la 186.3.102.206 y mascara de subred igual a 255.255.255.0, con velocidad de trasmisión de 16Mbps a continuación se detalla en la tabla 5 el direccionamiento de las direcciones IP públicas del instituto.

También cuenta con los servicios y beneficios de pertenecer al consorcio de CEDIA, mediante una solicitud de admisión, ya que al ser un institución de educación superior cuenta con los servicios de estimular, promover y coordinar el desarrollo de las tecnologías de información y las redes de telecomunicaciones e informática, enfocadas al

desarrollo científico, tecnológico, la tabla 4 muestra el direccionamiento de la dirección IP pública, a través de Router marca CISCO 881.

Uno de los beneficios de pertenecer a CEDIA es que la institución como miembros activo tiene acceso a velocidad de internet acordes a su necesidad. Este esquema permite reducir los costos a niveles muy por debajo de la media del mercado.

Tabla 5. Direccionamiento IPs Públicas

Dirección IP	**Mascara**	**Asignación**
186.3.102.202	255.255.255.248	Router ITCA
186.3.102.203	255.255.255.0	Pruebas
186.3.102.204	255.255.255.0	Router CEDIA
186.3.102.205	255.255.255.0	Router TELCONET
186.3.102.206	255.255.255.0	

Fuente: Dirección de tecnología de la información ITCA

3.4.2 Capa de distribución.

Dentro de la capa distribución se cuenta con un switch administrable capa 3 de la marca CISCO 2950 de 24 Puertos donde se encuentran adheridos los diferentes servicios.

Cuenta con ocho switchs de la marca CISCO SG300-28 donde se encuentran conectados los diferentes servicios que se detallan en la tabla 6.

Tabla 6. Distribución de Switch Rack 1

Numero	Switch	Numero de puertos	Identificación del switch	Servicio adherido
1	CISCO SG300	28 puertos	SW 1	**¿**
2	CISCO SG300	28 puertos	SW 2	**¿**
3	CISCO SG300	28 puertos	SW 3	**¿**
4	CISCO SG300	28 puertos	SW 4	**¿**
5	CISCO SG300	28 puertos	SW 5	**¿**
6	CISCO SG300	28 puertos	SW 6	**¿**
7	CISCO SG300	28 puertos	SW 8	**¿**
8	CISCO SG300	28 puertos	SW 8	**¿**

Fuente: Dirección de tecnología de la información ITCA

Además se encuentran seis Switch de la marca CISCO SG 200-26 donde están enrutados los servicios restantes que se detallan en la tabla 7.

Tabla 7. Distribución de Switch Rack 2

Número	Switch	Numero de puertos	Identificación del switch	Servicio adherido
1	CISCO SG200	26 puertos	SW 8	**Laboratorio**
2	CISCO SG200	26 puertos	SW 9	**Laboratorio 1**
3	CISCO SG200	26 puertos	SW 10	**Laboratorio 2**
4	CISCO SG200	26 puertos	SW 11	**Laboratorio 3**
5	CISCO SG200	26 puertos	SW 12	**Laboratorio 4**
6	CISCO SG200	26 puertos	SW 13	**Laboratorio 5**

Fuente: Dirección de tecnología de la información ITCA

3.4.3 Distribución de las VLAN's .

La tabla 8 se muestra el direccionamiento de las Vlans con su respectivo direccionamiento IP, con las que la institución cuenta en el momento.

Tabla 8. Distribución de Switch Rack 2

Numero de Vlan	Dirección IP	Servicio
Vlan 2	172.20.1.2	Administrativos
Vlan 3	172.20.1.3	Administrativos
Vlan 4	172.20.1.4	Sistemas
Vlan 5	172.20.1.5	Laboratorios
Vlan 6	172.20.1.6	Wireless
Vlan 7	172.20.1.7	Vigilancia
Vlan 8	172.20.1.8	Coordinadores
Vlan 9	172.20.1.9	Internet

Fuente: Dirección de tecnología de la información ITCA

3.4.4 Distribución del direccionamiento para los servidores del instituto.

La institución cuenta con los servidores que se muestran en la tabla 9.

Tabla 9. Distribución del direccionamiento IP de los servidores

Servidor	Dirección IP	Mascara de Red
FTTP	172.20.1.40	**255.255.X.X**
WEB	172.20.1.33	**255.255.X.X**
PROXY LABORATORIOS	172.20.1.16	**255.255.X.X**
PROXY ADMINISTRATIVOS	172.20.1.151	**255.255.X.X**
ACTIVE DIRECTORY	172.20.1.6	**255.255.X.X**
BACKUP	172.20.1.150	**255.255.X.X**
FACTURACIÓN	172.20.1.32	**255.255.X.X**
CAMARAS DE VILGILANCIA	172.20.1.48	**255.255.X.X**
VoIP	172.20.1.96	**255.255.X.X**

Fuente: Dirección de tecnología de la información ITCA

3.5 Especificaciones técnicas de los equipos de Networking.

A continuación de describe uno a uno, las especificaciones técnicas de los equipos físico que conforman la infraestructura de redes del Tecnológico ITCA

3.5.1 Router Cisco 1900

El Router de la serie 1900 que se indica en la Figura 19 encabeza la topología de la red y es de pertenencia de TELCONET, posee las características mostradas en la tabla 10.

Figura 19. Router CISCO 1900

Fuente: Recuperado de http://www.spetel.com/portfolio/cisco-serie-1900/

Tabla 10. Especificaciones técnicas del Router 1900

Especificaciones técnicas R1900	
Rendimiento	1 Gbps
Acho de banda	370 Mbps
Memoria RAM	3MB
Tasa de envío de paquetes	14.880 pps
Latencia	70 us
2 Puertos	10BASE-T
2 Puertos	100BASE-T
1 Puerto	Consola
Protocolo remoto de gestión	SNMP, RMON
Consumo	50 vatios
Voltaje nominal	CA 120

Fuente: Dirección de tecnología de la información ITCA

3.5.2 Router Cisco 881

El Router de la serie 881 que también se encuentra en la capa de CORE, que pertenece a CEDIA se muestra en la Figura 20, sus características se describen en la tabla 11.

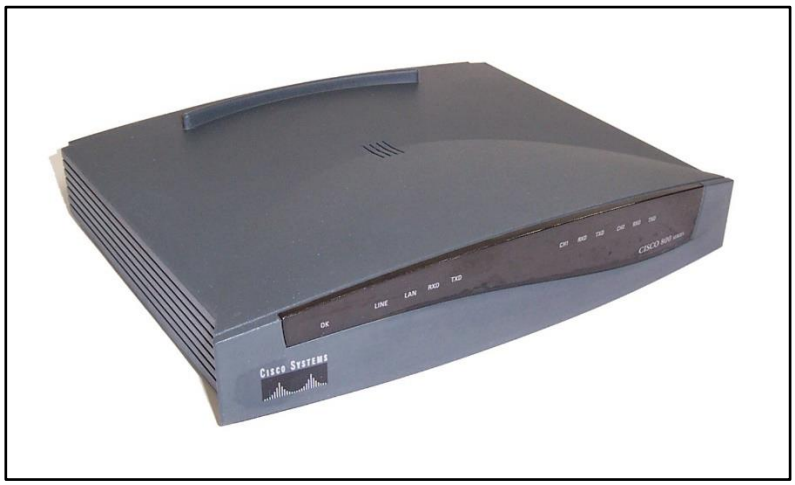


Figura 20. Router CISCO Serie 881

Fuente: Recuperado de http://www.ebay.es/itm/Cisco-803-Serie-800-ios-c800-y6-mw-ver-12-0-4-T1-Router

Tabla 11. Especificaciones técnicas del Router 881

Especificaciones técnicas R881	
Rendimiento	**1 Gbps**
Acho de banda	**370 Mbps**
Memoria flash	**128 MB**
Tasa de envío de paquetes	**14.880 pps**
Latencia	**70 us**
2 Puertos	**10BASE-T**
2 Puertos	**100BASE-T**
1 Puerto	**Consola**
Protocolo de enrutamiento	**BGP,EIGRP,RIP-1, RIP-2**
Protocolo remoto de gestión	**SNMP, RMON**
Consumo potencia	**50 vatios**
Volteje nominal	**CA 120**

Fuente: Dirección de tecnología de la información ITCA

2.3.3.3 Switch Cisco 2950

Switch administrable de 24 puertos, se muestra en la Figura 21, en este dispositivo se encuentran configuradas las Vlans, en la Tabla 12 se especifican las características principales del mismo.

Figura 21. Switch cisco 2950

Fuente: Recuperado de http://www.cableyes.com/des/doc/SWITCH%20CISCO%20CATALYST%202950.pdf

Tabla 12. Especificaciones técnicas del switch 2950

Especificaciones técnicas SW 2950	
Rendimiento	1 Gbps
Acho de banda	13.6 Gbps
Memoria flash	8 MB
Memoria DRAM	32 MB
Puertos	24 10/100Mbps
Norma	Soporte IEEE 802.1x Protocolo IEEE 802.1D Spanning-Tree Clase de servicio IEEE 802.1p (CoS) priorización VLAN IEEE 802.1Q 802.1s IEEE IEEE 802.1w
Protocolo de gestión	SNMP v1,v2 CDP
Consumo potencia	45 vatios
Volteje nominal	CA 120

Fuente: Dirección de tecnología de la información ITCA

3.5.3 Switch SG300-28

Es un switch de capa 2, se muestra en la Figura 22; en la topología de red existen ocho dispositivos de estas características, y sus especificaciones técnicas se detallan en la tabla 13.

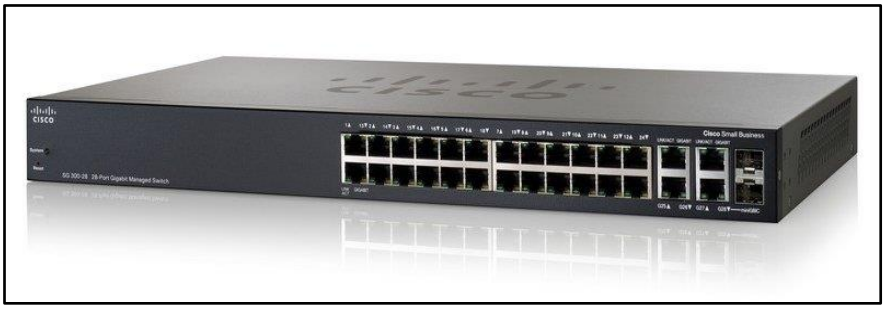


Figura 22. Switch CISCO SG300-28

Fuente: Recuperado de http://www.cisco.com/c/dam/en/us/products/collateral/switches/small-business-smart-switches/300_Series_Switches_DS_FINAL.pdf

Tabla 13. Especificaciones técnicas del Switch SG300-28

Especificaciones técnicas SG300-28	
Memoria flash	**16MB**
Memoria CPU	**128MB**
Capacidad de switching	**56,0 Gbps**
Velocidad de envio (paquetes de 64 Bytes)	**41,67 (mpps)**
Vlans	**Máximo 4096,simultaneas basadas en 802.1Q**
Puertos	**28 Gigabit Ethernet**
Tipo cableado	**Par trenzado UTP, categoría 5 o superior para 100BASE-T**
Norma	**Soporte IEEE 802.1x, Protocolo de expansión múltiple mediante 802.1s , VLAN IEEE 802.1Q**
Protocolo de gestión	**SNMP v1,v2 CDP**
Consumo de energía	**110 V**

Fuente: Dirección de tecnología de la información ITCA

3.5.4 Switch SG200-26

Es un switch de capa 2, se muestra en la Figura 23; en la topología de red existen seis dispositivos de estas características, cuyas especificaciones técnicas se detallan en la tabla 14.

Figura 23. Switch CISCO SG200-26

Fuente: Recuperado de http://www.cisco.com/c/dam/en/us/products/collateral/switches/small-business-smart-switches/300_Series_Switches_DS_FINAL.pdf

Tabla 14. Especificaciones técnicas del Switch SG200-26

Especificaciones técnicas SG200-26	
Memoria flash	16MB
Memoria CPU	128MB
Capacidad de switching	52 Gbps
Velocidad de envio (paquetes de 64 Bytes)	38,69 (mpps)
Vlans	Máximo 256,simultaneas basadas en 802.1Q
Puertos	28 Gigabit Ethernet
Tipo cableado	Par trenzado UTP, categoría 5 o superior para 100BASE-T
Norma	Soporte IEEE 802.1x, cpmpatibilidad con STP según estándar 802.1d, Protocolo de expansión múltiple mediante 802.1s , VLAN IEEE 802.1Q
Alimentación	**Tipo Ethernet POE**
Consumo de energía	**100 V**

Fuente: http://www.cisco.com/c/dam/en/us/products/collateral/switches/small-business-200-series-unmanaged-switches/data_sheet_c78-634369_Spanish.pdf

3.5.5 Central telefónica UC560-FXO-K9

La Figura 24 muestra la central telefónica que se utiliza en la red interna del ITCA, la cual tiene las características indicadas a continuación.

- Solución todo en uno basada en IP, diseñada para empresas en crecimiento con un máximo de cinco sitios conectados en red con marcado entre oficinas.

- Es un dispositivo de comunicaciones unificadas asequible que proporciona capacidades de comunicaciones de voz y datos, buzón de voz, contestador automático.

- Opciones de implementación flexibles para el procesamiento de llamadas, que incluyen una centralita privada (PBX) o el modo de sistema clave para una transmisión simple al sistema nuevo basada en el sistema telefónico existente.

- Contestador automático y mensajes de voz con todas las funciones que ayudan a mejorar la comunicación entre empleados y con los clientes.

- Enlace troncal del protocolo de inicio de sesión (SIP) económico e incorporado con configuraciones predeterminadas de los proveedores importantes.

- Los tres puertos de expansión Gigabit Ethernet se pueden usar con switches Cisco Small Business Pro ESW serie 500 con alimentación por Ethernet (PoE) para alimentar teléfonos IP, puntos de acceso y otros dispositivos SBCS.

Figura 24. Central Telefónica CISCO 560

Fuente: Recuperado de http://www.computadoresbogota.com/articulos/activos/catalogos/Cisco%20UC560-BRI-K9.pdf

3.5.6 Video vigilancia NVR (grabador de video de red)

La Figura 25 muestra el sistema de vigilancia que se utiliza en la red interna del ITCA, la cual tiene las características indicadas a continuación.

- Un NVR es un dispositivo físico o un software que se instala en una computadora, y administra las cámaras IP.

- Un NVR es muy similar a un DVR, la diferencia es que el DVR digitaliza, graba y administra imágenes enviadas desde cámaras de seguridad analógicas, en cambio un NVR, graba y administra imágenes ya digitales las cuales son enviadas desde las cámaras IP a través de una red.

- Se utiliza para cámaras de seguridad IP. Los NVR Stand Alone son un equipo físico (electrónica y software embebido) en un gabinete cerrado.

Figura 25. Video Vigilancia HIK VISION

Fuente: Recuperado de http://www.seagate.com/la/es/solutions/video-surveillance-systems/nvr-camera-systems/

CAPÍTULO IV

4 Análisis de riesgos en base a la metodología NIST SP 800 - 30

Para la realización del análisis de riesgo se utilizara la Guía del Instituto Nacional de estándares y tecnología NIST SP 800-30, con el fin de conocer los niveles actuales de seguridad de la información e identificar los requerimientos de seguridad en la red de Datos del Instituto Tecnológico Superior "José Chiriboga Grijalva".

4.1 Importancia del Análisis del riesgo.

El análisis de riesgo, se transforma en una herramienta importante para sustentar los incidentes de seguridad así como también para justificar una posible inversión y orientar los recursos de manera costo-beneficiosa para cualquiera entidad. Este tipo de análisis nos permite determinar a qué nivel dentro de la organización y en qué áreas, la seguridad tendrá jurisdicción.

4.1.1 Propósito del análisis de riesgo.

El análisis de riesgo tiene como propósito determinar los componentes de un sistema que requieren protección, las vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar el grado de riesgo.

4.1.2 Metodología de la evaluación del riesgo.

La metodología que se va a utilizar para la evaluación de riesgos en la red de Datos del Instituto Tecnológico Superior "José Chiriboga Grijalva", se ha tomado de la "Guía de Gestión de Riesgos para Sistemas de Tecnología de la Información "publicada por NIST 800 en su publicación especial número 30.

La guía Americana Internacional descrita por el (NIST); Instituto Nacional de Normas y Tecnología con sus siglas en inglés (National Institute of Standards and Technology). Documento que fue creado en el año 2002, y se encarga de contribuir con el proceso que debe llevarse a cabo en la gestión de riesgos. Con la finalidad de gestionar, controlar y mitigar el riesgo que se pueda evidenciar, dentro de una organización.
Esta Guía está estructurada por cinco secciones, que se describen a continuación:

- Sección 1: Introducción,
- Sección 2: Visión de la Gestión de Riesgos
- Sección 3: Evaluación del Riesgo
- Sección 4: Mitigación del Riesgo
- Sección 5: Evaluación y Valoración.

De acuerdo al alcance de este proyecto solo se concentrará en la sección 3: Evaluación del Riesgo, como un precedente para el evidenciar tanto amenazas y

vulnerabilidades que la red de datos del Tecnológico ITCA, presenta tomando en cuenta que esta guía ya define los pasos necesarios que deben complementarse para el análisis del riesgo.

4.2 Pasos de la metodología de evaluación del riesgo según la Guía NIST SP 800 - 30

La metodología de análisis y evaluación de riesgos está compuesta por nueve (9) pasos primarios, que se describen a continuación.

- Paso 1 - Caracterización de sistemas
- Paso 2 - Identificación de amenazas
- Paso 3 - Identificación de vulnerabilidades
- Paso 4 - Análisis de controles
- Paso 5 - Determinación de probabilidades
- Paso 6 - Análisis de impacto
- Paso 7 - Determinación de riesgos
- Paso 8 - Recomendaciones de control
- Paso 9 - Documentación de resultados

La figura 26 muestra en resumen la metodología de análisis y evaluación de riesgo de la norma NIST SP 800-30.

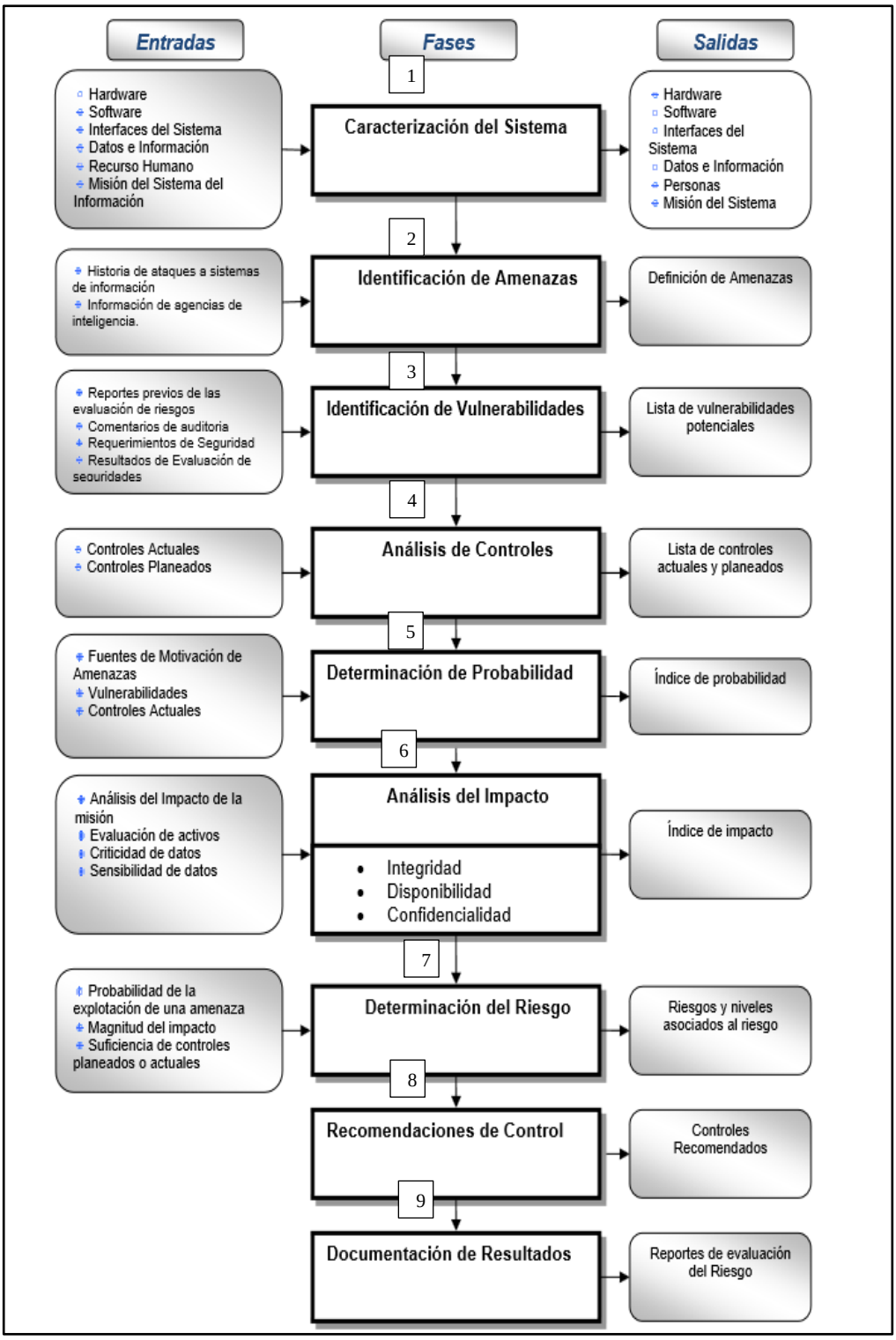


Figura 26. Metodología del análisis de riesgo

Fuente: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

4.2.1 Resumen teórico de la metodología de evaluación del riesgo según la Guía NIST SP 800 - 30.

A continuación se describe un resumen de la norma para detallar como cada paso debe ser desarrollado.

4.2.1.1 Caracterización de sistemas.

En el análisis de riesgos, el primer paso es definir el alcance del esfuerzo. En este paso, se identifican los límites del sistema de tecnología de la información que va a ser analizado, y los recursos que componen dicho sistema.

La caracterización de un sistema de tecnología de la información establece el alcance del esfuerzo de evaluación de riesgos, establece los límites de la autorización operacional y provee información relacionada con el hardware, software, conectividad, personal de soporte y áreas responsables, esenciales para la definición de los riesgos.

4.2.1.2 Identificación de Amenazas.

La meta de este paso es identificar las principales fuentes potenciales de amenazas y recopilar la información de las amenazas, la lista de fuentes de amenazas aplicables al sistema de tecnología de la información en evaluación.

4.2.1.3 Identificación de vulnerabilidades.

El análisis de las amenazas de un sistema de tecnología de la información incluye el análisis de las vulnerabilidades asociadas al ambiente del sistema. En este paso se desarrollar una lista de vulnerabilidades del sistema (defectos o debilidades) que podrían ser explotadas por fuentes de amenazas potenciales.

4.3.1.4 Análisis de Controles.

Se basa en el análisis de los controles que se encuentran implementados o cuya implementación está planeada por la entidad para minimizar o eliminar la probabilidad de que las amenazas exploten las vulnerabilidades del sistema.

Los controles de seguridad reúnen controles técnicos y no técnicos. Los controles técnicos son las protecciones incorporadas en el hardware, software o firmware (por ejemplo, mecanismos de control de acceso, mecanismos de identificación y autenticación, métodos de encripción, software de detección de intrusos, actualizaciones, parches, etc.).

Los controles no técnicos son controles administrativos y operacionales, tales como políticas de seguridad, procedimientos operacionales, metodologías y seguridad del personal, física y ambiental.

4.2.1.5 Determinación de la Probabilidad.

Se define como la probabilidad de que una vulnerabilidad pueda ser explotada por una fuente de amenaza y se puede describir como Alta, Mayor, posible, no esperada y remota.

Se deben tener en cuenta los siguientes factores a la hora de construir una escala de probabilidad que mida el grado en que pueden ser explotadas las vulnerabilidades existentes:

- Motivos de las fuentes de amenazas y su dimensión (capacidad de hacer daño).
- Naturaleza de las vulnerabilidades.
- Existencia y efectividad de los controles existentes.

4.2.1.6 Análisis de Impacto.

Se determina el impacto adverso resultante de una explotación exitosa de una amenaza sobre una vulnerabilidad.

4.2.1.7 Determinación del riesgo.

Las recomendaciones de control son los resultados del proceso de evaluación de riesgos y aportar información al proceso de mitigación de riesgos,

4.2.1.8 Recomendaciones de control.

La meta de las recomendaciones de control es reducir el nivel de riesgo encontrado en los activos del sistema y de los datos a un nivel aceptable. Es necesario tener en cuenta los siguientes factores:

- Efectividad de las opciones recomendadas.
- Legislación y regulaciones existentes.
- Política organizacional
- Impacto operacional
- Seguridad y confiabilidad

4.2.1.9 Documentación de resultados.

Una vez que se ha completado la evaluación del riesgo se ha determinado la amenaza y vulnerabilidades, Riesgos Evaluados, y los controles previstos recomendados, los resultados deben ser documentados .

4.3 Desarrollo de la metodología de evaluación del riesgo según la Guía NIST SP 800 - 30 para la red de datos del Tecnológico ITCA.

4.3.1 Paso 1: Caracterización de los sistemas.

Para el análisis de riesgo se han dividido los sistemas de la red de datos del tecnológico ITCA en cinco grupos de evaluación dentro de los que consta los siguientes que se detallan en la lista:

- Equipos de redes y comunicación
- Servidores de la red
- Host de usuario
- Host de administrativos
- Recurso humano

El proceso de la recopilación de la información es uno de los procesos más largos que se realiza al momento de caracterizar los sistemas, debido a que muestra el total de activos físicos a identificar para la evaluación del riesgo.

4.3.1.1 Calculo del nivel de importancia (NI) para los activos dentro de la caracterización de sistemas del Tecnológico ITCA.

Se determina como nivel de importancia (NI) a cada grupo de activos dentro de la institución en base a tres factores que son: confidencialidad, integridad y disponibilidad. A continuación se describe a cada uno de los factores involucrados para dicho cálculo.

- **Factor de Confidencialidad (Conf):** la confidencialidad asegura que la información sea accesible solo para aquellos usuarios que estén autorizados, es decir, evita que la información sea usada por usuarios no autorizados.

- **Factor de Integridad (Int):** asegura que la información no sea falsa, también asegura exactitud y completitud, es decir, que los datos que se han recibido y/o se han recuperado sean exactamente los mismos que fueron enviados y/o almacenados, la información no debe tener alguna modificación.

- **Factor de Disponibilidad (Disp):** garantiza que la información se encuentre siempre disponible, que los usuarios autorizados pueden tener acceso a ésta información cuando lo requieran o la necesiten.

Para poder establecer el nivel de importancia (NI) de cada activo, primero se describe las escalas y el criterio que se va a utilizar para tal efecto. Las tablas 15, especifica la escala para los tres factores primordiales en el análisis de la determinación del riesgo.

Tabla 15. Escala de valoración del factor Confidencialidad, Integridad y disponibilidad de los activos de información

FACTOR CONFIDENCIALIDAD (CONF)			**FACTOR INTEGRIDAD (INT)**	**FACTOR DISPONIBILIDAD (DISP)**
Nivel	Categoría	Descripción	Descripción	Descripción
1	**Bajo**	Puede ser revelado o proporcionado a cualquier persona	La modificación de su contenido no afectaría la entrega de servicios.	En caso de que la información no estuviese disponible, las consecuencias en la entrega de servicios podrían ser reducidas.
		Consecuencia imperceptible	**Consecuencia imperceptible**	**Consecuencia imperceptible**
2	**Medio**	Puede ser revelado o proporcionado a sólo usuarios del Tecnológico ITCA	La modificación de su contenido tendría una afectación media en la entrega de servicios.	En caso de que la información no estuviese disponible, las consecuencias en la entrega de servicios podrían ser moderadas.
		Consecuencia moderada	**Consecuencia moderada**	**Consecuencia moderada**
3	**Alto**	Puedes ser revelado solo a personal del Departamento de Sistemas del Tecnológico ITCA	La modificación de su contenido tendría una afectación media en la entrega de servicios.	En caso de que la información no estuviese disponible, las consecuencias en la entrega de servicios podrían ser altas
		Consecuencia alta	**Consecuencia alta**	**Consecuencia alta**
4	**Muy alto**	Puede ser revelado sólo al personal autorizado del departamento de sistemas, si así se autoriza.	La modificación de su contenido afectaría de manera muy relevante en la entrega de servicios	En caso de que la información no estuviese disponible, las consecuencias en la entrega de servicios podrían ser graves
		Consecuencias graves	**Consecuencias graves**	**Consecuencias graves**

Fuente: Recuperado de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

El producto de estos tres factores confidencialidad, integridad y disponibilidad

finalmente revela el Nivel de Importancia (NI) en la entrega de servicio para cada activo de la información.

$$(NI) = Disp \times Int \times Conf$$

Ecuación 1: Nivel de Importancia de los activos

Fuente: Recuperado de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

En la tabla 16 se establece la escala del Nivel de Importancia (NI), el mismo que puede ser mayor a 1 y menor o igual a 64.

Tomando en cuenta que: $1 \geq NI \leq 64$

Tabla 16. Rangos de Importancia de los activos de información.

RANGOS DEL NIVEL DE IMPORTANCIA (NI)		
Nivel	**Categoría**	Descripción
1 A 4	Bajo	Activo de importancia baja para asegurar la confidencialidad, integridad y disponibilidad de la información , asociada a la entrega de servicios a los usuarios de la red del Tecnológico ITCA
5 a 16	Medio	Activo de importancia media para asegurar la confidencialidad, integridad y disponibilidad de la información , asociada a la entrega de servicios a los usuarios de la red del Tecnológico ITCA
17 a 36	Alto	Activo de importancia alta para asegurar la confidencialidad, integridad y disponibilidad de la información , asociada a la entrega de servicios a los usuarios de la red del Tecnológico ITCA
37 a 64	Muy alto	Activo de importancia muy alta para asegurar la confidencialidad, integridad y disponibilidad de la información , asociada a la entrega de servicios a los usuarios de la red del Tecnológico ITCA

Fuente: Recuperado de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

4.3.1.2 Equipos redes de comunicación

Los equipos de comunicaciones y redes con las que cuenta el instituto se dividen en Router, y switchs que se describen las tablas 17 y 18.

Tabla 17. Caracterización de los Routers de comunicación.

EQUIPO	CANTIDAD	MODELO	DESCRIPCIÓN O UBICACIÓN
Router TELCONET	1	CISCO 1900	Data Center, planta baja, rack 1.
Router ITCA	1	CISCO 881	Data Center, planta baja, rack 1.

Fuente: Dirección de Sistemas Tecnológico ITCA

Tabla 18. Caracterización de los switch de comunicación

EQUIPO	CANTIDAD	MODELO	DESCRIPCIÓN O UBICACIÓN
Switch de Core capa 3	1	CISCO 2950 - 48	Data Center, Planta baja, rack 1.
Switch de conmutación capa 2	1	CISCO SG 200-26	Data Center, Planta alta 1, rack 1.
Switch de conmutación capa 2	1	CISCO SG 200-26	Data Center, Planta alta 1, rack 1.
Switch de conmutación capa 2	1	CISCO SG 200-26	Data Center, Planta baja, rack 1.
Switch de conmutación capa 2	1	CISCO SG 200-26	Data Center, Planta baja, rack 1.
Switch de conmutación capa 2	1	CISCO SG 200-26	Data Center, Planta baja, rack 1.
Switch de conmutación capa 2	1	CISCO SG 200-26	Data Center, Planta baja, rack 1.

Switch de Conmutación capa 2	1	CISCO SG 300-28	Data Center, Planta baja, rack 2.
Switch de Conmutación capa 2	1	CISCO SG 300-28	Data Center, Planta baja, rack 2.
Switch de Conmutación capa 2	1	CISCO SG 300-28	Data Center, Planta baja, rack 2.
Switch de Conmutación capa 2	1	CISCO SG 300-28	Data Center, Planta baja, rack 2.
Switch de Conmutación capa 2	1	CISCO SG 300-28	Data Center, Planta baja, rack 2.
Switch de Conmutación capa 2	1	CISCO SG 300-28	Data Center, Planta baja, rack 2.
Switch de conmutación capa 2	1	ADVANTEK NETWORK-24	**Data Center, Planta baja, rack 2.**

Fuente: Dirección de Sistemas Tecnológico ITCA

- Servidores de la red

Los servidores de la red representan una estructura unificada de gestión y procesamiento de información para el tecnológico ITCA en la tabla 19 se detallan los servidores que están en calidad operativa actualmente.

Tabla 19. Caracterización de los servidores de la red

IDENTIFICATIVO	UBICACIÓN	DESCRIPCIÓN	CARACTERÍSTICAS
Servidor FTP	Data Center, Planta baja, rack 3.	Servidor de correo interno para las diferentes carretas, rectorado , secretaria, seguridad, vinculación y sistemas	Servidor dedicado Centos -Intel Core i3 Quad-Core.
Servidor WEB	Data Center, Planta baja, rack	alojar sitios y aplicaciones, las cuales son accedidas por los usuarios utilizando un navegador que se comunica con el servidor utilizando el protocolo HTTP	Servidor HP proliant G7 -360
Servidor PROXY	Data Center, Planta baja, rack	Servidor intermediario entre los equipos de una red de área local LAN ITCA y la Red WAN	Servidor HP proliant G7- 380
Servidor FACTURACIÓN	Data Center, Planta baja, rack	Facturación interna de pensiones y matriculas del instituto	Servidor dedicado Centos -Intel Core i5 Quad-Core.
Servidor BACKUP	Data Center, Planta baja, rack	Copia de respaldo de todo el volumen de archivos guardados en cada servidor de la institución.	Servidor dedicado Centos- Intel Core i3 Quad-Core.
Servidor ACTIVE DIRECTORY	Data Center, Planta baja, rack	Estructura de manera jerárquica la red permite organizar usuarios, grupos de usuarios, permisos de acceso a la red.	Servidor dedicado Windows server 2012 -Intel Core i3 Quad-Core.

Fuente: Dirección de Sistemas Tecnológico ITCA

- Host de usuarios

Los host de usuarios estan divididos en cinco grupos de acuerdo a los laboratorios del Tecnologico ITCA, como se indica en la tabla 20 .

Tabla 20. Caracterización de los host de usuarios

LABORTORIO	# DE PC´s	IDENTIFICACION	UBICACIÓN
1	20	LAB1-PC1-LAB1-PC20	Planta baja, area laboratorios , Lab 1
2	20	LAB2-PC1-LAB2-PC2	Planta baja, área laboratorios , Lab 2
3	20	LAB3-PC1-LAB3-PC20	Planta baja, área laboratorios , Lab 3
4	20	LAB4-PC1-LAB4-PC20	Planta baja, área laboratorios , Lab 4
5	20	LAB5-PC1-LAB5-PC20	Planta baja, área laboratorios , Lab 5

Fuente: Dirección de Sistemas Tecnológico ITCA

- Host de administrativos

Dentro de este grupo de usurios se encuantran los host personales y de escritorio identificados de cada una de los administrativos y docentes de las carreras del instituto la tabla 21 , muestra una sección de los usuarios de la carrera de Administarción de empresas y rectorado , la tabla completa se encuantra en el Anexo 1.

Tabla 21. Caracterización de los host de administrativos

CARRERA ADE	
DIRECCIÓN IP	USUARIO
172.20.3.41	LILIANA TAPIA
172.20.3.42	FLOR RODRIGUEZ
172.20.3.43	JORGE SUAREZ
172.20.3.44	MIKAELA POSSO
172.20.3.45	GUIDO GUERRERO
172.20.3.46	MANUEL HIDALGO
172.20.3.47	----------
172.20.3.48	BAYARDO SALAZAR
172.20.3.49	JORGE SUAREZ
172.20.3.50	JORGE SUAREZ

Fuente: Dirección de Sistemas Tecnológico ITCA

- Recurso humano

El recurso humano es quiza el entorno más critico para la caracerización y evaluación del riegos dentro de la institucion ya que cada uno de los usurios que pertencen a ese grupo, desempeñan funciones diferentes de acuerdo a su rol de empleo. Para este caso se toma al recurso humano como un solo activo de avaluación, es decir usuarios invitados, estudiantes, area de sistemas etc ,de la red de datos**.**

4.3.2 Paso 2: identificación de amenazas.

Para la identifición de amenazas, se han evaluado con los mismos grupos de activos de la caracterización de sistemas, antes de realizar este paso se describe el proceso

de identificación de cada una de las amenazas que pueden presentarse dentro de la isntitución.

Una fuente de amenaza se define como cualquier circunstancia o evento el cual pueda causar daños a un sistema o activos de la institución. Las fuentes comunes de amenazas son las personas, la naturaleza y el ambiente.

4.3.2.1 Amenazas naturales.

Se describen las siguientes amenazas: Inundaciones, terremotos, tornados, deslizamientos de tierra, avalanchas, tormentas Eléctricas y otros eventos similares

4.3.2.2 Amenazas humanas

Se describen los eventos activados o causados por las personas, tales como actos no intencionados (errores en la entrada de datos) o malintencionados (ataques a la red, activación de software malicioso, acceso no autorizado a información confidencial).

4.3.2.3 Amenazas ambientales

Se describen las faltas prolongadas de energía eléctrica, polución, químicos, dispersión de líquidos.

4.3.3 Paso 3: Identificación de las vulnerabilidades

La vulnerabilidad pueden llevarse a efecto sea por una falla o debilidad en los activos de evaluación de riesgo. Una falla puede desencadenar en una potencial fuente de amenaza que se describen en la identificación de amenazas.

4.3.4 Paso 4: Análisis de controles

En este paso se describen si existen o estan dentro de una planifiación los controles para eliminar o mitigar la probalilidad de que una amenaza explote en amenaza.

4.3.5 Paso 5: Determinación de la probabilidad

La probabilidad se puede presentar cuando algún tipo de vulnerabilidad pueda llegar a ser una amenaza inminente .Para la determinación de la probabilidad se usan los niveles definidos por la guía NIST SP 800-30. La tabla 22 describe los niveles de probabilidad de una amenaza a ser evaluado en los activos de la institución.

Tabla 22. Estado de la probabilidad de amenazas

NIVEL DE PROBABILIDAD	DEFINICIÓN DE LA PROBABILIDAD
Alta	La fuente de la amenaza es altamente motivada y los controles para prevenir que se explote una vulnerabilidad son inefectivos
Media	La fuente de la amenaza es motivada y los controles para prevenir que se explote una vulnerabilidad impiden la explotación exitosa de una vulnerabilidad
Baja	La fuente de la amenaza carece de motivos y los controles de prevención implementados previenen o dificultan significativamente la explotación de la vulnerabilidad.

Fuente: Recuperado de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

4.3.6 Paso 6: Análisis del impacto

El paso más importante en la medición del nivel de riesgo es determinar el impacto resultante que una amenaza explota exitosamente una vulnerabilidad. La tabla 23 muestra la definición de la magnitud del impacto que describe la guía.

Definición de la magnitud del impacto

Tabla 23. Definición de la magnitud del impacto

MAGNITUD DE IMPACTO	DEFINICIÓN DEL IMPACTO
Alta	La explotación de una vulnerabilidad: Puede resultar en una alta pérdida de los principales activos tangibles o recursos. Puede significar violación, daño o dificultad de la misión reputación o interés de la institución. Puede resultar en muerte humana o una lesión seria
Media	La explotación de una vulnerabilidad: Puede resultar en una pérdida de los activos tangibles o recursos. Puede significar violación, daño o dificultad de la misión reputación o interés de la institución. Puede resultar en una lesión humana.
Baja	La explotación de una vulnerabilidad: Puede resultar en una pérdida de algunos activos. Puede afectar notablemente a la misión o intereses de la institución.

Fuente: Recuperado de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

4.3.7 Paso 7: Determinación del riesgo

Este paso permite evaluar el nivel del riesgo para los activos de la institución. Para el cálculo del nivel del riesgo se realiza una matriz, la misma que toma el nombre de matriz del nivel del Riesgo de acuerdo a la guía y que está dada en la tabla 24.

Para el cálculo de la matriz del nivel del Riesgo se emplea una matriz de 3x3, donde la filas corresponden a la probabilidad de amenaza (alta, media y baja) y las columnas al impacto de la amenaza (alto, medio y bajo).

La escala del nivel de riesgo es la siguiente:

- Baja: mayor a 1 hasta 10
- Media: mayor a 10 hasta 50
- Alta: mayor a 50 hasta 100

Tabla 24. Matriz del nivel de riesgo

Probabilidad de amenza	IMPACTO		
	Bajo (1-10)	Medio (10-50)	Alto (50-100)
Alta (1.0)	Bajo 10 x 1.0 = 10	Medio 50 x 1.0 = 50	Alto 100 x 1.0 = 100
Media (0.5)	Bajo 10 x 0.5 = 5	Medio 50 x 0.5 = 25	Medio 100 x 0.5 = 50
Baja (0.1)	Bajo 10 x 0.1 = 10	Bajo 50 x 0.1 = 50	Bajo 100 x 0.1 = 10

Fuente: Recuperado de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

4.3.8 Paso 8: Recomendaciones de control

Determina el impacto adverso resultante de una explotación exitosa de una amenaza sobre una vulnerabilidad.

De igual manera que en El Paso anterior, para el análisis del impacto se va a tomar en cuenta las magnitudes descritas en la guía NIST SP 800-30

El propósito de este paso es valorar el nivel de riesgo de un sistema de TI. La determinación del riesgo para una amenaza/vulnerabilidad en particular se expresa en función de:

- La probabilidad que una fuente de amenaza intente explotar una vulnerabilidad.
- Lo apropiado de los controles existentes o planeados para reducir o eliminar los riesgos.

4.3.9 Paso 9: Documentación de los resultados

Sólo cuando el análisis de riesgos finaliza se identificaron las fuentes de amenazas y vulnerabilidades, se evalúan los riesgos y se emitieron recomendaciones de control, los resultados se documentan en un informe oficial.

Un informe de análisis y evaluación de riesgos es un reporte de ayuda para la administración, los responsables de la misión, la toma de decisiones, el cálculo de

presupuestos y la gestión de cambios administrativos y operacionales en caso de ser requeridos.

4.4 Evaluación y control del riesgo

La realización de esta evaluación de riesgo implica un antecedente para determinar las causas de problemas tanto de riesgo, amenas y vulnerabilidades de los cinco activos del sistema que conforman la red de datos del tecnológico ITCA , para ello se han realizado entrevistas, revisión de las instalaciones, visitas en el sitio escaneo de puertos etc.

Esto permite a los encargados de la red de datos identificar, evaluar y reducir el riesgo a un nivel aceptable, mediante una solución posible de control apropiado.

Como se había mencionado en el paso 1 que corresponde a la caracterización de los sistemas, donde se identifican cinco activos para la evaluación, se procede a calcular el nivel de importancia que tiene cada uno de los activos, que se desarrolla en la tabla 25,26, 27, 28 , 29 a continuación.

Tabla 25. Cálculo de Nivel de Importancia para el activo equipos y redes de comunicación

CALCULO DEL NIVEL DE IMPORTANCIA						
ACTIVO	**TIPO DE ACTIVO**	**Conf**	**Int**	**Dis**		**NI**
	Router TELCONET	4	4	4	64	Muy alto

	Router ITCA	4	4	4	64	Muy alto
EQUIPOS Y REDES DE COMUNICACIÒN	Switch de Core capa 3 CISCO 2950 - 48	3	4	3	36	Alto
	Switch de conmutación capa 2 CISCO SG 200-26	3	4	3	36	Alto
	Switch de conmutación capa 2 CISCO SG 200-26	3	4	3	36	Alto
	Switch de conmutación capa 2 CISCO SG 200-26	3	4	3	36	Alto
	Switch de conmutación capa 2 CISCO SG 200-26	3	4	3	36	Alto
	Switch de conmutación capa 2 CISCO SG 200-26	3	4	3	36	Alto
	Switch de conmutación capa 2 CISCO SG 200-26	3	4	3	36	Alto
	Switch de conmutación capa 2 CISCO SG 300-28	3	4	3	36	Alto
	Switch de conmutación capa 2 CISCO SG 300-28	3	4	3	36	Alto
	Switch de conmutación capa 2 CISCO SG 300-28	3	4	3	36	Alto
	Switch de conmutación capa 2 CISCO SG 300-28	3	4	3	36	Alto

	Switch de conmutación capa 2 CISCO SG 300-28	3	4	3	36	Alto
	Switch de conmutación capa 2 CISCO SG 300-28	3	4	3	36	Alto
	Switch de conmutación capa 2 ADVANTEK NETWORK-24	3	4	3	36	Alto

Fuente: Dirección de Sistemas Tecnológico ITCA

Tabla 26. Cálculo de Nivel de Importancia para el activo servidores de la red.

CALCULO DEL NIVEL DE IMPORTANCIA						
ACTIVO	**TIPO DE ACTIVO**	**Conf**	**Int**	**Dis**		**NI**
SERVIDORES DE LA RED	Servidor FTP	3	3	2	18	Alto
	Servidor WEB	3	3	2	18	Alto
	Servidor PROXY	3	3	3	27	Alto
	Servidor FACTURACIÓN	4	4	4	64	Muy alto
	Servidor BACKUP	3	3	3	27	Alto
	Servidor ACTIVE DIRECTORY	3	3	3	27	Alto

Fuente: Dirección de Sistemas Tecnológico ITCA

Tabla 27. Cálculo de Nivel de Importancia para el activo host de usuarios

CALCULO DEL NIVEL DE IMPORTANCIA						
ACTIVO	**TIPO DE ACTIVO**	**Conf**	**Int**	**Dis**		**NI**
HOST DE USUARIOS	Laboratorio 1	2	3	2	12	Medio
	Laboratorio 2	2	3	2	12	Medio
	Laboratorio 3	2	3	2	12	Medio
	Laboratorio 4	2	3	2	12	Medio
	Laboratorio 5	2	3	2	12	Medio

Fuente: Dirección de Sistemas Tecnológico ITCA

Tabla 28. Cálculo de Nivel de Importancia para el activo host de administrativos

CALCULO DEL NIVEL DE IMPORTANCIA						
ACTIVO	**TIPO DE ACTIVO**	**Conf**	**Int**	**Dis**		**NI**
HOST DE ADMINISTRATIVOS (se toman cinco grupos como muestra del anexo A)	Rectorado	2	3	3	18	Alto
	Carrera ADE	2	3	3	18	Alto
	Carrera DIN	2	3	3	18	Alto
	Vinculación	2	3	3	18	Alto
	Facturación	2	3	3	18	Alto

Fuente: Dirección de Sistemas Tecnológico ITCA

Tabla 29. Cálculo de Nivel de Importancia para el activo recurso humano

CALCULO DEL NIVEL DE IMPORTANCIA						
ACTIVO	**TIPO DE ACTIVO**	**Conf**	**Int**	**Dis**	**NI**	
RECURSO HUMANO (se evaluan los mas presindibles)	Estudiantes	2	3	3	18	Alto
	Área de sistemas	2	3	3	18	Alto
	Invitados	2	3	3	18	Alto

Fuente: Dirección de Sistemas Tecnológico ITCA

4.5 Determinación de amenazas y de las acciones de la amenaza

En la tabla 30 se describen las amenazas que se han evidenciado y el impacto que se generaría en caso de que una amenaza llegue a materializarse dentro del tecnológico ITCA

Se han tomado como referencia tres tipos de causas a evaluar: Tecnológicas, Ambientales, y humanas

Tabla 30. Determinación de amenazas e impacto

TIPO	#	AMENAZAS	IMPACTO
TECNOLOGICAS	1	Daño del hardware	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.
	2	Daño del software	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.
	3	Daño de los medios de trasmisión	El activo no funciona correctamente e impide el servicio, por daño total del medio de trasmisión.
	5	Inhibición de los puertos	Los puertos no funcionan correctamente por desconexión e impide el servicio.
	6	Falla eléctrica	Desconexión total de los servicios para los usuarios, impide el normal funcionamiento.
	7	Falla del sistema de alimentación ininterrumpida (UPS)	Los activos dejan de funcionar correctamente por perdida de energía eléctrica, impide el servicio para todos los usuarios.
	8	Software no licenciado	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.
	9	Software desactualizado	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.
	10	Daño del sistema de aire acondicionado	Los activos que se encuentran dentro del área de comunicaciones o datacenter, pueden presentar algún tipo de afectación de modero a grave.
	11	Ataque a la red	Pérdida parcial o total de la información critica
	12	Falla de backup	Activo no configurado correctactamente o no existe tal servicio

Figura 30. Determinación de amenazas e impacto (continuación)

TIPO	#	AMENAZAS	IMPACTO
A M B I E N T A L E S	1	Terremotos/sismos	Daño total o parcial de la infraestructura de red de datos. Perdidas económicas y/o humanas.
	2	Erupciones volcánicas	Daño total o parcial de la infraestructura de red de datos.
	3	Deslizamientos	Perdidas económicas y/o humanas.
	4	Inundaciones	Daño total o parcial de la infraestructura de red de datos.
	5	Incendios	Perdidas económicas y/o humanas.

Figura 30. Determinación de amenazas e impacto (continuación)

TIPO	#	AMENAZAS	IMPACTO
H U M A N A S	**1**	Desconfiguración involuntaria	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.
	2	Desconexión del puerto	Los puertos no funcionan correctamente por desconexión e impide el servicio.
	3	Violación de la configuración de los activos de comunicaciones	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.
	4	Ingreso de personal no autorizado	Falla momentánea de los servicios, perdida de activos, pérdida económica, y violación de la confidencialidad.
	5	Suplantación de identidad	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.
	6	Error de etiquetación de los activos	Los activos pueden verse afectados, cambios inesperados de la configuración, desencadena en pérdida total o parcial de la información crítica.
	7	Mantenimiento inadecuado de los activos	Daño total o parcial de los activos de hardware o software, limita el funcionamiento de los servicios
	8	Robo o pérdida de los activos	Inhabilitación de los servicios, incluye pérdidas económicas
	9	Respaldos no adecuados	Perdida de información importante o crítica del activo afectado
	10	Robo o pérdida de la información contenida en los activos	Perdida de información importante o crítica del activo afectado
	11	Ataques a la red	Pérdida o daño de los activos, limita el funcionamiento de los servicios

Fuente: Dirección de Sistemas Tecnológico ITCA

4.6 Resultado de la evaluación del riesgo

Para el resultado de la evaluación del riesgo se encuentran las vulnerabilidades que se asocian a cada una de las amenazas para los tres tipos de causas , la tabla 31 muestra en resumen cada amenaza y la vulnerabilidad que puedes ser explotada.

Tabla 31. Evaluación de amenazas/vulnerabilidades

TIPO	#	AMENAZAS	VULNERABILIDAD
TECNOLOGICAS	**1**	Daño del hardware	No existen los repuestos para el correcto funcionamiento del hardware, falta de presupuesto.
	2	Daño del software	No cuenta con un protocolo de actualización del software.
	3	Daño de los medios de trasmisión	No cuenta con políticas del manejo del cableado estructurado.
	5	Inhibición de los puertos	No cuenta con un protocolo de manejo de puertos.
	6	Falla eléctrica	Sobrecarga de energía Fallas del proveedor de suministro eléctrico. Tableros eléctricos expuestos.
	7	Falla del sistema de alimentación ininterrumpida (UPS)	No existe un protocolo de contención ante un corte inesperado de energía.
	8	Software no licenciado	No se encuentra con las licencias actualizadas.
	9	Software desactualizado	No cuenta con un protocolo de actualización de software.
	10	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.
	11	Ataque a la red	Acceso a la terminal de administración. Uso de contraseñas no robustas o por defecto.
	12	Falla de backup	No cuenta con una política de respaldo total o parcial de la información.

Tabla 32. Evaluación de amenazas/vulnerabilidades (continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD
	1	Terremotos/sismos	El edificio no cuenta con una estructura antisísmica. Ibarra se encuentra en una zona propensa a sismos.
A **M** **B** **I** **E** **N** **T** **A** **L** **E** **S**			No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.
	2	Erupciones volcánicas	Ibarra se encuentra en una zona geográfica rodeada de volcanes. No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.
	3	Deslizamientos	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.
	4	Inundaciones	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.
	5	Incendios	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.

Tabla 33. Evaluación de amenazas/vulnerabilidades (continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD
	1	Desconfiguración involuntaria	No existe un protocolo adecuado de manejo de claves de los activos importantes.
	2	Desconexión del puerto	No cuenta con un protocolo de manejo de puertos. No cuenta con politicas del manejo del cableado estructurado.

	3	Violación de la configuración de los activos de comunicaciones	No existe una politica periodica de actualizaciones de calves.
H U M A N A S	**4**	Ingreso de personal no autorizado	No se cuenta con un registro de acceso, de personas a al departamento de sistemas
	5	Suplantación de identidad	No existe una adecuada gestión de claves de usuarios podrían ser compartidas o divulgadas inadecuadamente.
	6	Error de etiquetación de los activos	No cuenta con información actualizada de los activos
	7	Mantenimiento inadecuado de los activos	No cuenta con una politica de mantenimiento períodica de los activos
	8	Robo o pérdida de los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas
	9	Respaldos no adecuados	No existe una política adecuada de respaldar la información.
	10	Robo o pérdida de la información contenida en los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas.
	11	Ataques a la red (delincuencia, crackers, hackers, ex - empleados, personas mal intencionadas)	Acceso de personal no autorizado. No existe un mecanismo de control perimetral de la red.
H			No existe un control

U		eficiente de acceso a la
M		red inalámbrica (redes
A		abiertas).
N		No cuenta con políticas
A		de uso de la red.
S		No cuenta con políticas de manejo de la información confidencial.
		No cuenta con políticas de seguridad de sistemas operativos.
		No cuenta con políticas de seguridad de los activos de comunicaciones.
		No cuenta con política de manejo de claves de acceso para empleados y ex –empleados.

Fuente: Dirección de Sistemas Tecnológico ITCA

4.7 Acciones de mitigación del riesgo

Se describen las acciones de mitigación del riesgo para cada uno de los grupos de activos de la evaluación de riesgo realizado anteriormente. La tabla 34, muestra los controles de mitigación para el activo equipos de redes y comunicación.

Tabla 32. Controles mitigadores para el activo equipos de redes y comunicación.

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
TECNOLOGICAS	**1**	Daño del hardware	No existen los repuestos para el correcto funcionamiento del hardware, falta de presupuesto.	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.	Ninguna
	2	Daño del software	No cuenta con un protocolo de actualización del software.	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.	Ninguna
	3	Daño de los medios de trasmisión	No cuenta con políticas del manejo del cableado estructurado.	El activo no funciona correctamente e impide el servicio, por daño total del medio de trasmisión.	Aislamiento del cableado estructurado
	5	Inhibición de los puertos	No cuenta con un protocolo de manejo de puertos.	Los puertos no funcionan correctamente por desconexión e impide el servicio.	Habilitación de los puertos de acuerdo al tipo de usuarios
	6	Falla eléctrica	Sobrecarga de energía Fallas del proveedor de suministro eléctrico. Tableros eléctricos expuestos.	Desconexión total de los servicios para los usuarios, impide el normal funcionamiento.	Implementación de sistemas UPS. Poner a buen recaudo los tableros eléctricos.

Tabla 34. Controles mitigadores para el activo equipos de redes y comunicación. (Continuación)

comunicación. (continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
T E C N O L O G I C A S	**7**	Software no licenciado	No se encuentra con las licencias actualizadas.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Adquisición del licenciamiento**
	8	Software desactualizado	No cuenta con un protocolo de actualización de software.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Actualización periódica del software.**
	9	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.	Los activos que se encuentran dentro del área de comunicaciones o datacenter, pueden presentar algún tipo de afectación de modero a grave.	**Ninguna**
	10	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.	Los activos que se encuentran dentro del área de comunicaciones o datacenter, pueden presentar algún tipo de afectación de modero a grave.	**Ninguna**
	11	Ataque a la red	Pérdida parcial o total de la información critica	Pérdida parcial o total de la información critica	**Mantener monitoreo constante de la red, como un IPS para evitar ataques a la red de datos.**
	12	Falla de backup	Activo no configurado correctactamente o no existe tal servicio	Activo no configurado correctactamente o no existe tal servicio	**Ninguna**

Tabla 34. Controles mitigadores para el activo equipos de redes y comunicación. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
AMBIENTALES	**1**	Terremotos/sismos	· El edificio no cuenta con una estructura antisísmica. · Ibarra se encuentra en una zona propensa a sismos. · No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos. Perdidas económicas y/o humanas.	**Ninguna**
	2	Erupciones volcánicas	· Ibarra se encuentra en una zona geográfica rodeada de volcanes. · No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos.	**Ninguna**
	3	Deslizamientos	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Perdidas económicas y/o humanas.	**Ninguna**
	4	Inundaciones	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos.	**Ninguna**
	5	Incendios	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Perdidas económicas y/o humanas.	**Ninguna**

Tabla 34. Controles mitigadores para el activo equipos de redes y comunicación. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
	1	Desconfiguración involuntaria	No existe un protocolo adecuado de manejo de claves de los activos importantes.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Respaldo de configuraciones importantes**
HUMANAS	**2**	Desconexión del puerto	· No cuenta con un protocolo de manejo de puertos. · No cuenta con políticas del manejo del cableado estructurado.	Los puertos no funcionan correctamente por desconexión e impide el servicio.	· **Revisión del cableado estructurado.** · **Habilitación y des habilitación de puertos.**
	3	Violación de la configuración de los activos de comunicaciones	No existe una política periódica de actualizaciones de calves.	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.	**Ninguna**
	4	Ingreso de personal no autorizado	No se cuenta con un registro de acceso, de personas a al departamento de sistemas	Falla momentánea de los servicios, perdida de activos, pérdida económica, y violación de la confidencialidad.	**Ninguna**
	5	Suplantación de identidad	No existe una adecuada gestión de claves de usuarios podrían ser compartidas o divulgadas inadecuadamente.	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.	**Los empleados y estudiantes deben contar con claves y usuarios correctamente identificados.**

Tabla 34. Controles mitigadores para el activo equipos de redes y comunicación. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
HUMANAS	**6**	Error de etiquetación de los activos	No cuenta con información actualizada de los activos	Los activos pueden verse afectados, cambios inesperados de la configuración, desencadena en pérdida total o parcial de la información crítica.	**Se encuentra correctamente etiquetado e identificado**
	7	Mantenimiento inadecuado de los activos	No cuenta con una política de mantenimiento periódica de los activos	Daño total o parcial de los activos de hardware o software, limita el funcionamiento de los servicios	**Ninguna**
	8	Robo o pérdida de los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas	Inhabilitación de los servicios, incluye pérdidas económicas	**Se encuentran correctamente en inventario**
	9	Respaldos no adecuados	No existe una política adecuada de respaldar la información.	Perdida de información importante o crítica del activo afectado	**Ninguna**
	10	Robo o pérdida de la información contenida en los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas.	Perdida de información importante o crítica del activo afectado	**Ninguna**

Tabla 34. Controles mitigadores para el activo equipos de redes y comunicación. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
HUMANAS	**11**	Ataques a la red (delincuencia, crackers, hackers, ex - empleados, personas mal intencionadas)	· Acceso de personal no autorizado. · No existe un mecanismo de control perimetral de la red. · No existe un control eficiente de acceso a la red inalámbrica (redes abiertas). · No cuenta con políticas de uso de la red. · No cuenta con políticas de manejo de la información confidencial. · No cuenta con políticas de seguridad de sistemas operativos. · No cuenta con políticas de seguridad de los activos de comunicaciones. · No cuenta con política de manejo de claves de acceso para empleados y ex – empleados.	Perdida o daño de los activos, limita el funcionamiento de los servicios	**Mantener un constante monitoreo los activos de mayor criticidad. Al ser un activo de suma importancia debe de estar a buen recaudo.**

La tabla 35, muestra los controles de mitigación para el activo servidores de red

Tabla 33. Controles mitigadores para el activo servidores de la red

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
TECNOLOGICAS	**1**	Daño del hardware	No existen los repuestos para el correcto funcionamiento del hardware, falta de presupuesto.	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.	**Respaldar información y configuraciones.**
	2	Daño del software	No cuenta con un protocolo de actualización del software.	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.	**Respaldar información y configuraciones.**
	3	Daño de los medios de trasmisión	No cuenta con políticas del manejo del cableado estructurado.	El activo no funciona correctamente e impide el servicio, por daño total del medio de trasmisión.	**Aislamiento del cableado estructurado**
	5	Inhibición de los puertos	No cuenta con un protocolo de manejo de puertos.	Los puertos no funcionan correctamente por desconexión e impide el servicio.	**Habilitación de los puertos sólo los necesarios.**
	6	Falla eléctrica	· Sobrecarga de energía · Fallas del proveedor de suministro eléctrico. · Tableros eléctricos expuestos.	Desconexión total de los servicios para los usuarios, impide el normal funcionamiento.	**Implementación de sistemas UPS.**

Tabla 35. Controles mitigadores para el activo servidores de la red. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
	7	Software no licenciado	No se encuentra con las licencias actualizadas.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Licenciamiento adecuado**
TECNOLÓGICAS	**8**	Software desactualizado	No cuenta con un protocolo de actualización de software.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Actualización periódica del software.**
	9	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.	Los activos que se encuentran dentro del área de comunicaciones o datacenter, pueden presentar algún tipo de afectación de modero a grave.	**Ninguna**
	10	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.	Los activos que se encuentran dentro del área de comunicaciones o datacenter, pueden presentar algún tipo de afectación de modero a grave.	**Ninguna**
	11	Ataque a la red	Pérdida parcial o total de la información critica	Pérdida parcial o total de la información critica	**Mantener monitoreo cosnante de la red, como un IPS para evitar ataques a la red de datos.**
	12	Falla de backup	Activo no configurado correctactamente o no existe tal servicio	Activo no configurado correctactamente o no existe tal servicio	**Ninguna**

Tabla 35. Controles mitigadores para el activo servidores de la red. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
AMBIENTALES	**1**	Terremotos/sismos	· El edificio no cuenta con una estructura antisísmica. · Ibarra se encuentra en una zona propensa a sismos. · No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos. Perdidas económicas y/o humanas.	**Ninguna**
	2	Erupciones volcánicas	· Ibarra se encuentra en una zona geográfica rodeada de volcanes. · No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos.	**Ninguna**
	3	Deslizamientos	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Perdidas económicas y/o humanas.	**Ninguna**
	4	Inundaciones	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos.	**Ninguna**
	5	Incendios	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Perdidas económicas y/o humanas.	**Ninguna**

Tabla 35. Controles mitigadores para el activo servidores de la red. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
	1	Desconfiguración involuntaria	No existe un protocolo adecuado de manejo de claves de los activos importantes.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Respaldo de configuraciones importantes**
HUMANAS	**2**	Desconexión del puerto	· No cuenta con un protocolo de manejo de puertos. · No cuenta con políticas del manejo del cableado estructurado.	Los puertos no funcionan correctamente por desconexión e impide el servicio.	· **Revisión del cableado estructurado.**
	3	Violación de la configuración de los activos de comunicaciones	No existe una política periódica de actualizaciones de calves.	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.	**Ninguna**
	4	Ingreso de personal no autorizado	No se cuenta con un registro de acceso, de personas a al departamento de sistemas	Falla momentánea de los servicios, perdida de activos, pérdida económica, y violación de la confidencialidad.	**Ninguna**
	5	Suplantación de identidad	No existe una adecuada gestión de claves de usuarios podrían ser compartidas o divulgadas inadecuadamente.	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.	**Los empleados y estudiantes deben contar con claves y usuarios correctamente identificados.**

Tabla 35. Controles mitigadores para el activo servidores de la red. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
	6	Error de etiquetación de los activos	No cuenta con información actualizada de los activos	Los activos pueden verse afectados, cambios inesperados de la configuración, desencadena en pérdida total o parcial de la información crítica.	**Se encuentra correctamente etiquetado e identificado**
HUMANAS	**7**	Mantenimiento inadecuado de los activos	No cuenta con una política de mantenimiento periódica de los activos	Daño total o parcial de los activos de hardware o software, limita el funcionamiento de los servicios	**Ninguna**
	8	Robo o pérdida de los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas	Inhabilitación de los servicios, incluye pérdidas económicas	**Se encuentran correctamente en inventario**
	9	Respaldos no adecuados	No existe una política adecuada de respaldar la información.	Perdida de información importante o crítica del activo afectado	**Ninguna**
	10	Robo o pérdida de la información contenida en los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas.	Perdida de información importante o crítica del activo afectado	**Ninguna**

Tabla 35. Controles mitigadores para el activo servidores de la red. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
HUMANAS	**11**	Ataques a la red (delincuencia, crackers, hackers, ex - empleados, personas mal intencionadas)	· Acceso de personal no autorizado. · No existe un mecanismo de control perimetral de la red. · No existe un control eficiente de acceso a la red inalámbrica (redes abiertas). · No cuenta con políticas de uso de la red. · No cuenta con políticas de manejo de la información confidencial. · No cuenta con políticas de seguridad de sistemas operativos. · No cuenta con políticas de seguridad de los activos de comunicaciones. · No cuenta con política de manejo de claves de acceso para empleados y ex – empleados.	Perdida o daño de los activos, limita el funcionamiento de los servicios	**Se mantiene un constante monitoreo los activos de mayor criticidad.**

La tabla 36, muestra los controles de mitigación para el activo equipos host de usuario

Tabla 34. Controles mitigadores para el activo host de usuario.

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
TECNOLOGICAS	**1**	Daño del hardware	No existen los repuestos para el correcto funcionamiento del hardware, falta de presupuesto.	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.	**Respaldar información y configuraciones.**
	2	Daño del software	No cuenta con un protocolo de actualización del software.	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.	**Respaldar información y configuraciones.**
	3	Daño de los medios de trasmisión	No cuenta con políticas del manejo del cableado estructurado.	El activo no funciona correctamente e impide el servicio, por daño total del medio de trasmisión.	**Aislamiento del cableado estructurado**
	5	Inhibición de los puertos	No cuenta con un protocolo de manejo de puertos.	Los puertos no funcionan correctamente por desconexión e impide el servicio.	**Habilitación de los puertos sólo los necesarios.**
	6	Falla eléctrica	· Sobrecarga de energía · Fallas del proveedor de suministro eléctrico. · Tableros eléctricos expuestos.	Desconexión total de los servicios para los usuarios, impide el normal funcionamiento.	**Implementación de sistemas UPS.**

Tabla 36. Controles mitigadores para el activo host de usuario. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
TECNOLOGICAS	**7**	Software no licenciado	No se encuentra con las licencias actualizadas.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Licenciamiento adecuado**
	8	Software desactualizado	No cuenta con un protocolo de actualización de software.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Actualización periódica del software.**
	9	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.	Los activos que se encuentran dentro del area de comunicaciones o datacenter, pueden presentar algún tipo de afectación de modero a grave.	**Ninguna**
	10	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.	Los activos que se encuentran dentro del área de comunicaciones o datacenter, pueden presentar algún tipo de afectación de modero a grave.	**Ninguna**
	11	Ataque a la red	Pérdida parcial o total de la información critica	Pérdida parcial o total de la información critica	**Mantener monitoreo costante de la red, como un IPS para evitar ataques a la red de datos.**
	12	Falla de backup	Activo no configurado correctactamente o no existe tal servicio	Activo no configurado correctactamente o no existe tal servicio	**Ninguna**

Tabla 36. Controles mitigadores para el activo host de usuario. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
AMBIENTALES	**1**	Terremotos/sismos	· El edificio no cuenta con una estructura antisísmica. · Ibarra se encuentra en una zona propensa a sismos. · No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos. Perdidas económicas y/o humanas.	**Ninguna**
	2	Erupciones volcánicas	· Ibarra se encuentra en una zona geográfica rodeada de volcanes. · No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos.	**Ninguna**
	3	Deslizamientos	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Perdidas económicas y/o humanas.	**Ninguna**
	4	Inundaciones	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos.	**Ninguna**
	5	Incendios	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Perdidas económicas y/o humanas.	**Ninguna**

Tabla 36. Controles mitigadores para el activo host de usuario. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
HUMANAS	**1**	Desconfiguración involuntaria	No existe un protocolo adecuado de manejo de claves de los activos importantes.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Respaldo de configuraciones importantes**
	2	Desconexión del puerto	· No cuenta con un protocolo de manejo de puertos. · No cuenta con políticas del manejo del cableado estructurado.	Los puertos no funcionan correctamente por desconexión e impide el servicio.	· **Revisión del cableado estructurado.**
	3	Violación de la configuración de los activos de comunicaciones	No existe una política periódica de actualizaciones de calves.	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.	**Ninguna**
	4	Ingreso de personal no autorizado	No se cuenta con un registro de acceso, de personas a al departamento de sistemas	Falla momentánea de los servicios, perdida de activos, pérdida económica, y violación de la confidencialidad.	**Ninguna**
	5	Suplantación de identidad	No existe una adecuada gestión de claves de usuarios podrían ser compartidas o divulgadas inadecuadamente.	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.	**Los empleados y estudiantes deben contar con claves y usuarios correctamente identificados.**

Tabla 36. Controles mitigadores para el activo host de usuario. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
	6	Error de etiquetación de los activos	No cuenta con información actualizada de los activos	Los activos pueden verse afectados, cambios inesperados de la configuración, desencadena en pérdida total o parcial de la información crítica.	**Se encuentra correctamente etiquetado e identificado**
HUMANAS	**7**	Mantenimiento inadecuado de los activos	No cuenta con una política de mantenimiento periódica de los activos	Daño total o parcial de los activos de hardware o software, limita el funcionamiento de los servicios	**Ninguna**
	8	Robo o pérdida de los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas	Inhabilitación de los servicios, incluye pérdidas económicas	**Se encuentran correctamente en inventario**
	9	Respaldos no adecuados	No existe una política adecuada de respaldar la información.	Perdida de información importante o crítica del activo afectado	**Ninguna**
	10	Robo o pérdida de la información contenida en los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas.	Perdida de información importante o crítica del activo afectado	**Ninguna**

Tabla 36. Controles mitigadores para el activo host de usuario. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
HUMANAS	**11**	Ataques a la red (delincuencia, crackers, hackers, ex - empleados, personas mal intencionadas)	· Acceso de personal no autorizado. · No existe un mecanismo de control perimetral de la red. · No existe un control eficiente de acceso a las redes inalámbricas (redes abiertas). · No cuenta con políticas de uso de la red. · No cuenta con políticas de manejo de la información confidencial. · No cuenta con políticas de seguridad de sistemas operativos. · No cuenta con políticas de seguridad de los activos de comunicaciones. · No cuenta con política de manejo de claves de acceso para empleados y ex – empleados.	Perdida o daño de los activos, limita el funcionamiento de los servicios	· **Se mantiene un constante monitoreo los activos de mayor criticidad.** · **Informar y capacitar al personal políticas y protocolos que deben mantenerse en la institución.**

La tabla 37, muestra los controles de mitigación para el activo host de administativos

Tabla 35. Controles mitigadores para el activo host de administrativos

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
TECNOLOGICAS	**1**	Daño del hardware	No existen los repuestos para el correcto funcionamiento del hardware, falta de presupuesto.	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.	**Respaldar información y configuraciones.**
	2	Daño del software	No cuenta con un protocolo de actualización del software.	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.	**Respaldar información y configuraciones.**
	3	Daño de los medios de trasmisión	No cuenta con políticas del manejo del cableado estructurado.	El activo no funciona correctamente e impide el servicio, por daño total del medio de trasmisión.	**Aislamiento del cableado estructurado**
	5	Inhibición de los puertos	No cuenta con un protocolo de manejo de puertos.	Los puertos no funcionan correctamente por desconexión e impide el servicio.	**Habilitación de los puertos sólo los necesarios.**
	6	Falla eléctrica	· Sobrecarga de energía · Fallas del proveedor de suministro eléctrico. · Tableros eléctricos expuestos.	Desconexión total de los servicios para los usuarios, impide el normal funcionamiento.	**Implementación de sistemas UPS.**

Tabla 37. Controles mitigadores para el activo host de administrativos. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
	7	Software no licenciado	No se encuentra con las licencias actualizadas.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Licenciamiento adecuado**
TECNOLÓGICAS	**8**	Software desactualizado	No cuenta con un protocolo de actualización de software.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Actualización periódica del software.**
	9	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.	Los activos que se encuentran dentro del área de comunicaciones o datacenter, pueden presentar algún tipo de afectación de modero a grave.	**Ninguna**
	10	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.	Los activos que se encuentran dentro del área de comunicaciones o datacenter, pueden presentar algún tipo de afectación de modero a grave.	**Ninguna**
	11	Ataque a la red	Pérdida parcial o total de la información critica	Pérdida parcial o total de la información critica	**Mantener monitoreo constante de la red, como un IPS para evitar ataques a la red de datos.**
	12	Falla de backup	Activo no configurado correctactamente o no existe tal servicio	Activo no configurado correctactamente o no existe tal servicio	**Ninguna**

Tabla 37. Controles mitigadores para el activo host de administrativos. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
AMBIENTALES	1	Terremotos/sismos	· El edificio no cuenta con una estructura antisísmica. · Ibarra se encuentra en una zona propensa a sismos. · No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos. Perdidas económicas y/o humanas.	**Ninguna**
	2	Erupciones volcánicas	· Ibarra se encuentra en una zona geográfica rodeada de volcanes. · No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos.	**Ninguna**
	3	Deslizamientos	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Perdidas económicas y/o humanas.	**Ninguna**
	4	Inundaciones	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos.	**Ninguna**
	5	Incendios	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Perdidas económicas y/o humanas.	**Ninguna**

Tabla 37. Controles mitigadores para el activo host de administrativos. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
HUMANAS	**1**	Desconfiguración involuntaria	No existe un protocolo adecuado de manejo de claves de los activos importantes.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Respaldo de configuraciones importantes**
	2	Desconexión del puerto	· No cuenta con un protocolo de manejo de puertos. · No cuenta con políticas del manejo del cableado estructurado.	Los puertos no funcionan correctamente por desconexión e impide el servicio.	· **Revisión del cableado estructurado.**
	3	Violación de la configuración de los activos de comunicaciones	No existe una política periódica de actualizaciones de calves.	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.	**Ninguna**
	4	Ingreso de personal no autorizado	No se cuenta con un registro de acceso, de personas a al departamento de sistemas	Falla momentánea de los servicios, perdida de activos, pérdida económica, y violación de la confidencialidad.	**Ninguna**
	5	Suplantación de identidad	No existe una adecuada gestión de claves de usuarios podrían ser compartidas o divulgadas inadecuadamente.	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.	**Los empleados y estudiantes deben contar con claves y usuarios correctamente identificados.**

Tabla 37. Controles mitigadores para el activo host de administrativos. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
HUMANAS	**6**	Error de etiquetación de los activos	No cuenta con información actualizada de los activos	Los activos pueden verse afectados, cambios inesperados de la configuración, desencadena en pérdida total o parcial de la información crítica.	**Se encuentra correctamente etiquetado e identificado**
	7	Mantenimiento inadecuado de los activos	No cuenta con una política de mantenimiento periódica de los activos	Daño total o parcial de los activos de hardware o software, limita el funcionamiento de los servicios	**Ninguna**
	8	Robo o pérdida de los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas	Inhabilitación de los servicios, incluye pérdidas económicas	**Se encuentran correctamente en inventario**
	9	Respaldos no adecuados	No existe una política adecuada de respaldar la información.	Perdida de información importante o crítica del activo afectado	**Ninguna**
	10	Robo o pérdida de la información contenida en los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas.	Perdida de información importante o crítica del activo afectado	**Ninguna**

Tabla 37. Controles mitigadores para el activo host de administrativos. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
H U M A N A S	**11**	Ataques a la red (delincuencia, crackers, hackers, ex - empleados, personas mal intencionadas)	Acceso de personal no autorizado. No existe un mecanismo de control perimetral de la red. No existe un control eficiente de acceso a la red inalámbrica (redes abiertas). No cuenta con políticas de uso de la red. No cuenta con políticas de manejo de la información confidencial. No cuenta con políticas de seguridad de sistemas operativos. No cuenta con políticas de seguridad de los activos de comunicaciones. No cuenta con política de manejo de claves de acceso para empleados y ex –empleados.	Perdida o daño de los activos, limita el funcionamiento de los servicios	**Informar y capacitar al personal políticas y protocolos que deben mantenerse en la institución.**

La tabla 38, muestra los controles de mitigación para el activo recusrso humano

Tabla 36. Controles mitigadores para el activo Recurso humano.

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
TECNOLÓGICAS	**1**	Daño del hardware	No existen los repuestos para el correcto funcionamiento del hardware, falta de presupuesto.	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.	**Respaldar información y configuraciones.**
	2	Daño del software	No cuenta con un protocolo de actualización del software.	El activo no funciona correctamente e impide el servicio por pérdida total o parcial.	**Respaldar información y configuraciones.**
	3	Daño de los medios de trasmisión	No cuenta con políticas del manejo del cableado estructurado.	El activo no funciona correctamente e impide el servicio, por daño total del medio de trasmisión.	**Aislamiento del cableado estructurado**
	5	Inhibición de los puertos	No cuenta con un protocolo de manejo de puertos.	Los puertos no funcionan correctamente por desconexión e impide el servicio.	**Habilitación de los puertos sólo los necesarios.**
	6	Falla eléctrica	· Sobrecarga de energía · Fallas del proveedor de suministro eléctrico. · Tableros eléctricos expuestos.	Desconexión total de los servicios para los usuarios, impide el normal funcionamiento.	**Implementación de sistemas UPS.**

Tabla 38. Controles mitigadores para el activo Recurso humano. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
	7	Software no licenciado	No se encuentra con las licencias actualizadas.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Licenciamiento adecuado**
TECNOLÓGICAS	**8**	Software desactualizado	No cuenta con un protocolo de actualización de software.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Actualización periódica del software.**
	9	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.	Los activos que se encuentran dentro del área de comunicaciones o datacenter, pueden presentar algún tipo de afectación de modero a grave.	**Ninguna**
	10	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.	Los activos que se encuentran dentro del área de comunicaciones o datacenter, pueden presentar algún tipo de afectación de modero a grave.	**Ninguna**
	11	Ataque a la red	Pérdida parcial o total de la información critica	Pérdida parcial o total de la información critica	**Mantener monitoreo contante de la red, como un IPS para evitar ataques a la red de datos.**
	12	Falla de backup	Activo no configurado correctactamente o no existe tal servicio	Activo no configurado correctactamente o no existe tal servicio	**Ninguna**

Tabla 38. Controles mitigadores para el activo Recurso humano. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
AMBIENTALES	**1**	Terremotos/sismos	· El edificio no cuenta con una estructura antisísmica. · Ibarra se encuentra en una zona propensa a sismos. · No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos. Perdidas económicas y/o humanas.	**Existe un plan de contingencia para evacuacion de personal administrativo y estudiantes actualmente.**
	2	Erupciones volcánicas	· Ibarra se encuentra en una zona geográfica rodeada de volcanes. · No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos.	**Ninguna**
	3	Deslizamientos	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Perdidas económicas y/o humanas.	**Ninguna**
	4	Inundaciones	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Daño total o parcial de la infraestructura de red de datos.	**Ninguna**
	5	Incendios	No existe un plan de capacitación para el personal, para manejar este tipo de emergencias.	Perdidas económicas y/o humanas.	**Ninguna**

Tabla 38. Controles mitigadores para el activo Recurso humano. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
HUMANAS	**1**	Desconfiguración involuntaria	No existe un protocolo adecuado de manejo de claves de los activos importantes.	Los activos, incluidos los de software y hardware no funcionan de manera eficiente, impide que los servicios sean usados de manera correcta.	**Respaldo de configuraciones importantes**
	2	Desconexión del puerto	· No cuenta con un protocolo de manejo de puertos. · No cuenta con políticas del manejo del cableado estructurado.	Los puertos no funcionan correctamente por desconexión e impide el servicio.	· **Revisión del cableado estructurado.**
	3	Violación de la configuración de los activos de comunicaciones	No existe una política periódica de actualizaciones de calves.	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.	**Ninguna**
	4	Ingreso de personal no autorizado	No se cuenta con un registro de acceso, de personas a al departamento de sistemas	Falla momentánea de los servicios, perdida de activos, pérdida económica, y violación de la confidencialidad.	**Ninguna**
	5	Suplantación de identidad	No existe una adecuada gestión de claves de usuarios podrían ser compartidas o divulgadas inadecuadamente.	Cambio no autorizado de la configuración de uno o varios activos importantes, puede presentar inhabilitación total o parcial de los servicios.	**Los empleados y estudiantes deben contar con claves y usuarios correctamente identificados.**

Tabla 38. Controles mitigadores para el activo Recurso humano. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
HUMANAS	**6**	Error de etiquetación de los activos	No cuenta con información actualizada de los activos	Los activos pueden verse afectados, cambios inesperados de la configuración, desencadena en pérdida total o parcial de la información crítica.	**Se encuenta correctamente etiquetado e identificado**
	7	Mantenimiento inadecuado de los activos	No cuenta con una política de mantenimiento periódica de los activos	Daño total o parcial de los activos de hardware o software, limita el funcionamiento de los servicios	**Ninguna**
	8	Robo o pérdida de los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas	Inhabilitación de los servicios, incluye pérdidas económicas	**Se encuentran correctamente en inventario**
	9	Respaldos no adecuados	No existe una política adecuada de respaldar la información.	Perdida de información importante o crítica del activo afectado	**Ninguna**
	10	Robo o pérdida de la información contenida en los activos	No se cuenta con una política registro de acceso, de personas a al departamento de sistemas.	Perdida de información importante o crítica del activo afectado	**Ninguna**

Tabla 38. Controles mitigadores para el activo Recurso humano. (Continuación)

TIPO	#	AMENAZAS	VULNERABILIDAD	IMPACTO/ACCIONES DE LA AMENAZA	ACCIONES DE MITIGACIÓN
H U M A N A S	**11**	Ataques a la red (delincuencia, crackers, hackers, ex - empleados, personas mal intencionadas)	· Acceso de personal no autorizado. · No existe un mecanismo de control perimetral de la red. · No existe un control eficiente de acceso a la red inalámbrica (redes abiertas). · No cuenta con políticas de uso de la red. · No cuenta con políticas de manejo de la información confidencial. · No cuenta con políticas de seguridad de sistemas operativos. · No cuenta con políticas de seguridad de los activos de comunicaciones. · No cuenta con política de manejo de claves de acceso para empleados y ex – empleados.	Perdida o daño de los activos, limita el funcionamiento de los servicios	**Informar y capacitar al personal políticas y protocolos que deben mantenerse en la institución.**

4.8 Conclusiones finales de metodología de evaluación del riesgo según la Guía NIST SP 800 - 30 para la red de datos del Tecnológico ITCA.

4.8.1 Para el activo redes y comunicación.

Para este grupo de activo donde se encuentran los Router del proveedor de internet, y el router principal de la institución, dispositivos de suma importancia para que toda la infraestructura funcione de manera adecuada, se recomienda:

- No utilizar contraseñas por defecto, e implementar una política de cambio periódico de contraseñas para evitar que cualquier persona pueda ingresar a los servidores.
- Desarrollar un manual de administración de este tipo de activos.
- Realizar una bitácora de sucesos importante para este tipo de activos.
- Realizar un backup de las configuraciones que se encuentran en los activos.
- Implementar una solución de control perimetral de la red.

Dentro de este grupo de activos se describen los switch de conmutación, siendo el más importante el switch de capa 3 donde serán configuradas todas las Vlans, por consiguiente para este grupo de activos se recomienda:

- No utilizar contraseñas por defecto, e implementar una política de cambio periódico de contraseñas
- Realizar backups periódicos de las diferentes configuraciones contenidas, documentarlas y validar que estén realizados de forma correcta.
- Realizar un manual de procedimientos ante ocurrencia de sucesos ante amenazas.

4.8.2 Para el activo Servidores

- Implementar una política de control de cambios, informar al personal de los cambios que se van a realizar en los servidores.

- Implementar una política de cambio periódico de contraseñas para evitar que cualquier persona pueda ingresar a los servidores.

- Realizar backups periódicos de las diferentes configuraciones contenidas en los servidores que posee la Institución, documentarlas y validar que estén realizados de forma correcta.

- Implementar una política de respaldo de información de los servidores que se tienen en la empresa

4.8.3 Para el activo host de usuarios

- Implementar una política de mantenimientos periódicos de los host de los laboratorios, así se evitará el daño de las diferentes partes y elementos de estos equipos.

- Implementar una política de respaldo de información, enseñarle al usuario que debe respaldar periódicamente su información, puesto que son activos que fácilmente se pueden sustraer.

4.8.5 Para el activo host de administrativos

- Implementar una política de actualización de equipos de escritorio cada cierto periodo de tiempo.
- Implementar una política de backups de equipos, tener a la mano algunos equipos de backups por si acaso llegue a fallar alguno.

- Mantener actualizado el antivirus, lo cual hace que todos los equipos de la empresa cuenten con protección para evitar posibles ataques de virus, spam, etc.

- Implementar una política de respaldo de información, enseñarle al usuario que debe respaldar periódicamente su información, puesto que son activos que

fácilmente se pueden sustraer.

4.8.6 Para el activo recurso humano

- Implementar una política de capacitaciones periódicas a los empleados en los diferentes equipos que se maneja en la empresa.
- Implementar una política de remplazo del personal ausente.

CAPÍTULO V

5 Diseño e implementación del sistema de seguridad perimetral en la red del instituto

En este capítulo se procederá con la configuración de los equipos necesarios para la implementación de la seguridad perimetral, así como para la IPS, Firewall y Segmentación lógica de la red.

5.1 Análisis de los tipos de firewall.

Los firewall son un sistema integrado de software o hardware, para protección de redes, y host en particular, el objetivo principal de este tipo de sistemas es evitar intrusiones no autorizadas que puedan provocar vulnerabilidad, a los activos o redes de información.

5.1.1 Funciones principales de un firewall.

Entre las más importantes se puede mencionar las siguientes:

- Preservar la seguridad y la privacidad de la información
- Proteger una red doméstica o empresarial
- Mantener a buen recaudo la información almacenada en la red, servidores, bases de datos, o hosts de usuarios.
- Evitar intrusiones de usuarios no autorizados o no deseados dela red

5.5.1 Limitaciones del firewall.

Dentro de las limitaciones de un firewall se encuentran las siguientes:

- El firewall en principio es probable que no pueda proteger a ciertas vulnerabilidades internas como por ejemplo usuarios que sustraigan datos de servidores, host u otros activos dentro de la institución.
- El firewall no puede proteger contra ataques de ingeniería social como hackers que suplanten identidad al ingresar a los sistemas vulnerables.
- Los firewall no protegen a los ataques que atraviesen el firewall por lo que no podrá repeler la totalidad de ataques que podría sufrir la red.
- El firewall no puede proteger contra los posibles ataques a la red por virus informáticos a través de archivos de software.
- El firewall no puede proteger de las fallas de seguridad de los servicios y protocolos, de los cuales se permita el tráfico es decir si la configuración no se efectúa correctamente.
- El firewall no puede proteger contra los ataques que se efectúen fuera de su punto de operación o jurisdicción.

5.5.2 Tipos de firewall.

Por lo general se han clasificado en tres tipos de firewall**:**

5.1.3.1 Firewall personales.

Como su nombre mismo lo indica, su función personal es proteger a un solo host en específico, permite controlar el acceso a las aplicaciones instaladas, en el host son de costo bajo y de algunos de distribución gratuita.

5.1.3.2 Firewall basados en hardware.

Este tipo de sistemas o dispositivos externos que se colocan sobre los dispositivos destinados para el acceso a internet. Son dispositivos separados que controlan su propio sistema operativo y proporcionan una línea de defensa contra ataques, el mayor inconveniente es el alto costo económico y son propios del tipo de fabricante.

5.1.3.3 Firewall basados en software.

Son sistemas basados en software libre y los alguno de licencia gratuita se conocen como firewall software y puede ser usado con mayor libertad. Los firewalls software se instalan en el ordenador (como cualquier otro programa) y pueden ser configurados de diversas maneras, permitiendo cierto control sobre su funcionalidad y sus características de protección como controles de privacidad y filtrado de web entre otras. Por otra parte están los de software comercial poseen casi la mayoría de características que los anteriores, pero con mayor nivel de protección y control, estos por lo general tienen un costo económico relativamente no tan alto como los basado en hardware.

5.2 Políticas de seguridad en la red.

La decisión de instalar un firewall puede estar influenciada por dos niveles de política de la red de datos como la distribución y uso del sistema.

- La política de acceso a la red define los servicios que se permitirán o negarán de manera explícita es la política de más alto nivel.
- También define cómo se utilizan los servicios la política de bajo nivel define cómo se restringirá en realidad el acceso y determinará los servicios especificados en la política de nivel superior.

Las dos políticas básicas en la configuración de un firewall y que cambian radicalmente la filosofía fundamental de la seguridad en la institución están dadas por:

- Política permisiva: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.
- La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico Potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

5.3 Descripción y selección del software para el desarrollo del diseño del sistema de seguridad Perimetral.

La descripción del software, busca seleccionar la mejor opción, para el desarrollo de la seguridad perimetral. A continuación se describen algunos de ellos y sus características principales

5.3.1 Monowall

Monowall es un proyecto destinado a crear un paquete completo de software embebido servidor de seguridad que, cuando se utiliza junto con un computador integrado, proporciona todas las características importantes de las cajas de firewall comercial (incluyendo la facilidad de uso) a una fracción del precio (software libre). Está basado en una versión de FreeBSD junto con un servidor web, PHP y otras utilidades de unos pocos. (Zapata, 2012)

5.3.1.1 Características de Monowall.

- Router NAT (Network Address Translation) para utilizar las direcciones IP privadas se esconden detrás de la dirección IP pública del ISP. El reenvío de puerto asociado con la dirección IP pública a una IP y un puerto de una estación de la red local es posible.
- Protocolo de enrutamiento RIPv2 protocolo de información de enrutamiento) para la configuración dinámica de las tablas de enrutamiento.
- Firewall para la función de filtrado de paquetes con SPI (Stateful Packet Inspection) para filtro basado en el estado de la conexión.

- De portal cautivo , cuyo objetivo es permitir el acceso a la red a través de una autenticación web.
- VPN Host-to-LAN para habilitar los equipos cliente para conectarse a la red local a través de Internet.
- Autenticación Radius , para permitir el acceso a la red a través del punto de acceso WiFi .
- Servidor DNS multizona, para establecer su propia zona DNS y registros asociados.
- Cliente DNS si necesitamos un nombre DNS para llegar al router.
- Servidor DHCP para asignar automáticamente direcciones IP a las estaciones clientes que lo soliciten.

5.3.2 IpCop.

IPCop es una distribución Linux que implementa un firewall y proporciona una simple interfaz web de administración basándose en una computadora personal, lanzada por primera en el año 2001. IPCop tiene como objetivos ser un firewall sencillo, con pocos requerimientos hardware orientado a usuarios domésticos o a pequeñas empresas. (Sanchez, 2012)

5.3.2.1 Características de IpCop.

- Gestión del tráfico en entrada y salida
- La Administración se realiza mediante una interfaz Web segura
- Administración a distancia con protocolo SSH

- Servicio de DNS dinámicos
- Servicio Proxy Avanzado, a nivel trasparente y aplicación. Server DHCP
- Sistema añadido de detección de intrusos

5.3.3 Pfsense.

Pfsense es una distribución basada en FreeBSD, para usarlo en servicios de redes LAN y WAN tales como firewall, enrutador, servidor de balanceo de carga, su objetivo es tener un firewall fácilmente configurable a través de una interface web incluyendo los equipos de una sola tarjeta. Es una solución muy completa, bajo licencia BSD y, de libre distribución. (Zapata, 2012)

5.3.1 Características de Pfsense.

- Filtrado de origen a destino de IP, protocolo IP, puerto de origen y destino para TCP y UDP tráfico
- Habilitación de límites para conexiones simultaneas con reglas de base
- Políticas de enrutamiento con alta flexibilidad para la selección del gateway sobre las reglas de base para el equilibrio de ancho de banda, WAN múltiple, backup sobre más ADSL, etc.
- Posibilidad de creación de Alias de grupos de IP y nombres de IP, redes y puertas. Estas características ayudan a mantener la configuración limpia y fácil de entender, especialmente con configuraciones con varios IP públicos y numerosos Servers
- Filtración y posibilidad de puentear interfaces y filtrar el tráfico entre estas

- Posibilidad de inhabilitar la filtración para utilizar pfSense como solo Router

5.4 Elección final de software

Para el desarrollo del proyecto se ha seleccionado el software Pfsense siendo un sistema operativo más estable para los servicios necesarios que se mencionan a continuación en la tabla 39.

Tabla 37. Servicios de Pfsense

Servicios	**Descripción**
Firewall	Pfsense puede ser configurados como firewall permitiendo y denegando trafico determinado en la red, de entrada o de salida a partir de una dirección ya sea de red, host tanto de origen como destino.
Servidor VPN	Pfsense se puede configurar como un servidor VPN usando protocolos de tunneling tales como IPSec, PPTP, entre otras
Balanceo de carga	Pfsense puede ser configurado como servidor de balanceo de carga tanto entrante como saliente, esta característica es usada comúnmente en servidores web, de correo, de DNS. También para proveer estabilidad y redundancia en él envió de tráfico a través del enlace WAN evitando los cuellos de botella
Estado del Sistema	Pfsense es un firewall, el cual como característica principal guarda el estado de las

	conexiones abiertas en una tabla. La mayoría de los firewall no tienen la capacidad de controlar con precisión la tabla de estado.
Servidor DNS y cache DNS	Pfsense se puede configurar como un servidor DNS primario y reenviador de consultas de DNS.
Servidor DHCP	También funciona como servidor de DHCP, se puede también implementar VLAN desde Pfsense.
Enrutamiento estático	Funciona como un enrutador ya que entrega direccionamiento IP y hace el mapeo hacia afuera.
Monitoreo continuo	Puede mostrar las siguientes componentes: utilización de CPU, rendimiento, estado del firewall, reportes por cada interfaz, manejo de tráfico y ancho de banda.

Fuente: http://www.firewallhardware.es/pfsense.html

5.5 Distribución lógica de la red del Tecnológico ITCA

Para lograr un correcto diseño de seguridad perimetral como primer paso se realiza la distribución de las Vlans de acuerdo al tipo de servicios que se presenta y de acuerdo a las necesidades de la red.

Se han designado 16 Vlans con su direccionamiento IP y se han asignado de acuerdo a la dirección de red 172.20.0.1/24. La tabla 40 muestra el direccionamiento que se ha designado

Tabla 38. Distribución de las Vlans para la segmentación lógica

Numero de Vlan	Dirección IP	Mascara	Servicio
Vlan 1	172.10.1.0	255.255.255.0	**Por defecto**
Vlan 2	172.20.1.1	255.255.255.0	**Servidores**
Vlan 3	172.20.2.1	255.255.255.0	**Administrativos**
Vlan 4	172.20.3.1	255.255.255.0	**Sistemas**
Vlan 5	172.20.4.1	255.255.255.0	**Laboratorios**
Vlan 6	172.20.5.1	255.255.255.0	**Wireless**
Vlan 7	172.20.6.1	255.255.255.0	**Vigilancia**
Vlan 8	172.20.7.1	255.255.255.0	**Coordinadores**
Vlan 9	172.20.8.1	255.255.255.0	**Internet**
Vlan 10	172.20.9.1	255.255.255.0	**Laboratorio3**
Vlan 11	172.20.10.1	255.255.255.0	**Wireless-Estudiantes**
Vlan 12	172.20.11.1	255.255.255.0	**Wireless- Docentes**
Vlan 13	172.20.12.1	255.255.255.0	**- Wireless Administrativos**
Vlan 14	172.20.1.14	255.255.255.0	**Wireless- Invitados**
Vlan 15	172.20.15.1	255.255.255.0	**Cyber**
Vlan 16	172.2016.1	255.255.255.0	**CACMU**

Fuente: Basado en investigación teórica y práctica

5.5.1 Distribución de las direcciones IP para las Vlans.

Luego de haber designado el direccionamiento para cada una de las Vlans se desarrolla la distribución de las direcciones IP de la red 172.20.1.1 de cada Vlan la tabla 41 muestra el direccionamiento de la Vlan 2 de servidores. La distribución de las demás Vlans se encuentra en el anexo 2.

Tabla 39. Distribución de las IP de la Vlan 2

SOFTWARE / APP	**DIRECCION IP**
SSOO WIN 7	172.20.1.15
D-VIEW CAM	172.20.1.15
ACADÉMICO1	172.20.1.6
ACADÉMICO	172.20.1.20
WINDOWS 7	172.20.1.20
WINDOWS SERVER 2012	172.20.1.150
FTTP	172.20.1.40
WEB	172.20.1.33
PROXY LABORATORIOS	172.20.1.16
PROXY ADMINISTRATIVOS	172.20.1.151
ACTIVE DIRECTORY	172.20.1.6
BACKUP	172.20.1.150
FACTURACIÓN	172.20.1.32
CAMARAS DE VILGILANCIA	172.20.1.48
VoIP	172.20.1.96

Fuente: Basado en investigación teórica y práctica

5.6 Diseño del sistema de Seguridad Perimetral.

El diseño permite desarrollar la mejor solución que se acople a las necesidades para mejorar la seguridad de los activos de la red de datos del Tecnológico ITCA.

Para esto se han dividido la red en tres zonas la red WAN, red de la zona desmilitarizada DMZ y la red local LAN, La figura 27 muestra el diseño de Seguridad Perimetral.

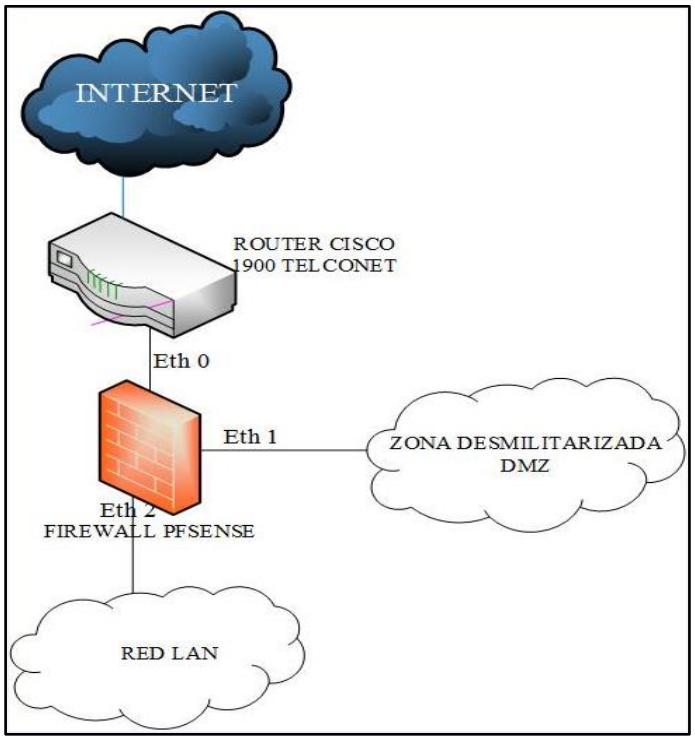


Figura 27. Topología del diseño del firewall

Fuente: Basado en investigación teórica y práctica

5.6.1 Direccionamiento del diseño de seguridad perimetral del Tecnológico ITCA.

La tabla 42 muestra el direccionamiento propuesto, que se lleva acabo para el diseño del firewall.

Tabla 40. Direccionamiento del diseño de red

Red	Dirección IP	Mascara
Red WAN	192.168.137.2	**255.255.255.0**
Red DMZ	172.16.101.0	**255.255.255.0**
Red LAN	172.16.4.1	**255.255.255.0**

Fuente: Basado en investigación teórica y práctica

5.6.2 Principios y características de diseño.

El Firewall es colocado entre la red local LAN y la red WAN y por ende separa la red de la zona desmilitarizada DMZ

5.6.2.1 Objetivos

- Establecer un enlace controlado
- Proteger la red local de ataques
- Proveer un único punto de choque

5.7 Configuración de los equipos del sistema de seguridad perimetral para la red de datos del tecnológico ITCA.

En este capítulo se detalla el proceso de configuración e implementación que comprende el sistema de seguridad perimetral, y de la nueva segmentación como la configuración del servidor en el cual se alberga el firewall.

5.7.1 Configuración de los equipos de red

Para la configuración del switch de Core se realiza un procedimiento establecido de la siguiente manera, la configuración completa se encuentra en el anexo 3.la imagen 43 muestra el resumen de la configuración de las Vlans.

- Configuración de Nombre
- Configuración de las contraseñas para ingreso de consola y telnet
- Configuración del Banner
- Configuración de VTP Server
- Configuración de las nuevas VLANs
- Configuración de la IP en las Interfaces de VLAN
- Configuración de los Enlaces de Troncal

Tabla 41. Resumen de la configuración de las Vlans

```
SW-ITCA-CORE#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/1, Fa1/2, Fa1/3
                                                Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                Fa1/8, Fa1/9, Fa1/10, Fa1/11
                                                Fa1/12, Fa1/13, Fa1/14, Fa1/15
2    servidores                       active
3    Administrativos                  active
4    Sistemas                         active
5    Laboratorios                     active
6    Wireless                         active
7    Vigilancia                       active
8    Coordinadores                    active
9    Internet                         active
10   Laboratorio3                     active
11   W_Estudiantes                    active
12   W_Docentes                       active
13   W_Administrativos                active
14   W_Invitados                      active
15   Cyber                            active
16   CACMU                            active
1002 fddi-default                     active

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
6    enet  100006     1500  -      -      -        -    -        0      0
7    enet  100007     1500  -      -      -        -    -        0      0
8    enet  100008     1500  -      -      -        -    -        0      0
9    enet  100009     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
11   enet  100011     1500  -      -      -        -    -        0      0
12   enet  100012     1500  -      -      -        -    -        0      0
13   enet  100013     1500  -      -      -        -    -        0      0
14   enet  100014     1500  -      -      -        -    -        0      0
15   enet  100015     1500  -      -      -        -    -        0      0
16   enet  100016     1500  -      -      -        -    -        0      0
```

Fuente: Basado en investigación teórica y práctica

5.7.2 Configuración de las interfaces del firewall Pfsense

Para la configuración del Firewall Pfsense, los pasos de instalación se pueden observar en el Anexo 4, después de obtener una configuración exitosa se deben configurar las zonas de la red, las interfaces del firewall y las reglas que permitirán o denegarán el acceso a los diferentes servicios.

Las figura 28, 29 y 30 muestran la configuración de las tarjetas Ethernet para cada una de las zonas establecidas la red WAN, red LAN y red DMZ

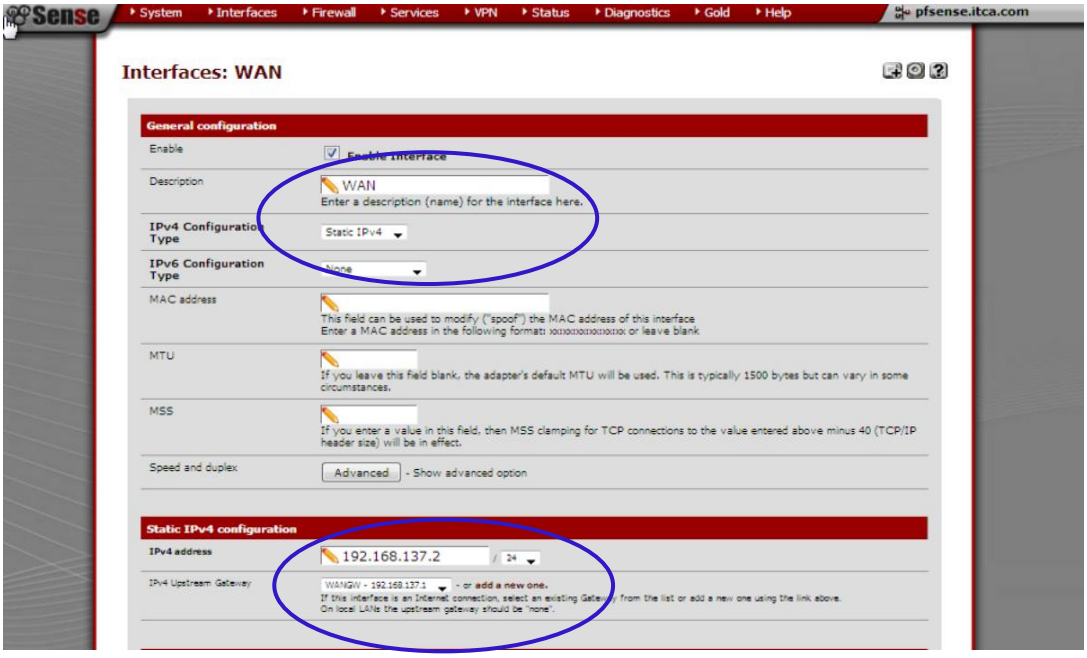


Figura 28. Configuración de la red WAN

Fuente: Pfsense versión 2.2.5

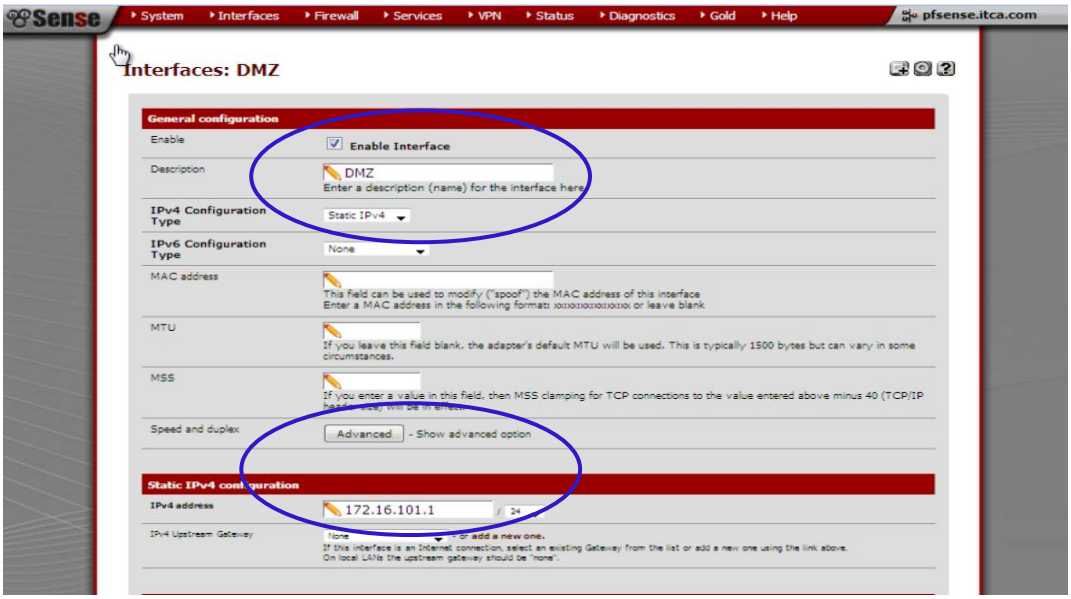


Figura 29. Configuración de la red DMZ

Fuente: Pfsense versión 2.2.5

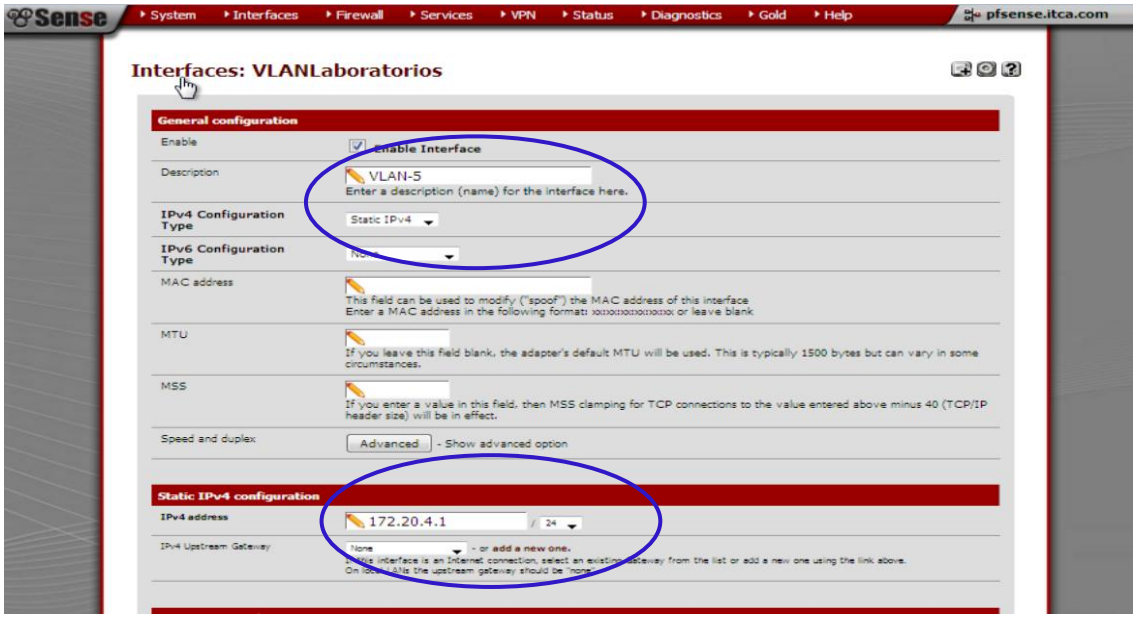


Figura 30. Configuración de la red LAN

Fuente: Pfsense versión 2.2.5

5.7.3 Configuración de firewall Pfsense Vlans

Se configura cada Vlan para permitir el acceso a internet entre el Firewall Pfsense y el switch de Core, de la siguiente forma se selecciona la interfaz, numero de Vlan y una descripción de la Vlan. La figura 31 muestra como debe ser configura está configurada la Vlan 5.

Figura 31.configuración de la Vlan 5 acceso a internet.

Fuente: Pfsense versión 2.2.5

- Una vez creado las Vlans, seleccionamos la interfaz física y la Vlan de la siguiente manera en la figura 32.

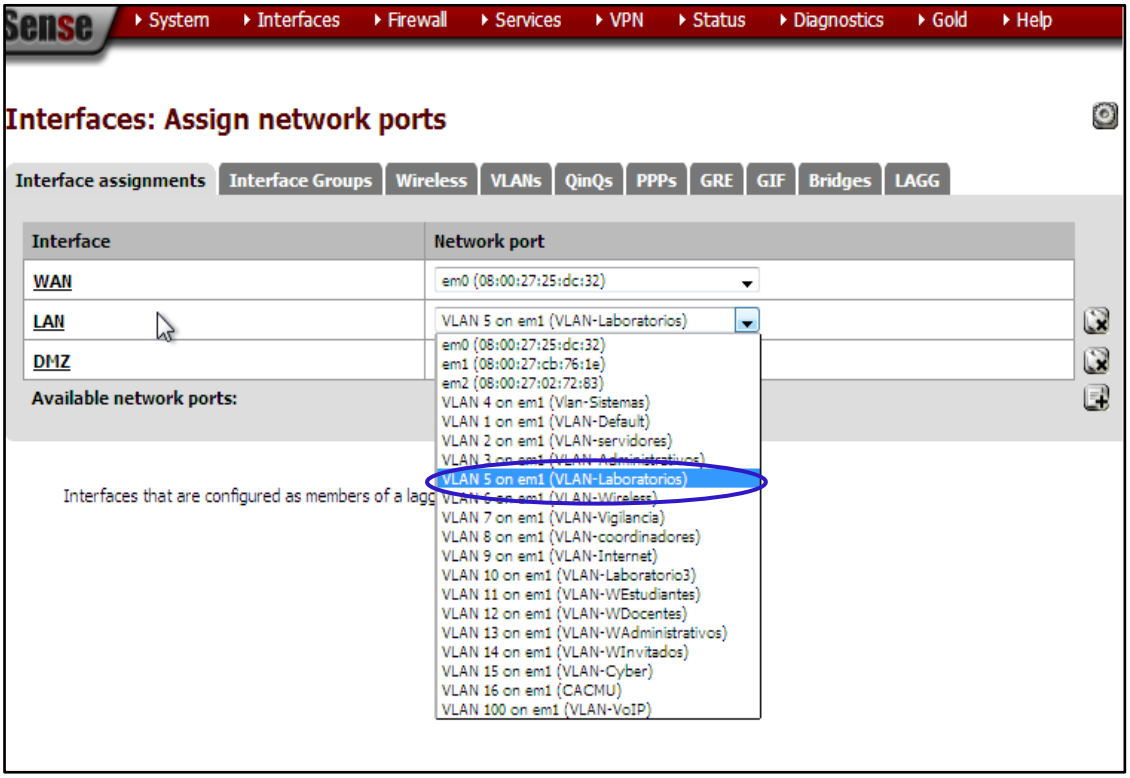


Figura 32.asignación de la Vlan 5 hacia la red LAN

Fuente: Pfsense versión 2.2.5

De la siguiente manera como describe la figura 33 muestra la configuración de la interfaces para acceso a internet.

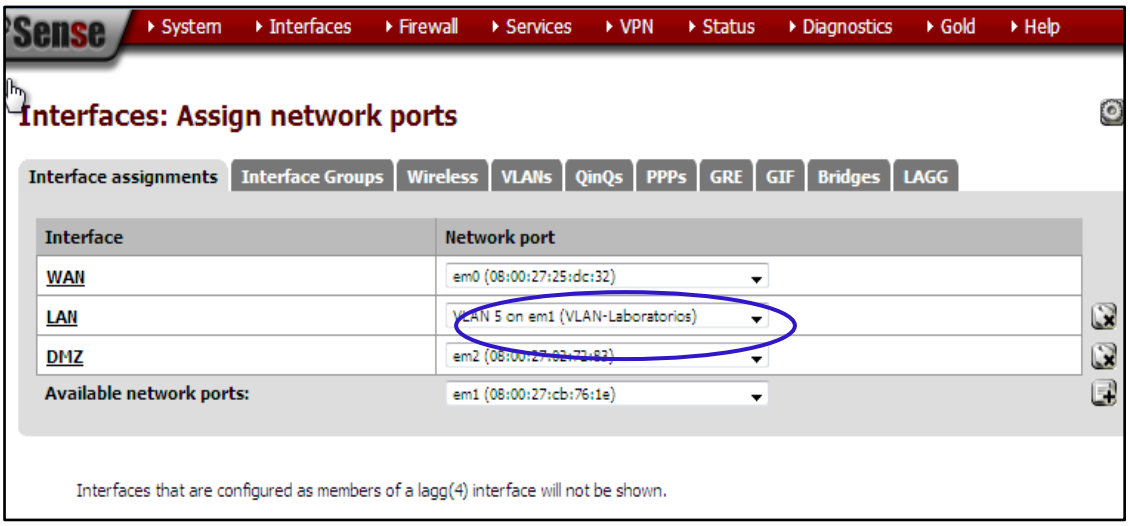


Figura 33. Asignación a las interfaces con la Vlan 5

Fuente: Pfsense versión 2.2.5

- habilitamos la interfaz LAN y configuramos la dirección IP, el nombre de la interfaz y los parámetros necesarios. La figura 34 muestra la configuración de IPV4 estático y guardar la configuración necesaria.

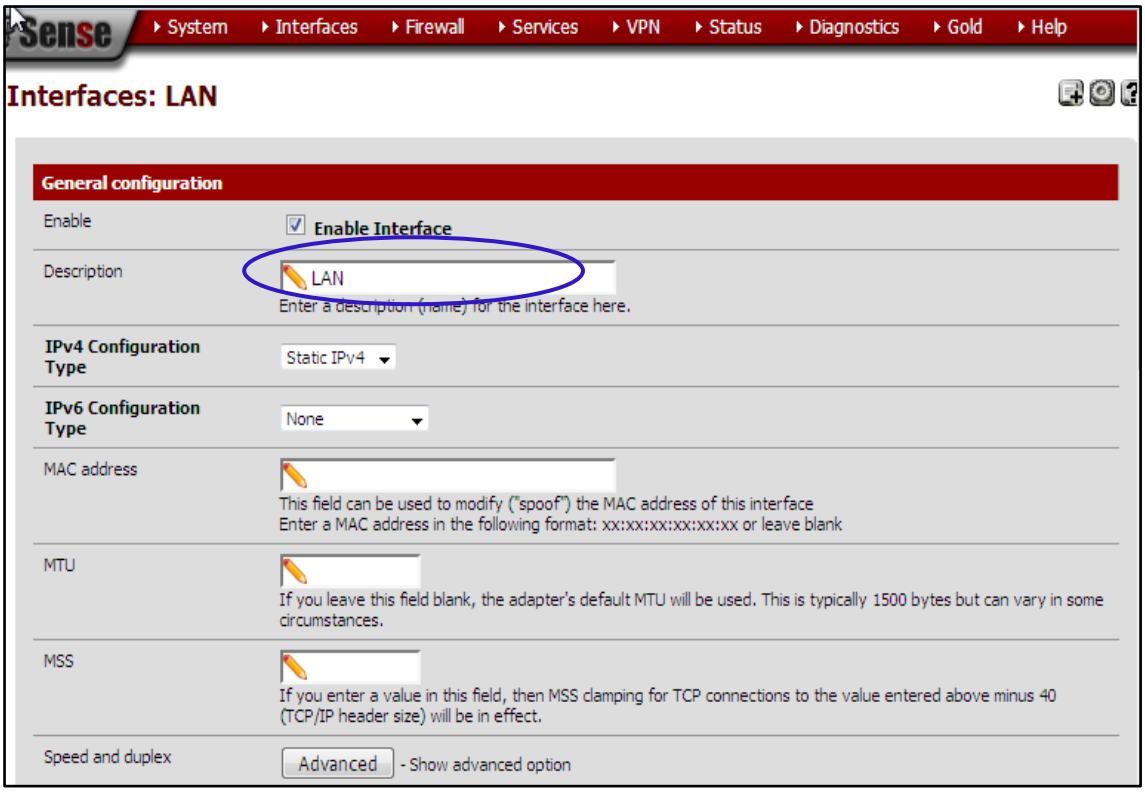


Figura 34.selección de la interfaz LAN

Fuente: Pfsense versión 2.2.5

- ahora se cambia la descripción y seleccionamos IPV4 estático, para colocar su respectiva IP a la VLAN 5. Guardamos los cambios y aplicamos como en la figura 35.

Figura 35. Cambio de la interfaz LAN por la Vlan 5

Fuente: Pfsense versión 2.2.5

Ahora las interfaces deben quedar configuradas de la siguiente manera como indica la figura 36.

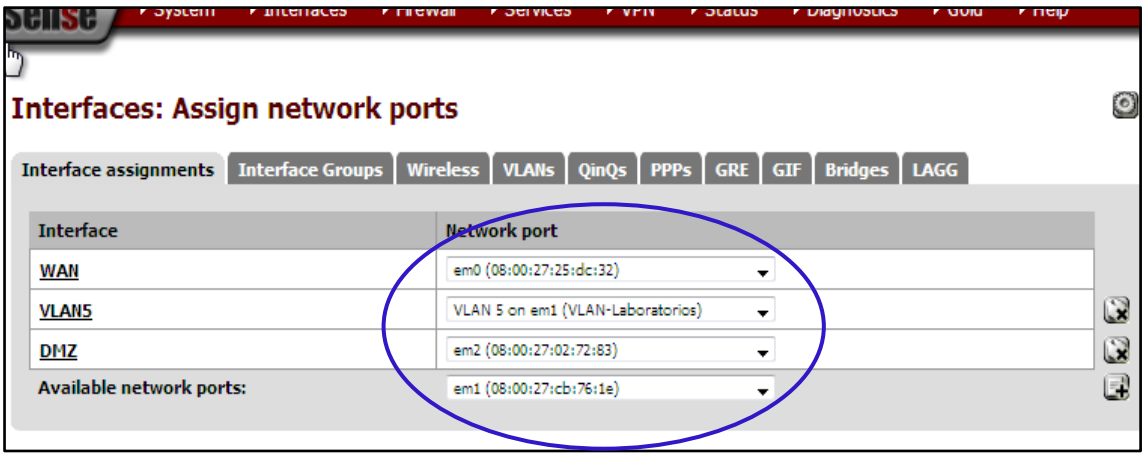


Figura 36. Asignación de las tarjetas de las redes

Fuente: Pfsense versión 2.2.5

5.7.4 Configuración del NAT en Pfsense

NAT es un mecanismo utilizado Pfsense para intercambiar los paquetes entre dos redes que asignan mutuamente direcciones y permite el acceso a los servidores desde el exterior (puertos y puerta de enlace), lo que popularmente se llama como "abrir puertos"

La imagen 37 muestra cómo se configura el NAT para la red de la siguiente manera Damos clic en el signo (+), para generar nueva regla de NAT y Colocar la dirección de red de la Vlan como origen, y por el momento cualquier puerto y cualquier destino. Después se puede ir adaptando a las necesidades del diseño de la red siempre guardar la configuración.

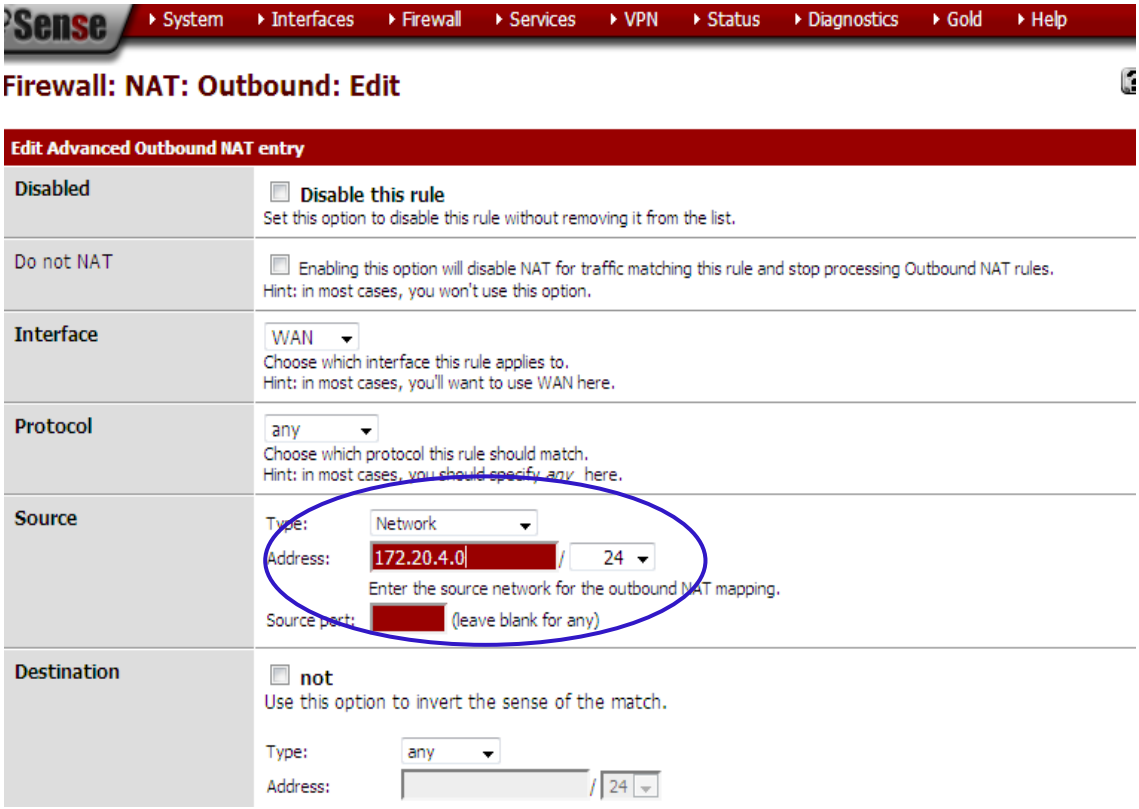


Figura 37.configuración de una regla NAT

Fuente: Pfsense versión 2.2.5

- La imagen 38 muestra cómo debe quedar la configuración para la red de la siguiente manera la dirección 172.16.101.0 que es la red DMZ se habilita el NAT para acceso a toda la red LAN, la dirección 172.16.1.0 que corresponde a la red de servidores y la dirección 172.20.4.1, en este caso se ha habilitado los puertos 80 para HTTP, 443 para HTTS y 53 para DNS

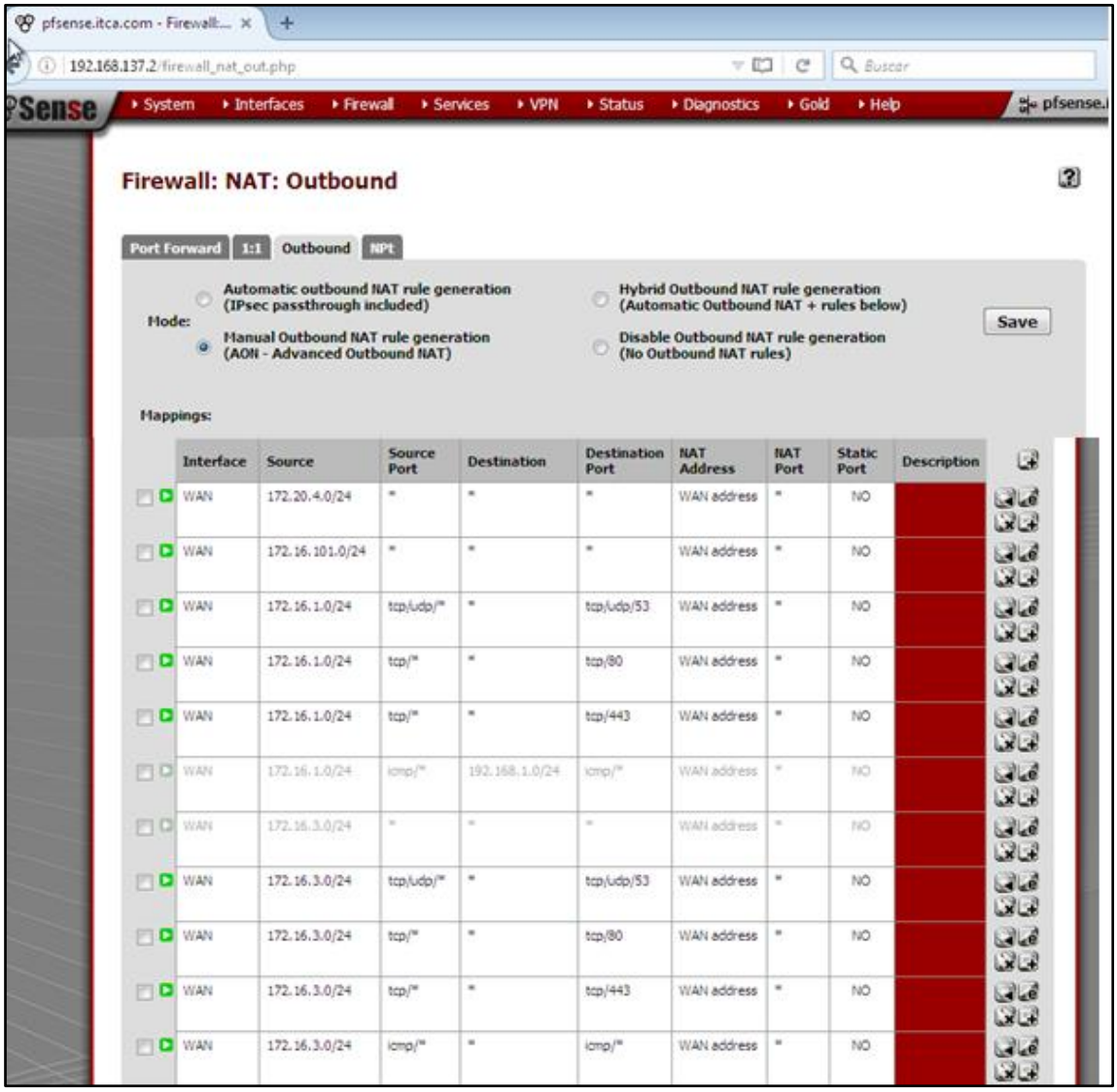


Figura 38. Habitación de puertos para el NAT

Fuente: Pfsense versión 2.2.5

5.7.5 Configuración de Squid Proxy

Squid proporciona un servicio de proxy que soporta peticiones HTTP, HTTPS y FTP para los equipos de la red que necesitan acceder a Internet y a su vez provee la funcionalidad de caché especializado en el cual almacena de forma local las páginas consultadas recientemente por los usuarios. De esta forma, incrementa la rapidez de acceso a los servidores de información Web y FTP que se encuentran fuera de la red LAN

La figura 39 muestra habilitación de Squid Accede al Administrador Web de su pfSense, y haga clic en "Server -> Packages", desplázar por la lista y encontrará Squid y haga clic en "+" para instalar, espere a que finalice el proceso y vuelva a la sección de paquetes para buscar squidguard e instalar también este paquete anteriormente ya se ha instalado una lista negra como se muestra en la figura 40.

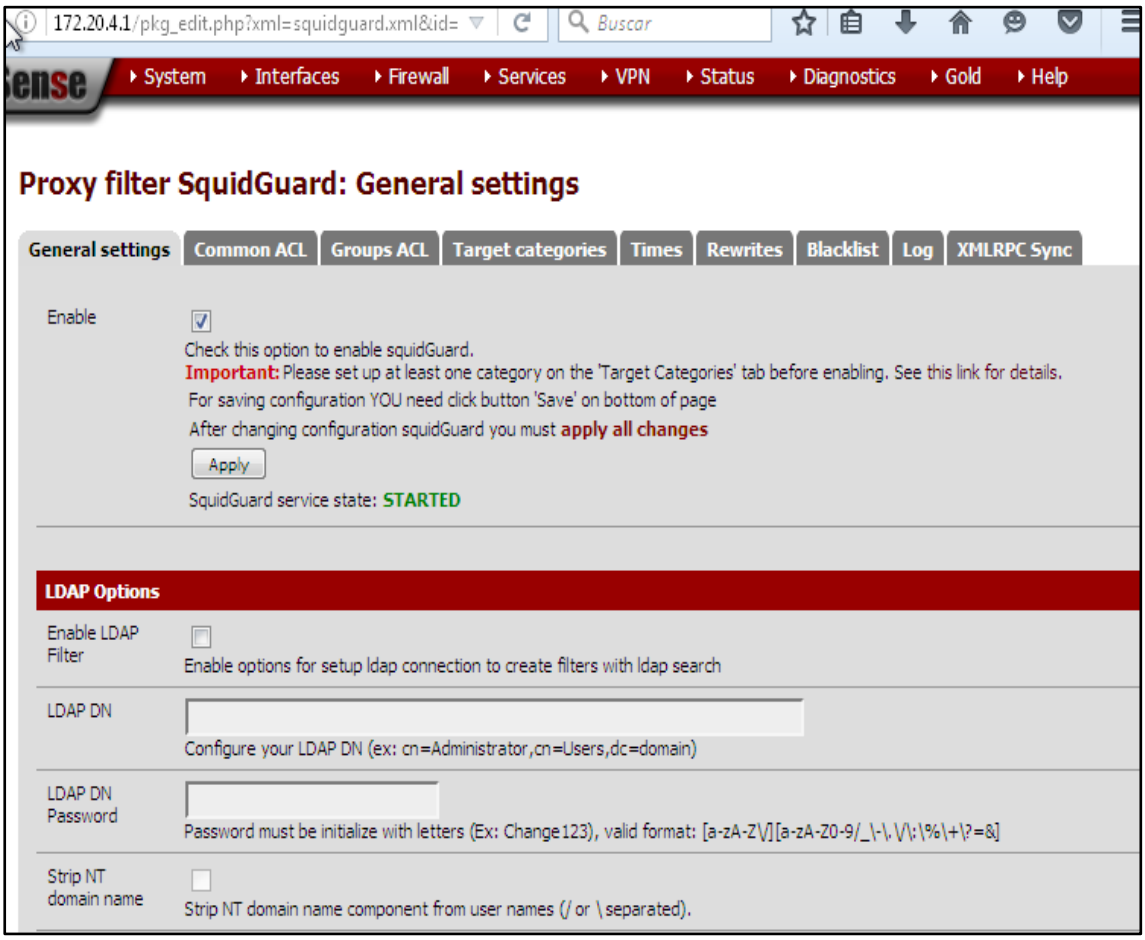


Figura 39. Habilitación de proxy Squid

Fuente: Pfsense versión 2.2.5

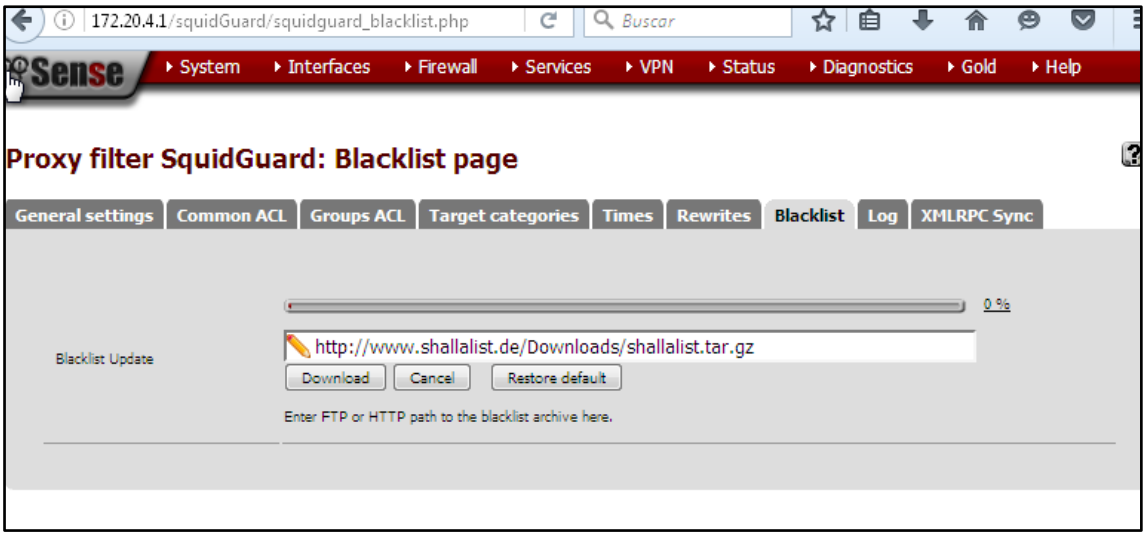


Figura 40.descarga de la lista negra

Fuente: Pfsense versión 2.2.5

- Target Categories permite generar 2 categorías para el bloqueo en la red LAN una para redes sociales y otra para impedir el tipo de descargas .exe, como se indica en la tabla 41.

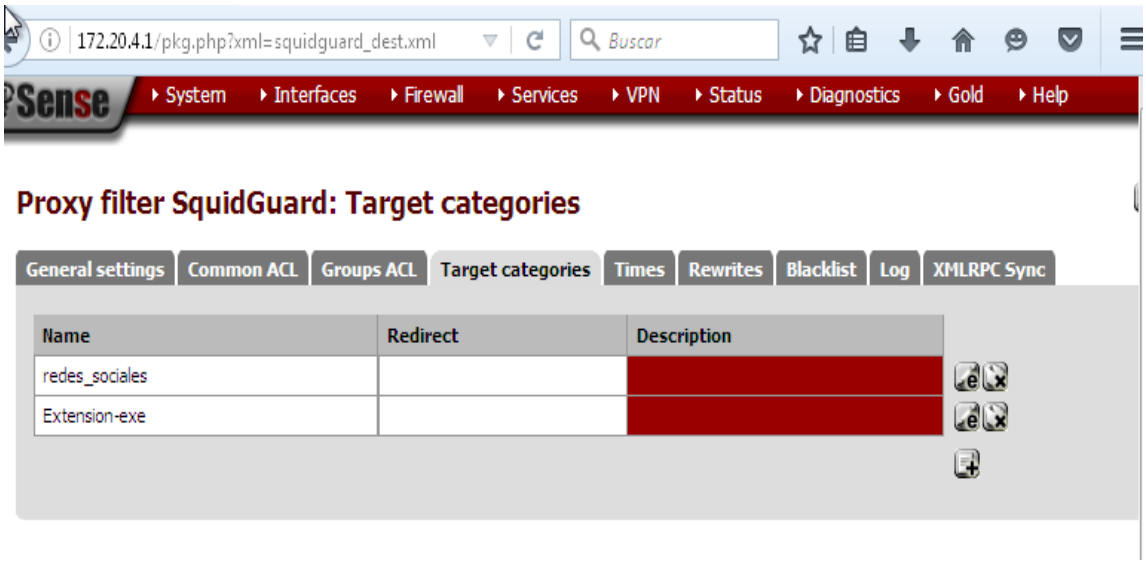


Figura 41.Bloqueo de páginas no deseadas

Fuente: Pfsense versión 2.2.5

- Para especificar cuáles son la redes sociales que se bloquean se ubica directamente el dominio de las paginas como se muestra en la figura 42

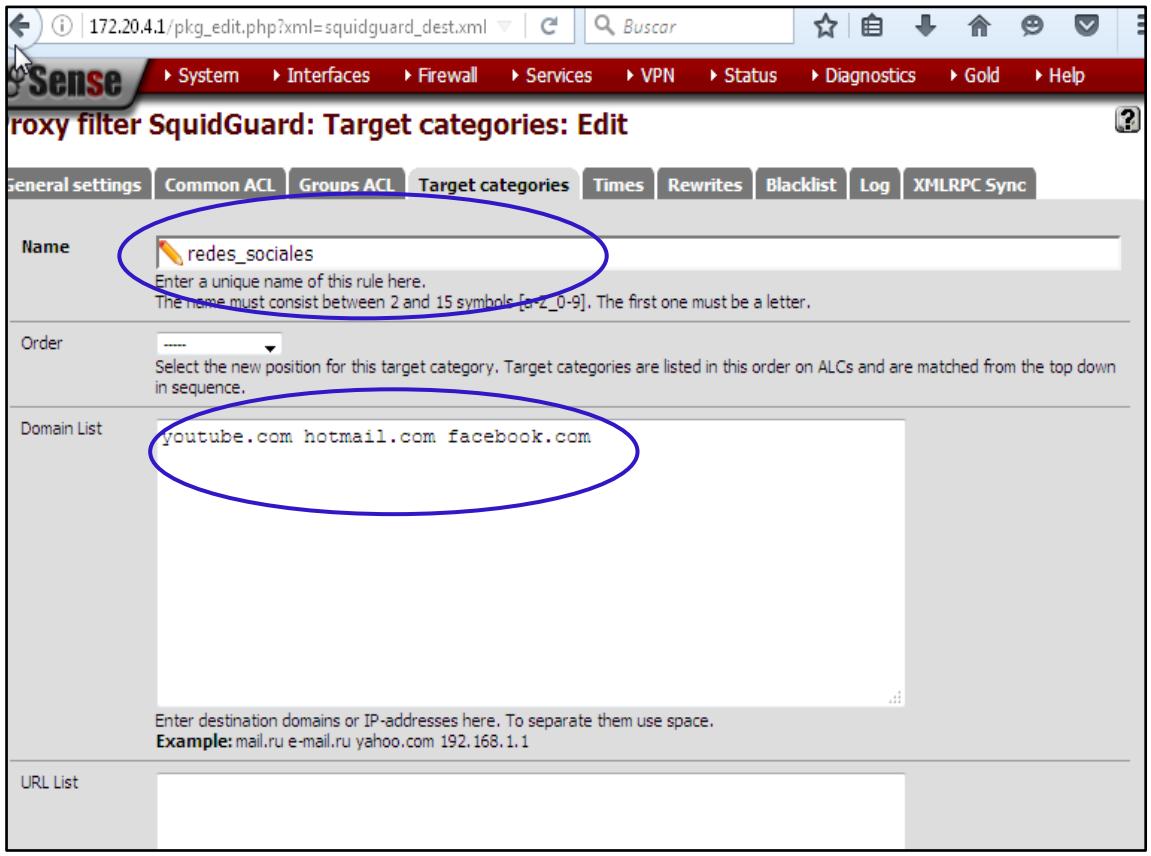


Figura 42. Bloqueo por dominio de las redes sociales

Fuente: Pfsense versión 2.2.5

El bloqueo de las descargas de igual manera se ubica el nombre de la extensión para cada una de las que sean necesarias como se muestra en la figura 43.

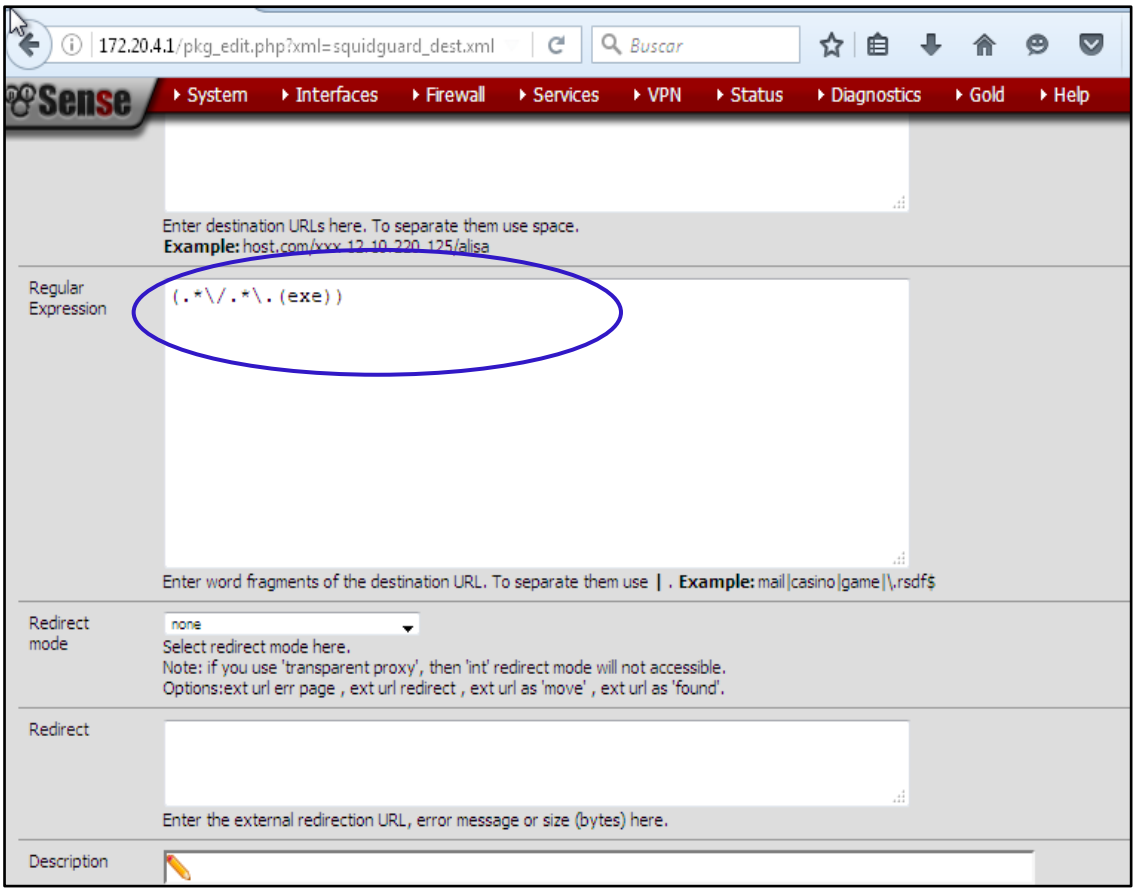


Figura 43. Bloqueo de las descargas

Fuente: Pfsense versión 2.2.5

5.7.6 Reglas del proxy

En la pestaña “groups acl” para crear una lista de acceso ACL. Se ubica la dirección IP o de red a la cual se le quiere aplicar las reglas del proxy como se muestra en la figura 44.

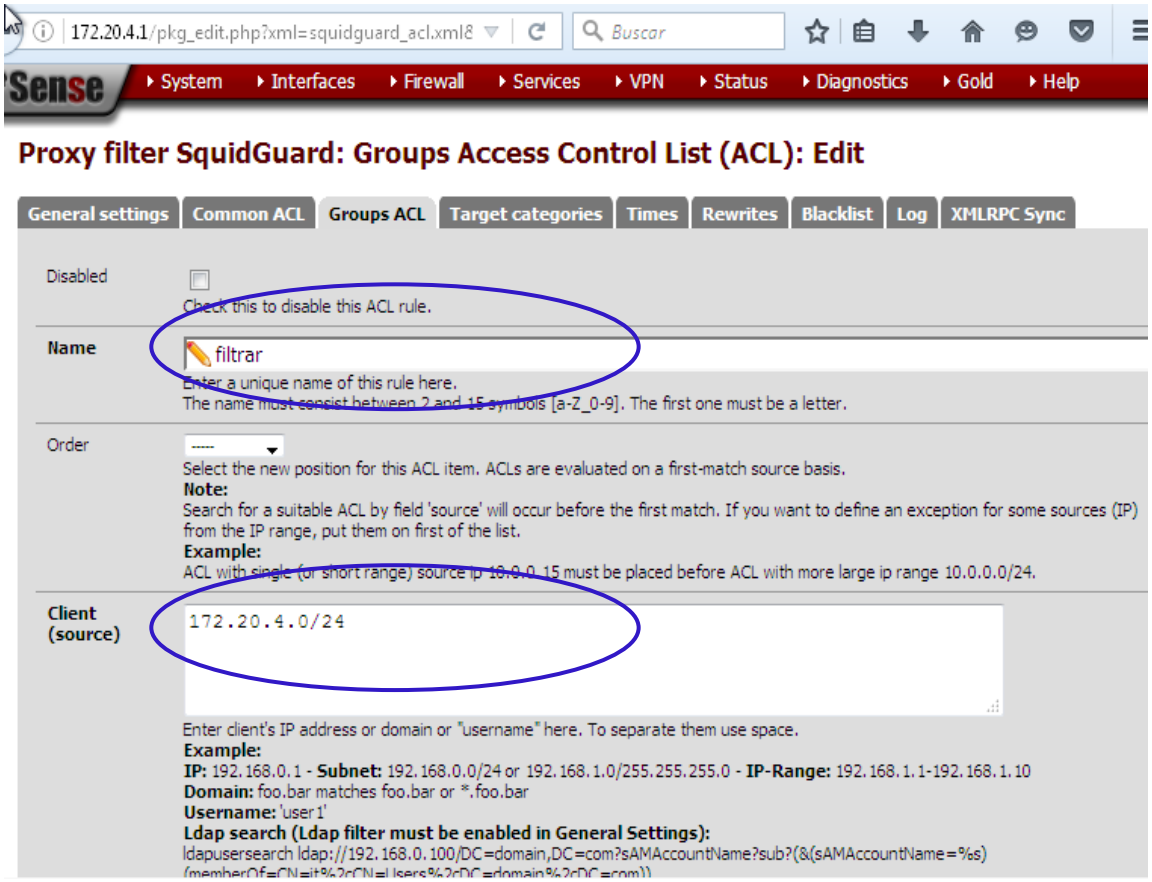


Figura 44.creación de la lista de acceso ACL

Fuente: Pfsense versión 2.2.5

- Se seleccionaTarget Rules, para las opciones de la lista negra y de las categorías que fueron creadas. Para aplicar las reglas. Vamos a denegar páginas con la opción denny para las redes sociales, descargas .exe, y páginas pornográficas, como se muestra en la figuras 45,46 y 47 respectivamente.

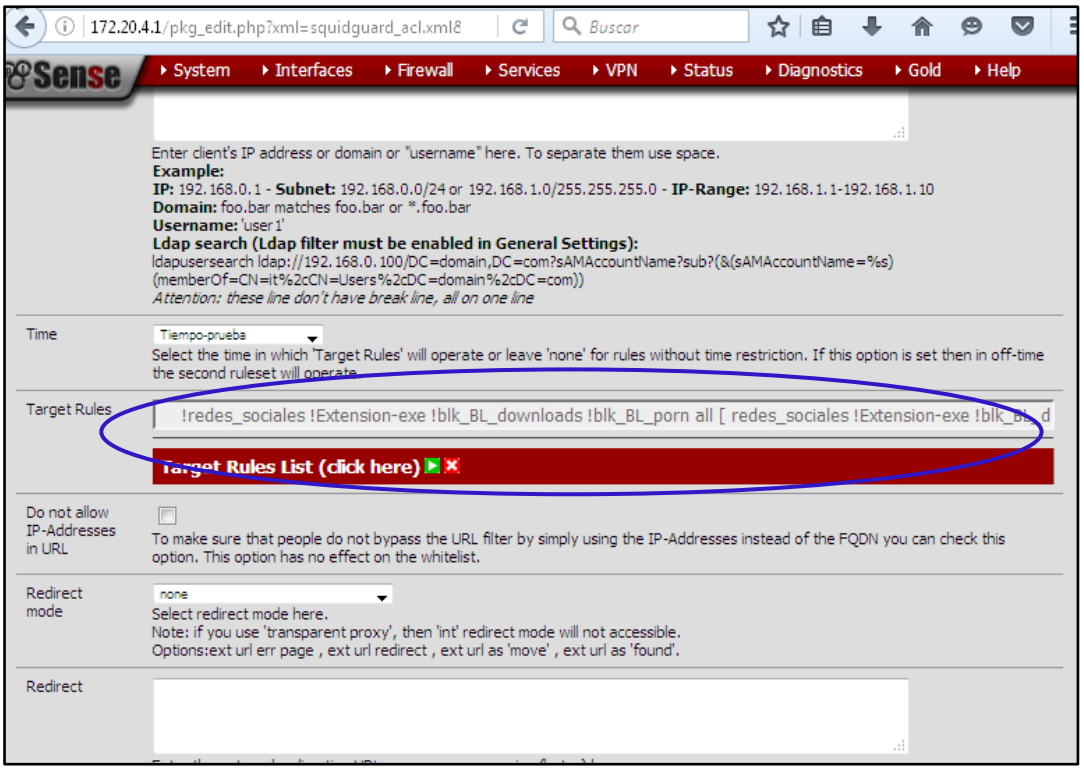


Figura 45. Bloqueo de la páginas de redes sociales.

Fuente: Pfsense versión 2.2.5

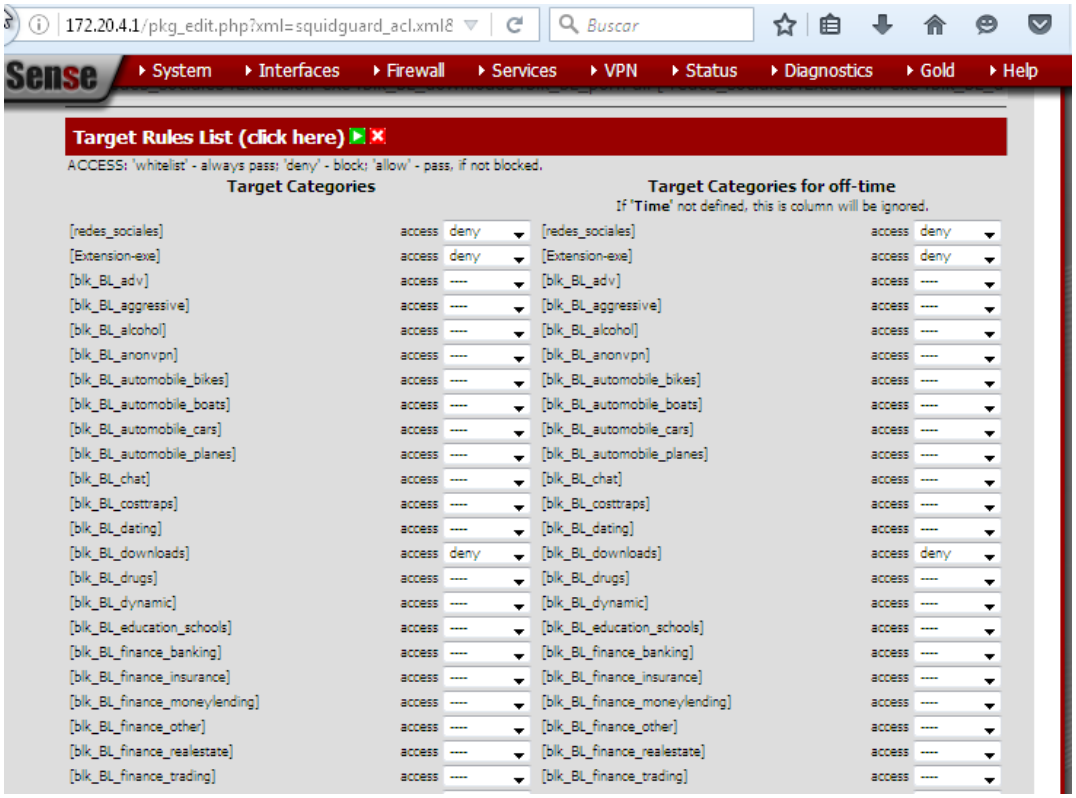


Figura 46. Bloqueo de la páginas para descargas

Fuente: Pfsense versión 2.2.5

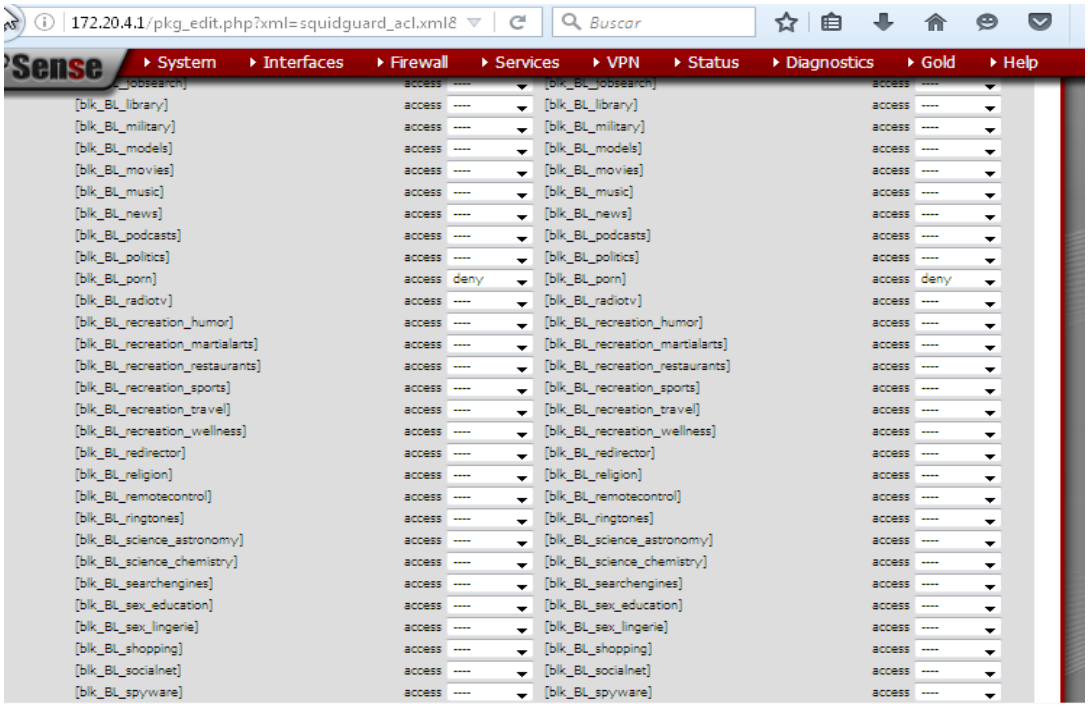


Figura 47. *Bloqueo de la páginas pornográficas*

Fuente: Pfsense versión 2.2.5

- En la pestaña de “General Settings”, para iniciar el servicio del proxy como se muestra en la figura 48.

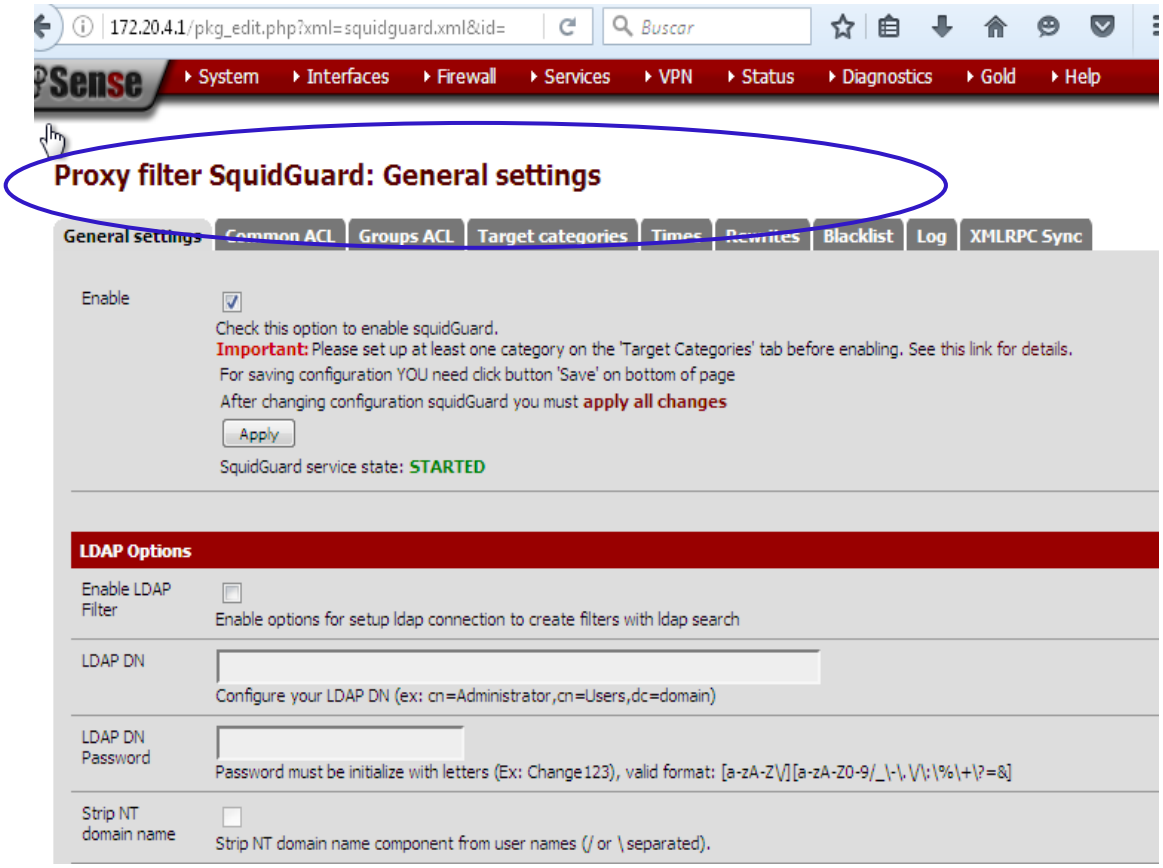


Figura 48. Inicialización del servicio proxy Squid

Fuente: Pfsense versión 2.2.5

5.7.7 Reglas de firewall Pfsense.

Las reglas del firewall se aplican para las tres zonas determinadas para la red WAN, red LAN y la zona desmilitarizada DMZ, donde se deniega el acceso mediante puertos para implementar la seguridad.

En la tablas 49,50 y 51 de muestra la configuración de las reglas para el diseño de las tres zonas en el mismo orden respectivamente.

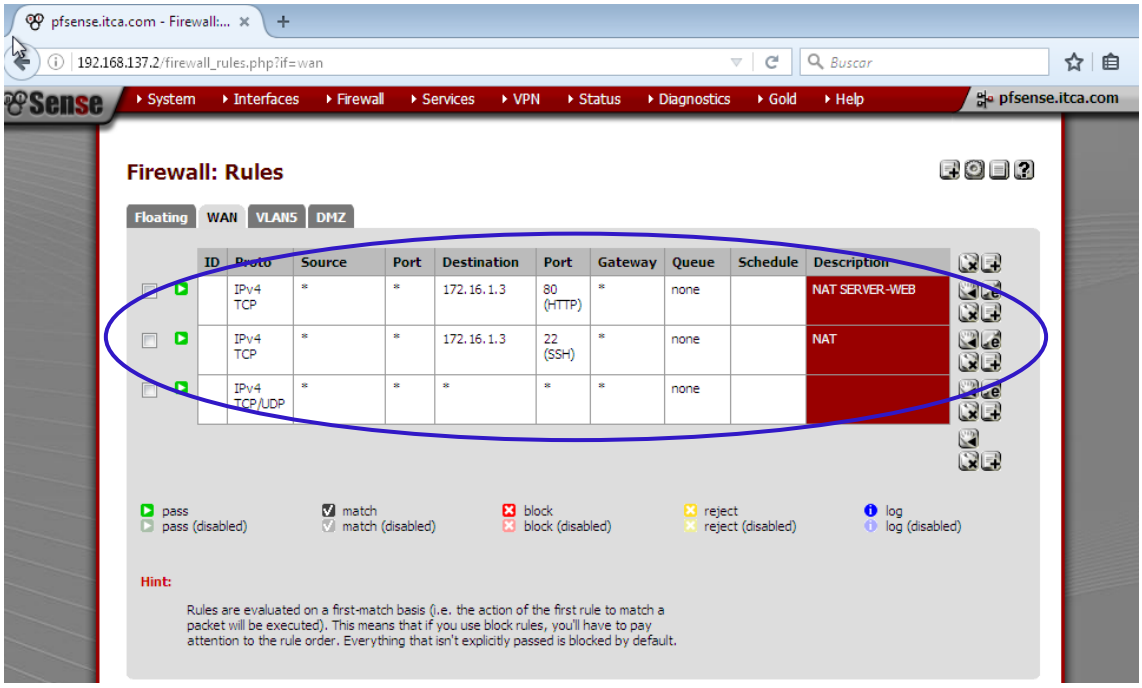


Figura 49. Reglas del firewall para la red WAN

Fuente: Pfsense versión 2.2.5

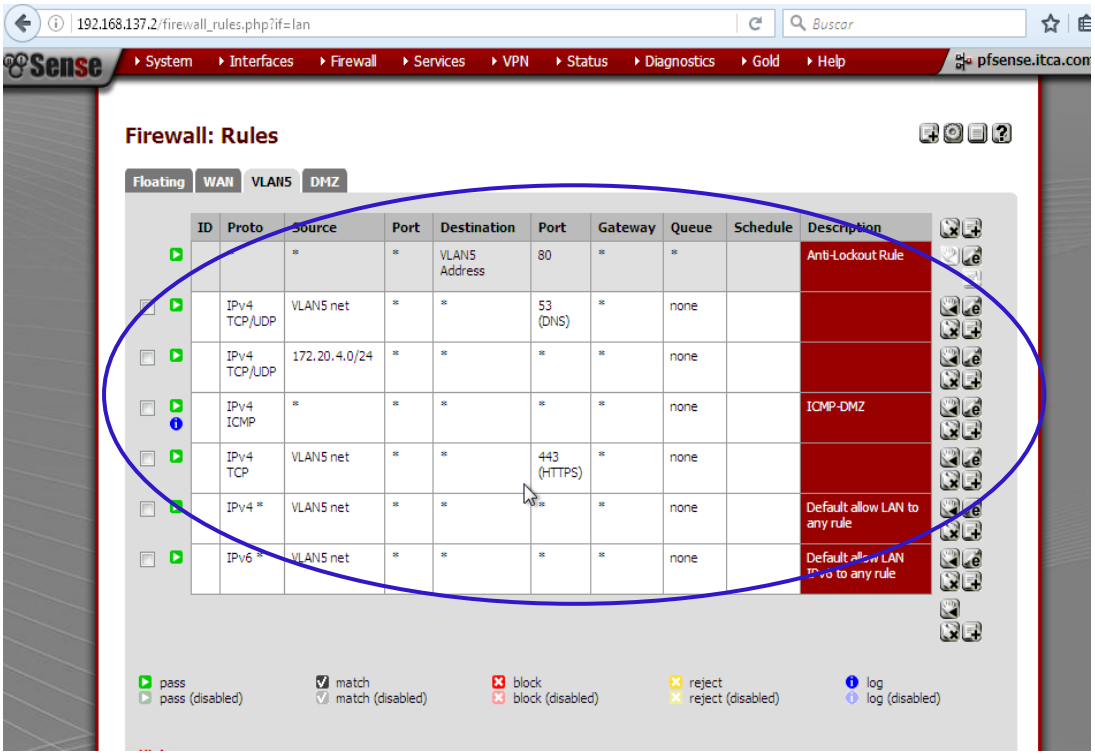


Figura 50. Reglas del firewall para la red LAN

Fuente: Pfsense versión 2.2.5

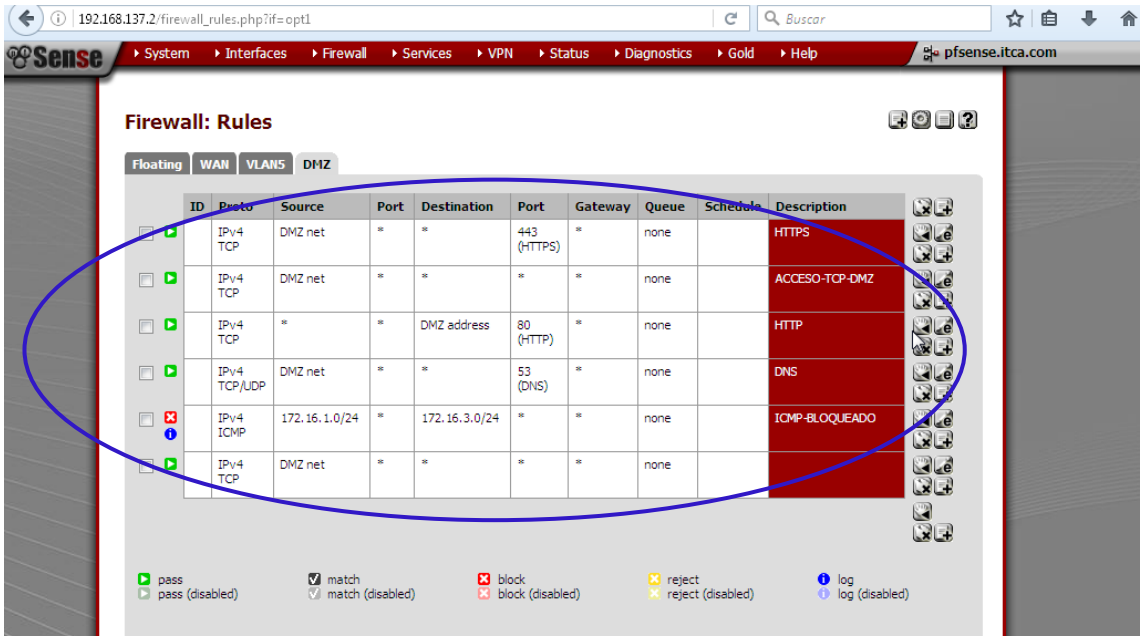


Figura 51. Reglas del firewall para la red DMZ

Fuente: Pfsense versión 2.2.5

5.8 Implementación real del firewall Pfsense en la red del Tecnológico ITCA

La implementación del firewall se realiza con un nuevo direccionamiento es decir con las direcciones IP físicas reales en la red que se muestran en la tabla 45.

Tabla 42. Direccionamiento de la implementación firewall Pfsense

Red	Dirección IP	Mascara	gateway
Red WAN	186.3.102.202	255.255.255.0	186.3.102.201
Red DMZ	172.20.20.1	255.255.255.0	----------
Red LAN	172.20.102.1	255.255.255.0	----------

Fuente: Dirección de Sistemas Tecnológico ITCA

- Configuración de las interfaces del firewall Pfsense Real para la red LAN como se muestra en la imagen de la figura 52.

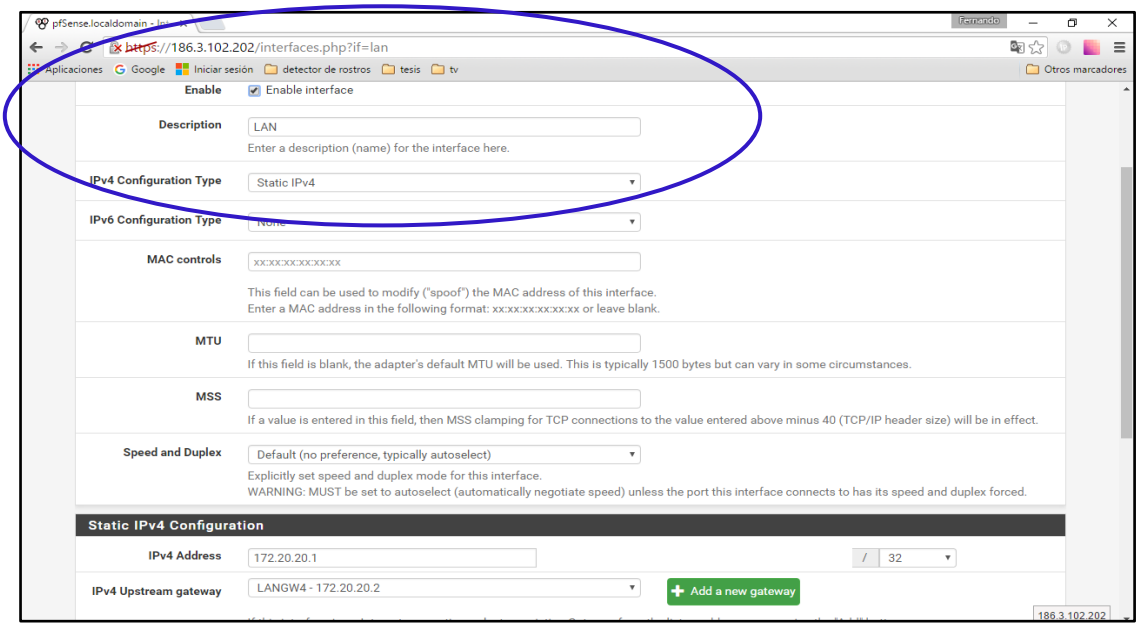


Figura 52. Configuración de interfaz LAN

Fuente: Pfsense versión 2.2.5

- Configuración de las interfaces del firewall Pfsense Real para la red WAN como se muestra en la imagen de la figura 53.

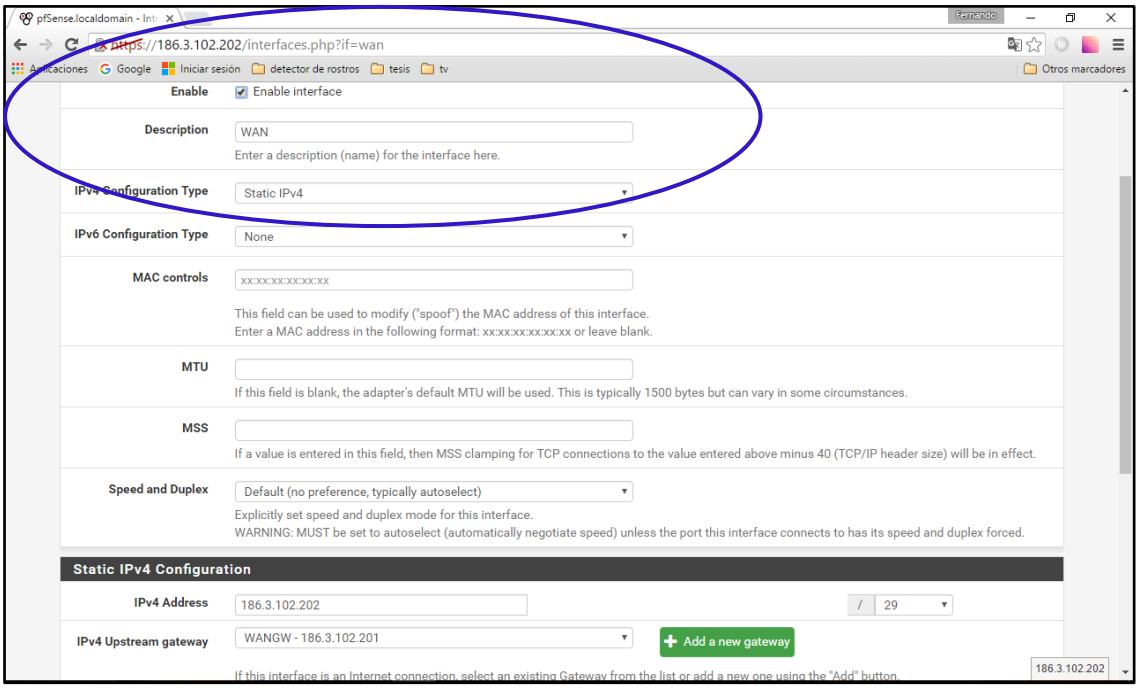


Figura 53. Configuración de interfaz WAN

Fuente: Pfsense versión 2.2.5

- Configuración de las interfaces del firewall Pfsense Real para la red DMZ como se muestra en la imagen de la figura 54.

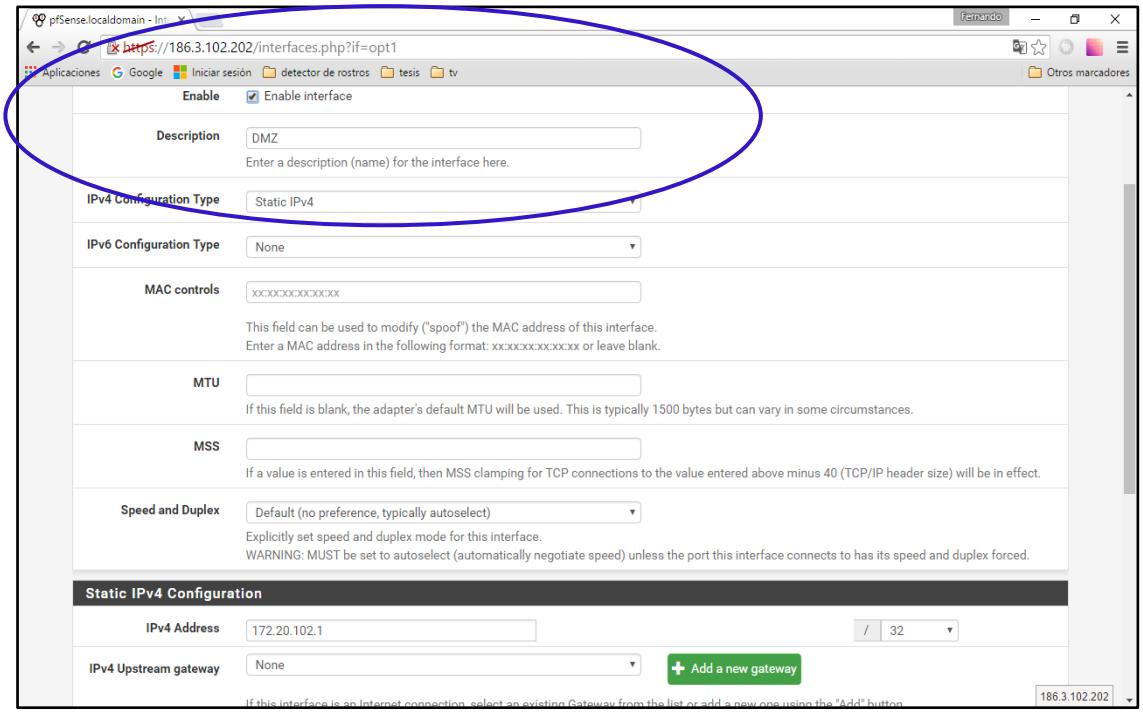


Figura 54. Configuración de interfaz DMZ

Fuente: Pfsense versión 2.2.5

5.9 Implementación real del servidor de dominio de nombres y gateway en la red del Tecnológico ITCA

Para habilitar el acceso a internet se habilita los DNS públicos de la red como se muestra en la figura 55.

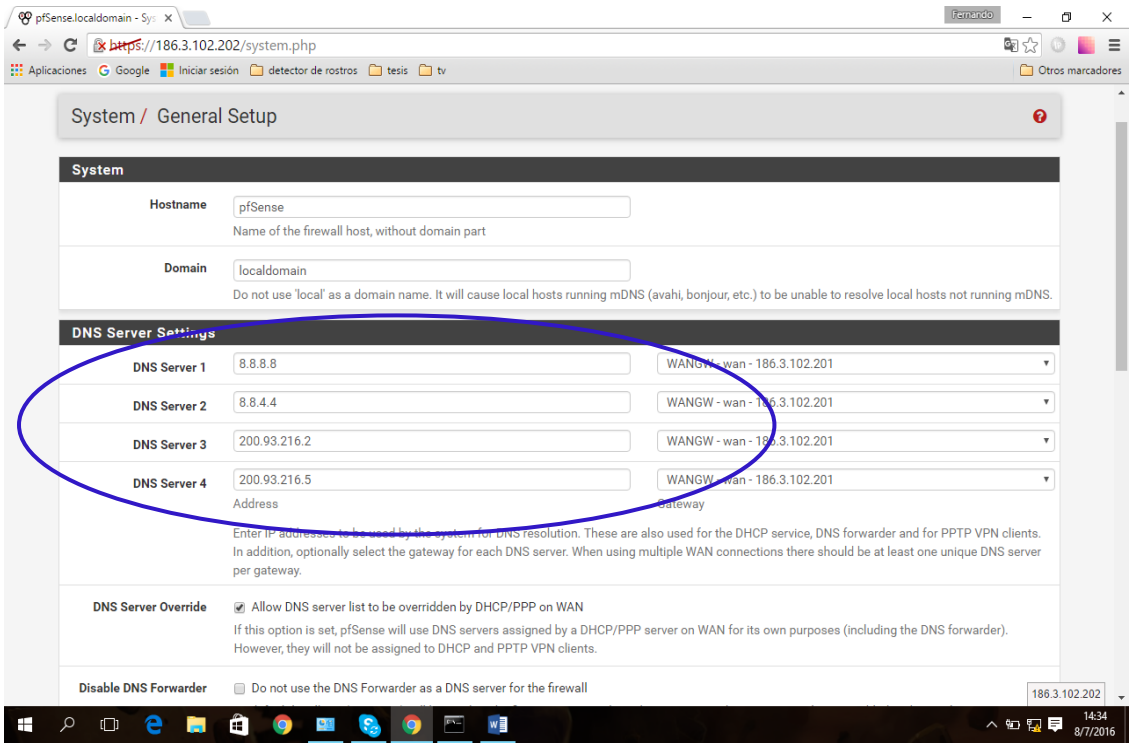


Figura 55. Servidor DNS para el firewall real

Fuente: Pfsense versión 2.2.5

5.9.1 Implementación real NAT red del Tecnológico ITCA.

En NAT para intercambiar los paquetes entre dos redes que asignan mutuamente direcciones y permite el acceso a los servidores desde el exterior. Se permite el trafico TPC de la WAN se habilitan los puestos de comunicación 8080 para HTTP y los de acceso TELNET 2221 como se muestra en la figura 56.

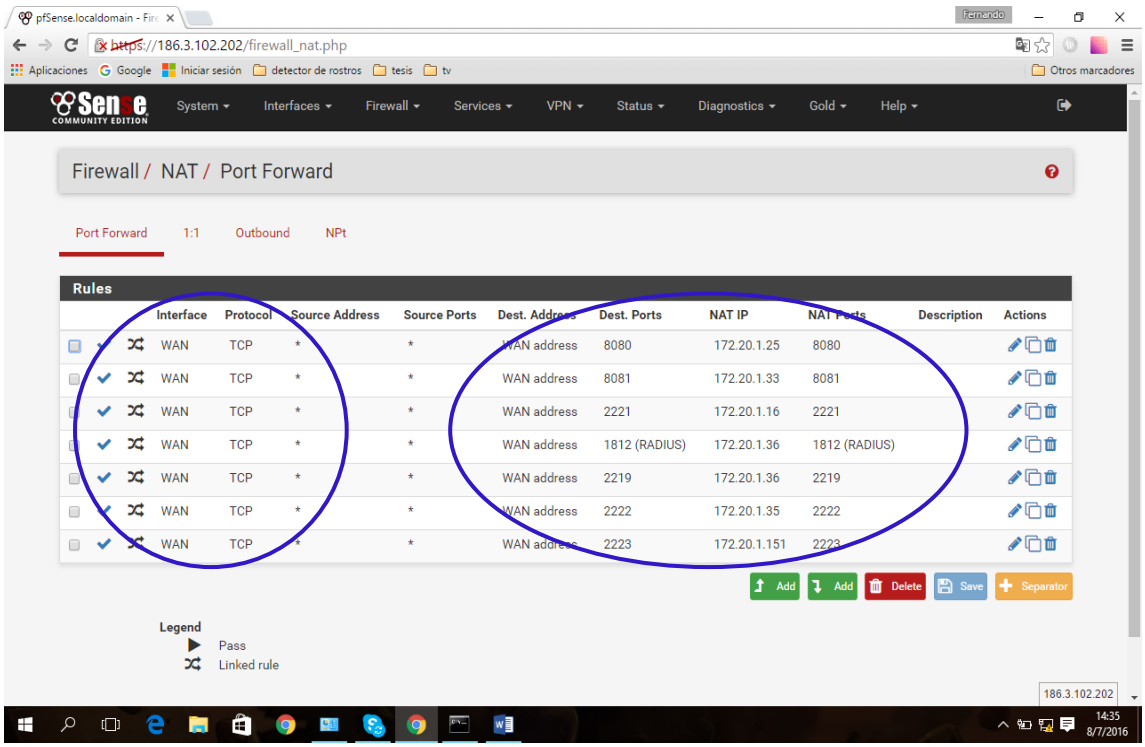


Figura 56. Habilitación del NAT en Firewall real

Fuente: Pfsense versión 2.2.5

5.9.2 Implementación de la reglas del firewall en red del Tecnológico ITCA.

Se aplican las reglas para las tres redes red WAN, LAN y Zona DMZ, se ha denegado todo por defecto y solo se habilita lo necesario como se muestra en la figuras 57, 58 y 59. Para las tres redes antes mencionadas.

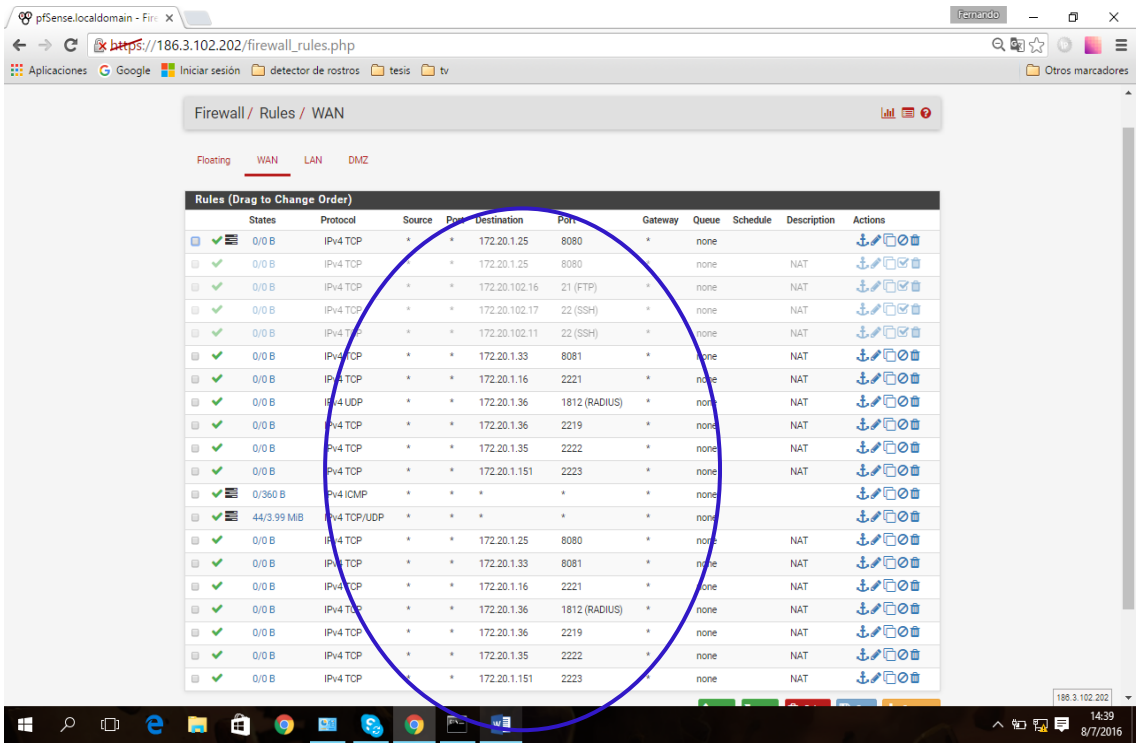


Figura 57. ***Reglas del firewall para la red WAN***

Fuente: Pfsense versión 2.2.5

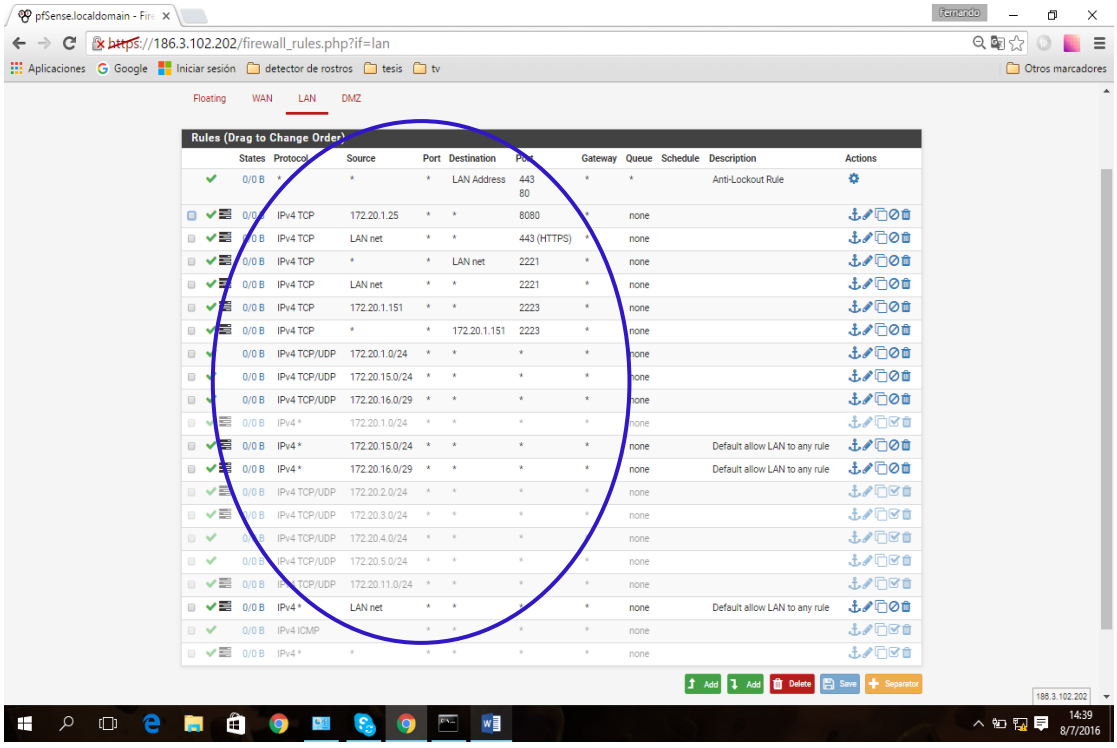


Figura 58. ***Reglas del firewall para la red LAN***

Fuente: Pfsense versión 2.2.5

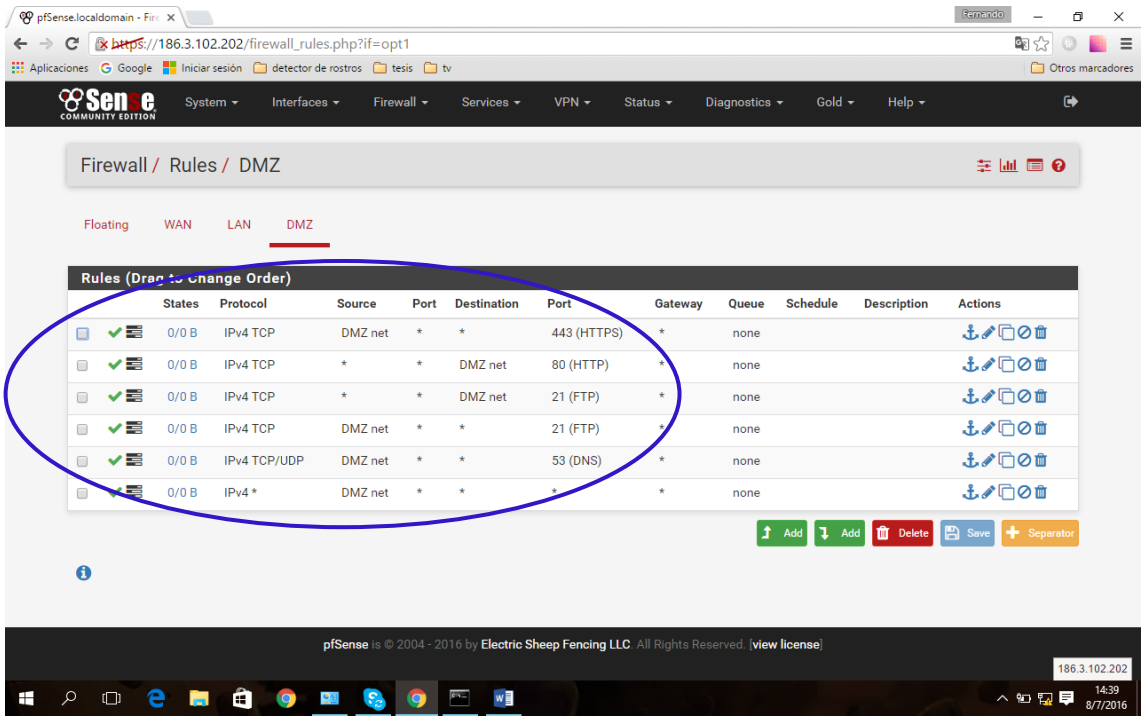


Figura 59. Reglas del firewall para la red LAN

Fuente: Pfsense versión 2.2.5

5.9.3 Saturación del firewall implementado en red del Tecnológico ITCA.

En el desarrollo de la implantación se configuran las tres redes, red LAN, WAN Y DMZ en la puesta en marcha del firewall la red empieza con una saturación relativamente alta como se muestra en la figura 60.

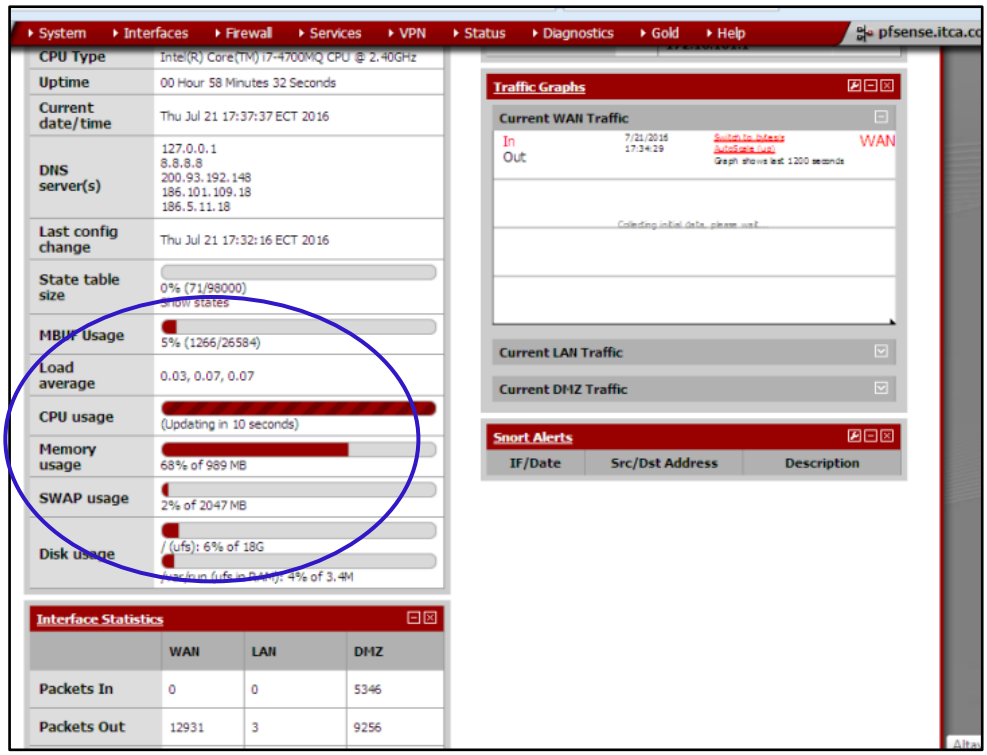


Figura 60.saturación del servidor firewall Pfsense implantado

Fuente: Pfsense versión 2.2.5

5.10 sistema de prevención de intrusos (IPS).

El software de Pfsense incluye un paquete de instalación de un sistema de prevención de intrusos Snort. Se puede configurar para que simplemente registrar eventos y alertas de red detectados y/o bloquear las amenazas.

Este paquete está disponible para instalar desde System> Packages como se muestra en la figura 61.

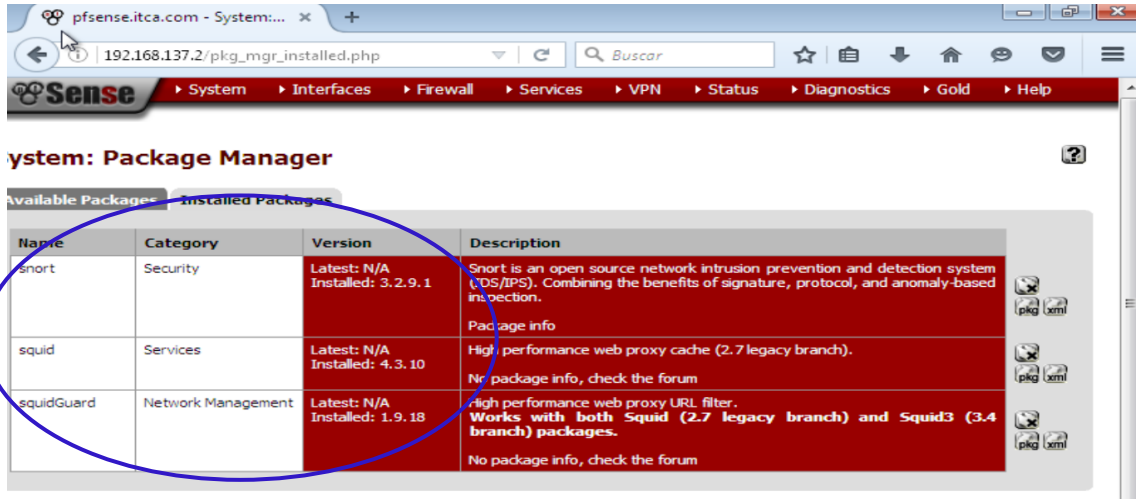


Figura 61.instalación del software Snort

Fuente: Pfsense versión 2.2.5

Se crea automáticamente una lista de las direcciones IP que conforman el sistema Snort, se añaden las direcciones de red y subredes de la red LAN y DMZ como se muestra en la figura 62.

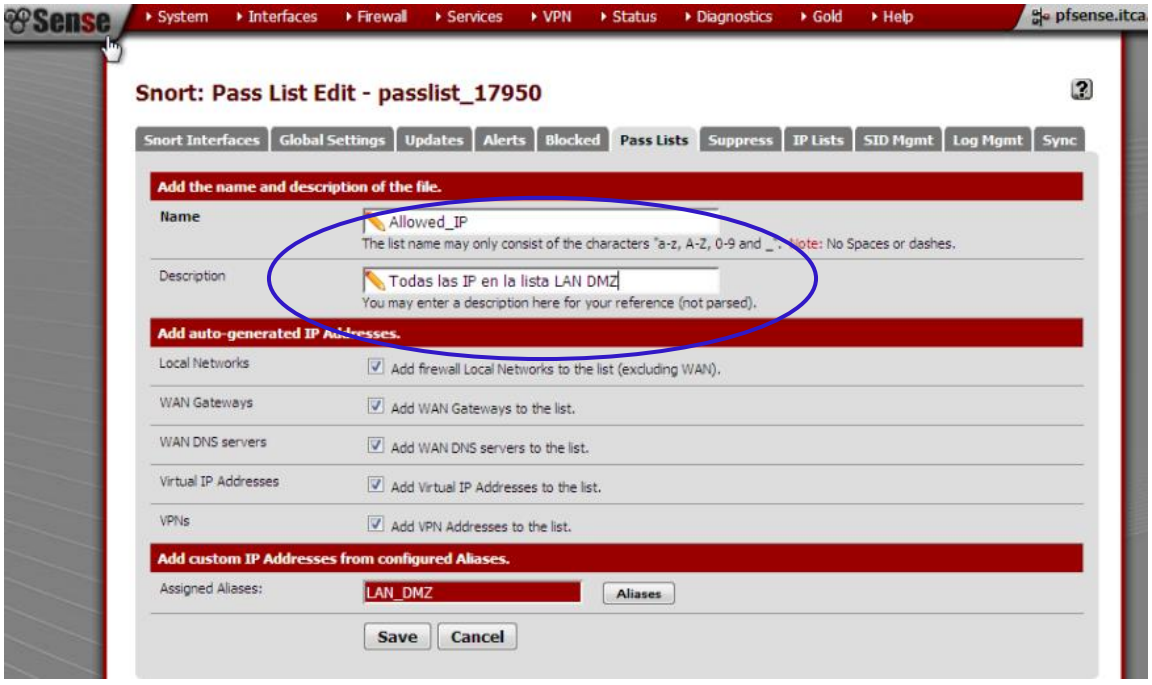


Figura 62. Creación de la lista de direcciones IP en Snort.

Fuente: Pfsense versión 2.2.5

Se debe reiniciar los servicios Snort para que se inicialice la figura 63 y 64 muestra el proceso.

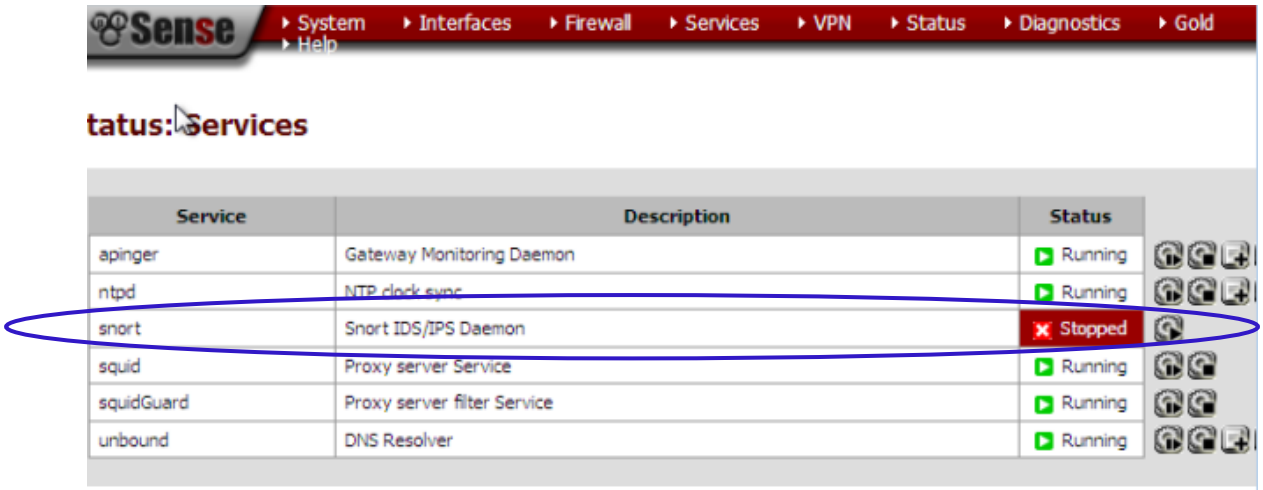


Figura 63. Servicio de Snort no inicializado

Fuente: Pfsense versión 2.2.5

Debe reiniciarse el servidor para que vuelva a funcionar de manera correcta como muestra la figura 64.

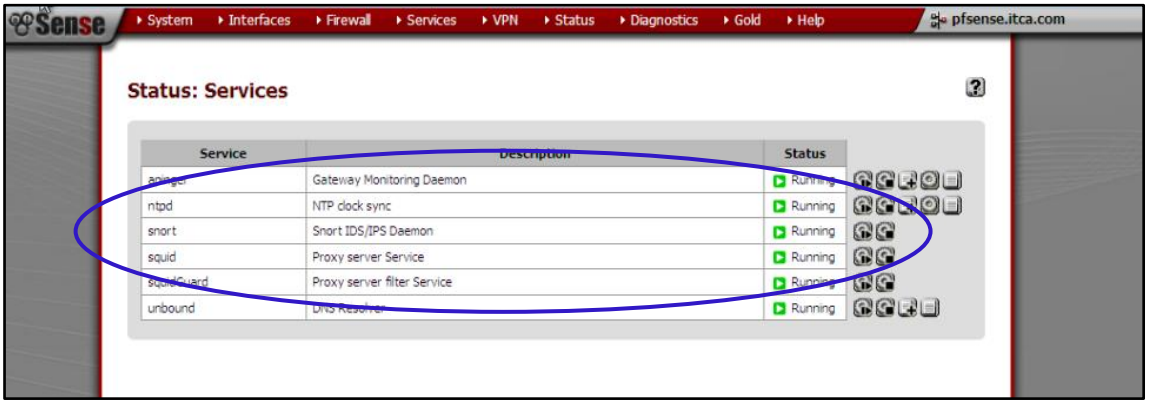


Figura 64. Servicio de Snort inicializado

Fuente: Pfsense versión 2.2.5

Elección de reglas de seguridad en Snort para que el sistema se encuentre correctamente funcionando se ubica en las listas siguientes como muestra la figura 65 y 66.

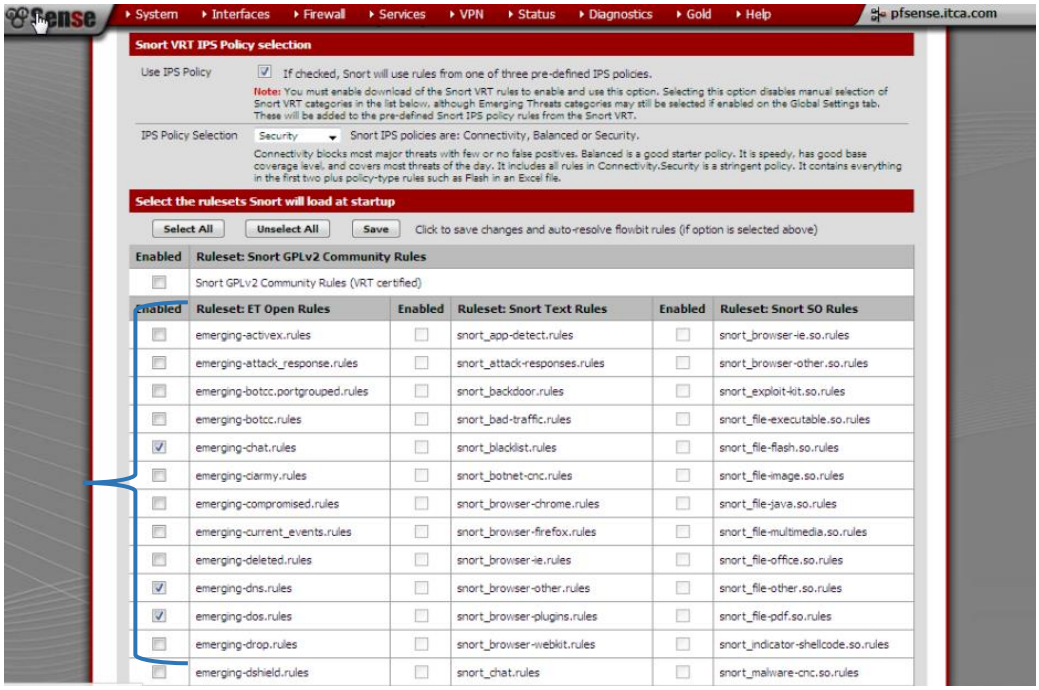


Figura 65. Reglas de Snort seleccionadas

Fuente: Pfsense versión 2.2.5

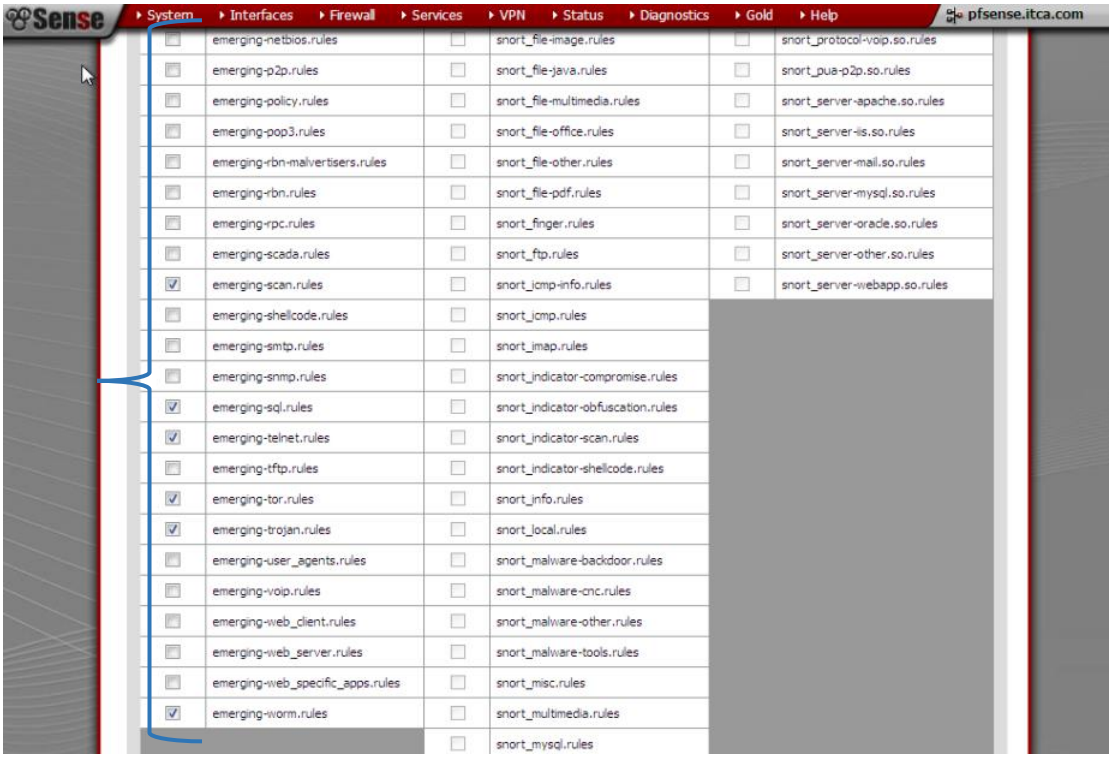


Figura 66. Reglas de Snort seleccionadas (continuación)

Fuente: Pfsense versión 2.2.5

CAPÍTULO VI

6 Pruebas de verificación y funcionamiento del sistema de seguridad perimetral.

Se simularán varios ataques informáticos, para realizar las pruebas de funcionamiento y aplicabilidad los cuales demostrarán el correcto funcionamiento del sistema de Seguridad Perimetral.

6.1 Pruebas del servicio Squid

A continuación se realiza pruebas apegándose a las ciertas políticas de seguridad como por ejemplo la limitación, de la navegación a ciertas páginas.

6.1.1 acceso a internet a través de proxy Squid

La siguiente regla en, Squid permite el acceso a red de internet, la figura 67 muestra que el acceso a la red es exitoso para la página principal del navegador de Google Chrome.

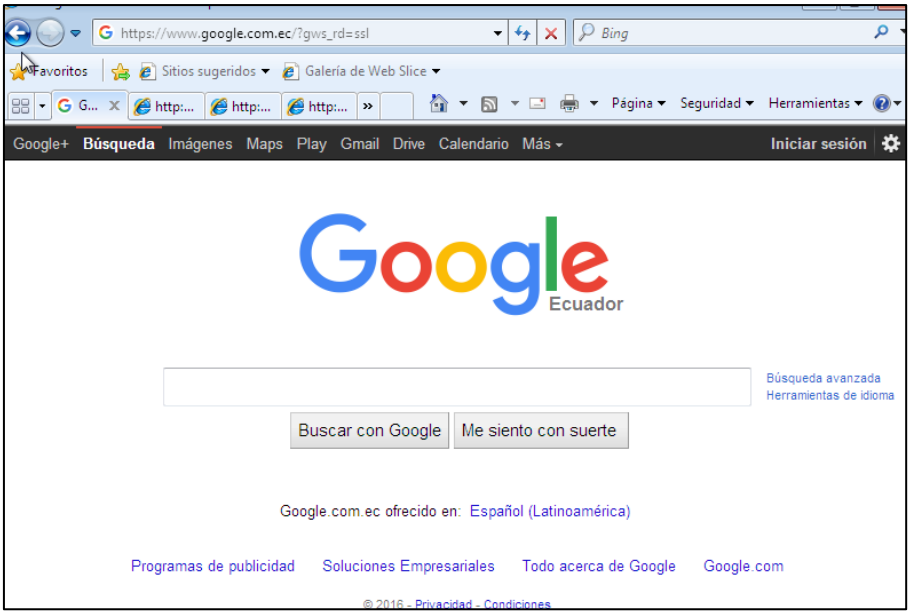


Figura 67.acceso exitoso a Google

Fuente: Pfsense versión 2.2.5

6.1.2 Degación de las páginas de restringidas

Ya se había configurado anteriormente la restricción a las páginas de acceso a redes sociales, descargas y páginas pornográficas, las imágenes 68,69 ,70 y 71 muestran la negación de acceso a estas páginas al tratar de abrir desde el navegador.

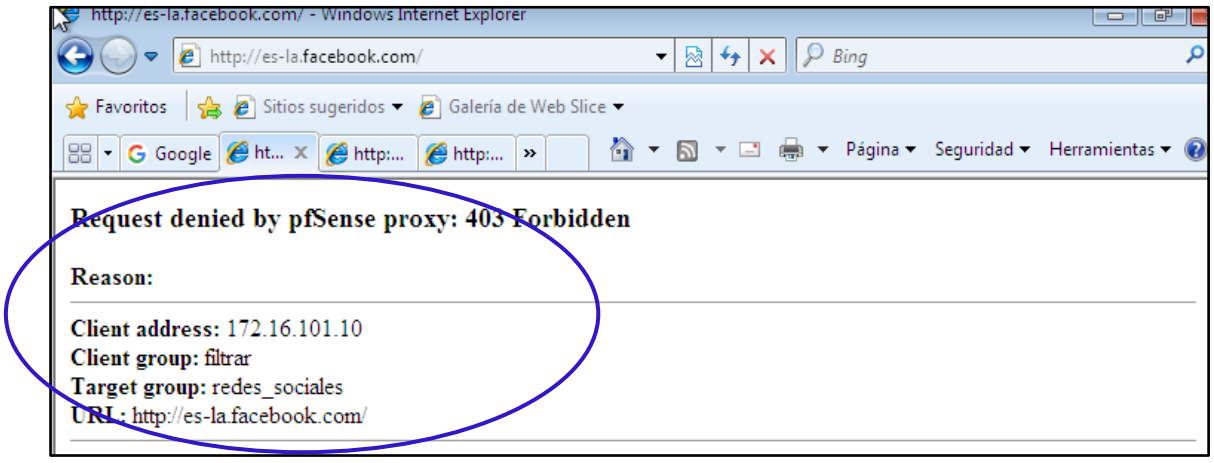


Figura 68. Restricción a la página de Facebook

Fuente: Pfsense versión 2.2.5

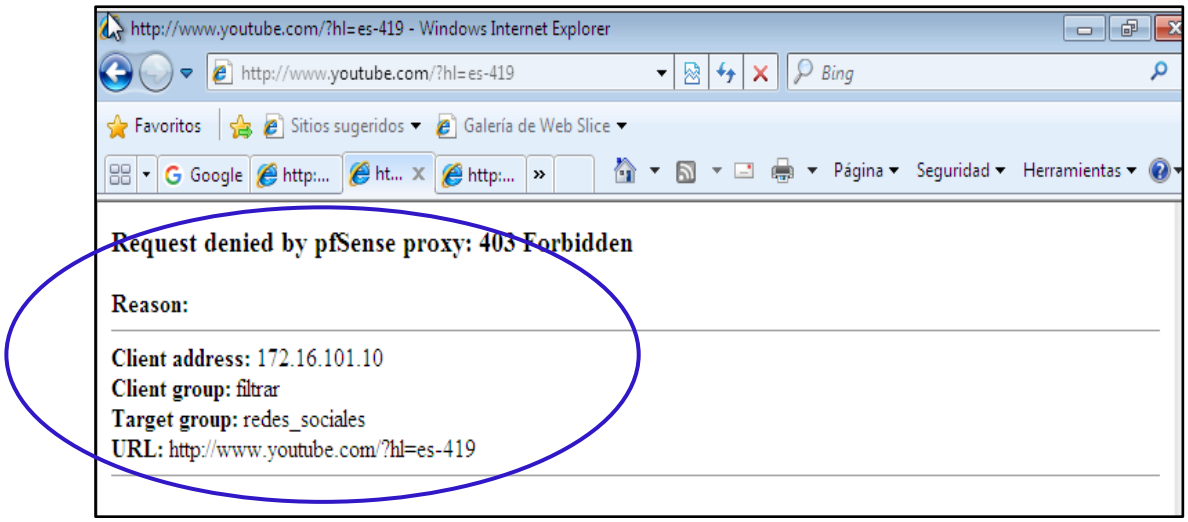


Figura 69. Restricción a la página de vide youtube

Fuente: Pfsense versión 2.2.5

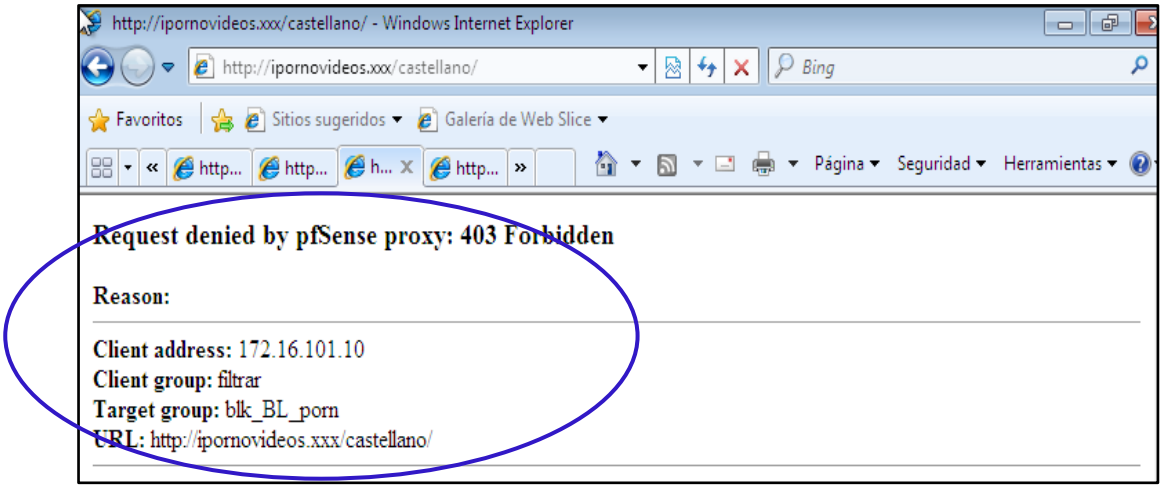


Figura 70. Restricción a la página pornografica

Fuente: Pfsense versión 2.2.5

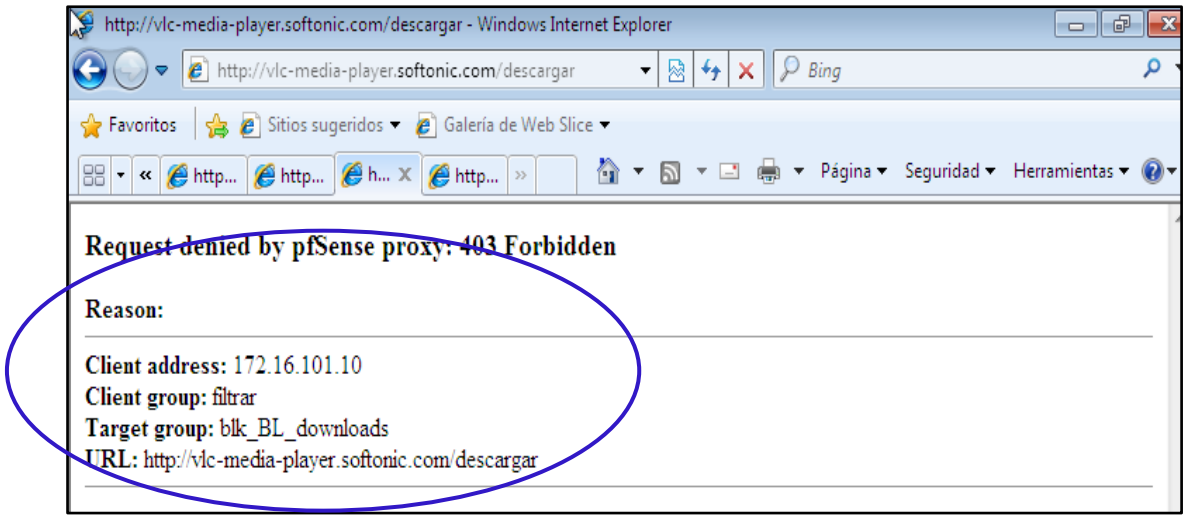


Figura 71. Restricción a la página de descargar softonic

Fuente: Pfsense versión 2.2.5

6.2 Ataque de envenenamiento a la red, mediante ataque hombre en el medio, utilizando kali-linux

Un Ataque de Hombre en el Medio o abreviado con MITM es una forma de realizar una escucha a escondidas en el cual un atacante realizan conexiones independientes con las víctimas y se retransmiten los mensajes entre ellos, haciéndolos creer que están hablando directamente el uno con el otro sobre una conexión privada, cuando en realidad la conversación completa es controlada por un atacante.

Se utilizarán las herramientas de Kali Linux que son ettercapp y driffnet donde, el o los atacantes deben ser capaz de husmear todos los mensajes pasando entre las dos víctimas.

Para continuar con el ataque por envenenamiento de utiliza la herramienta de ettercap que se inicializa mediante el comando ~# ettercap –G como indica la figura 72.

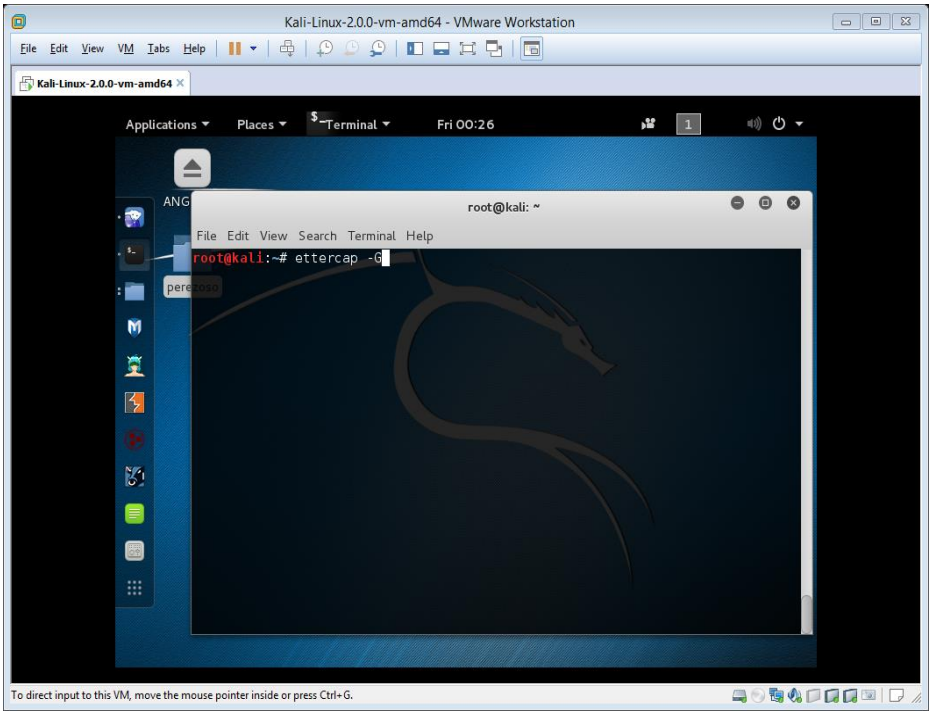


Figura 72 muestra la ejecución del comando de ettercap en Kali Linux

Fuente: herramienta Kali-linux

A continuación como indica la figura 73 se elige la opción unified sniffing para realizar la escucha.

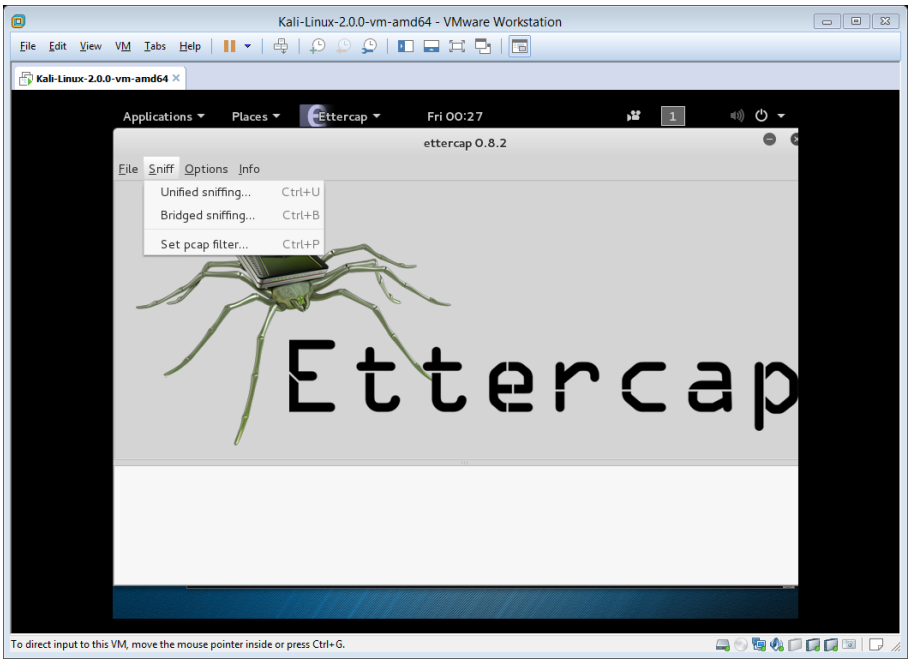


Figura 73 selecciona la opción para empezar con la escucha

Fuente: herramienta Kali-linux

Se continúa con la selección de la tarjeta de red que permite la conexión a internet como indica la figura 74

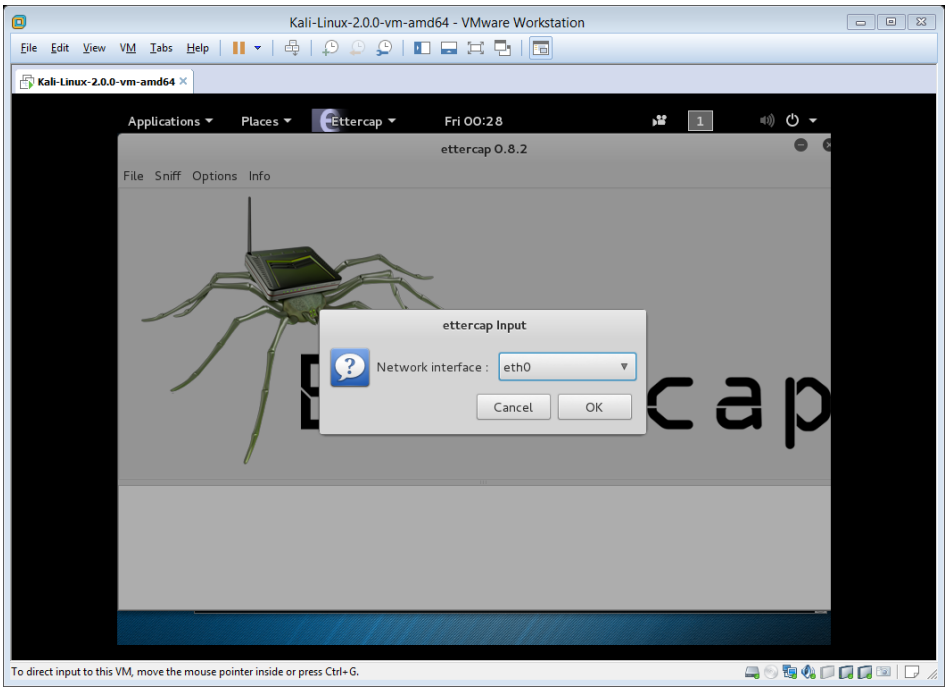


Figura 74 Selección de la tarjeta de red

Ahora se procede con el escaneo de host que están en la red como indica la figura 75 y 76

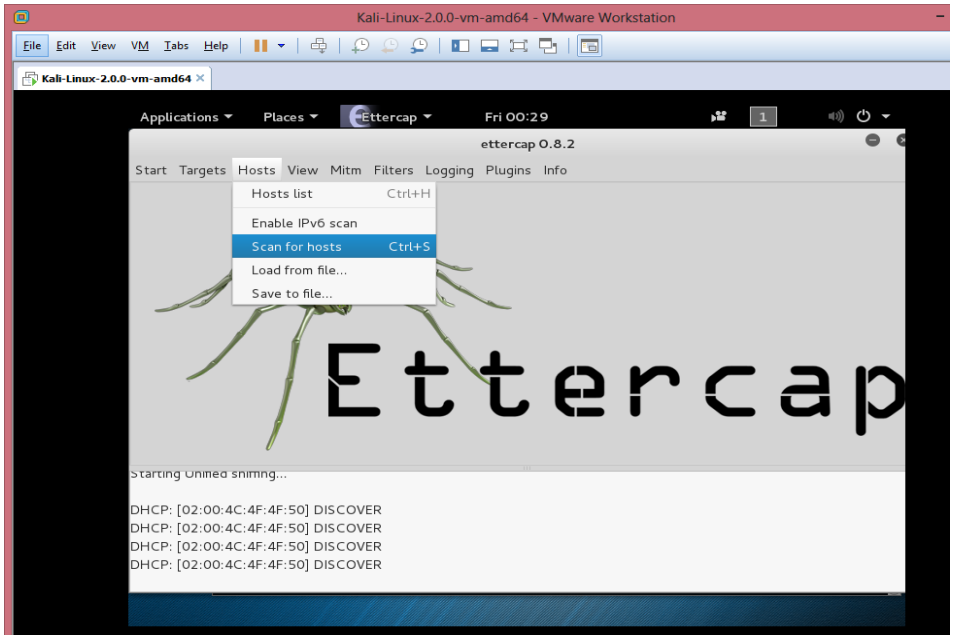


Figura 75 Selección del host para escanear

Fuente: herramienta Kali-linux

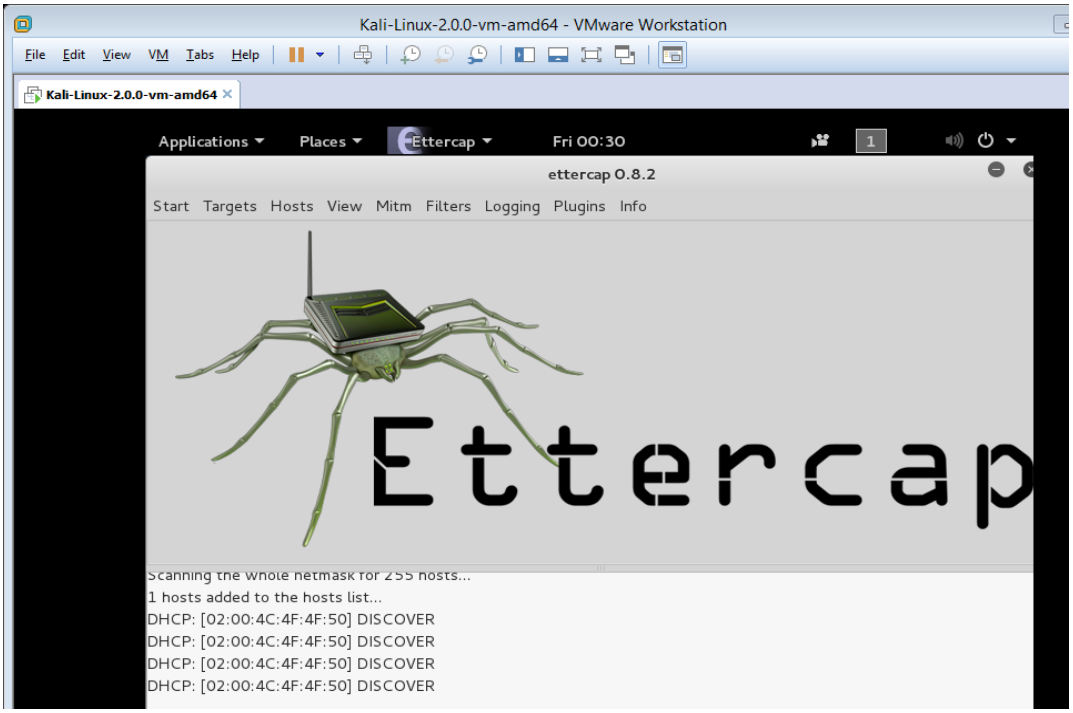


Figura 76 Selección del host para escanear

Fuente: herramienta Kali-linux

Se puede muestra la lista de host encontrados en la red que se realizó el escaneo como indica la figura 77.

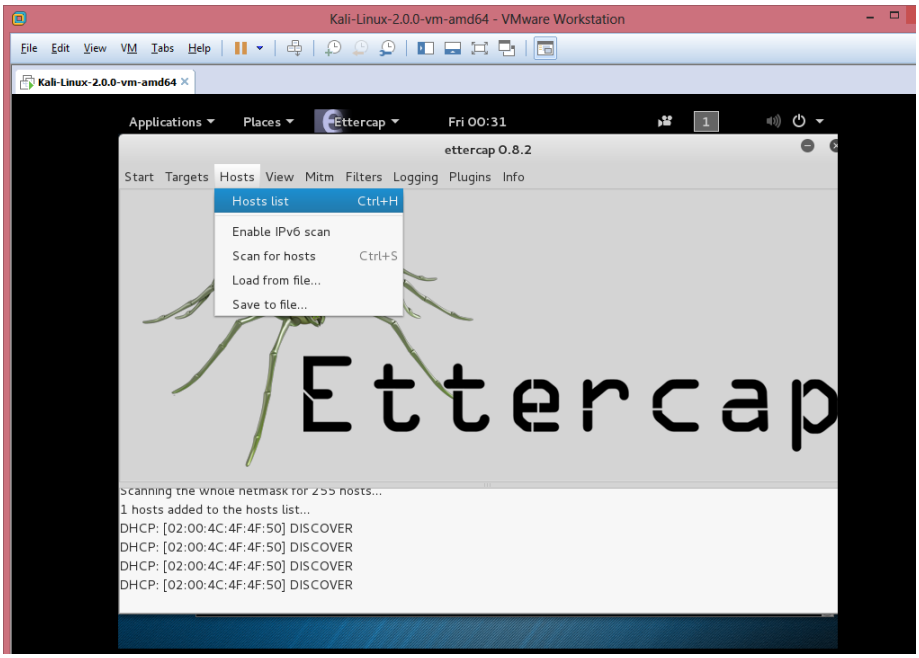


Figura 77 lista de los host escaneados

Fuente: herramienta Kali-linux

Seleccionamos el host víctima mediante la dirección IP para realizar el ataque y se agrega como objetivo 1 como indica la figura 78.

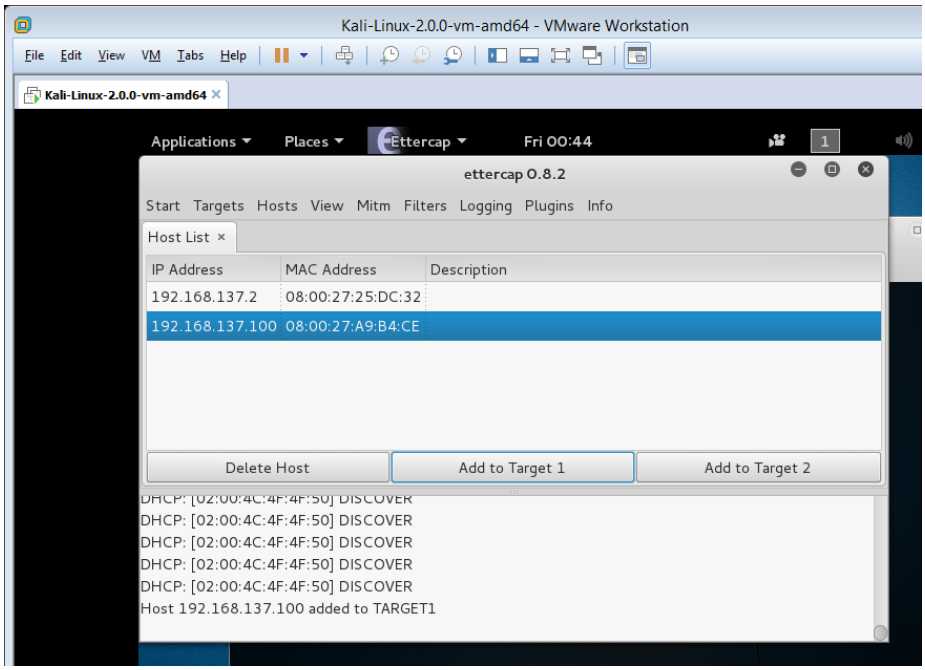


Figura 78 Selección del host y la dirección IP

Fuente: herramienta Kali-linux

A continuación selecciona el firewall pfsense como objetivo 2 como indica la figura 79

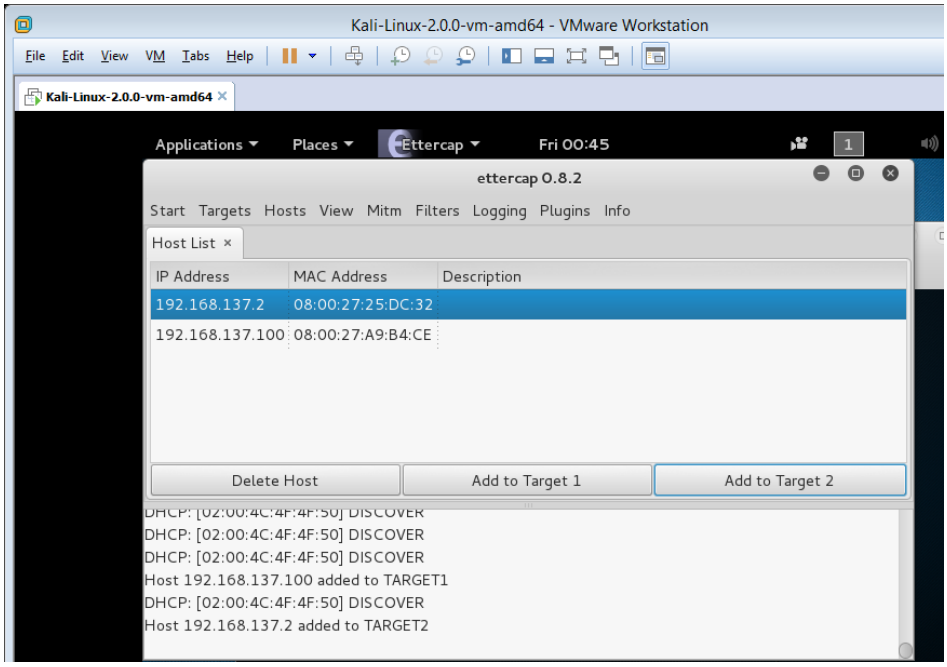


Figura 79 Firewall Pfsense como objetivo 2

Fuente: herramienta Kali-linux

Se activa el módulo de envenenamiento como indica la figura 80 .

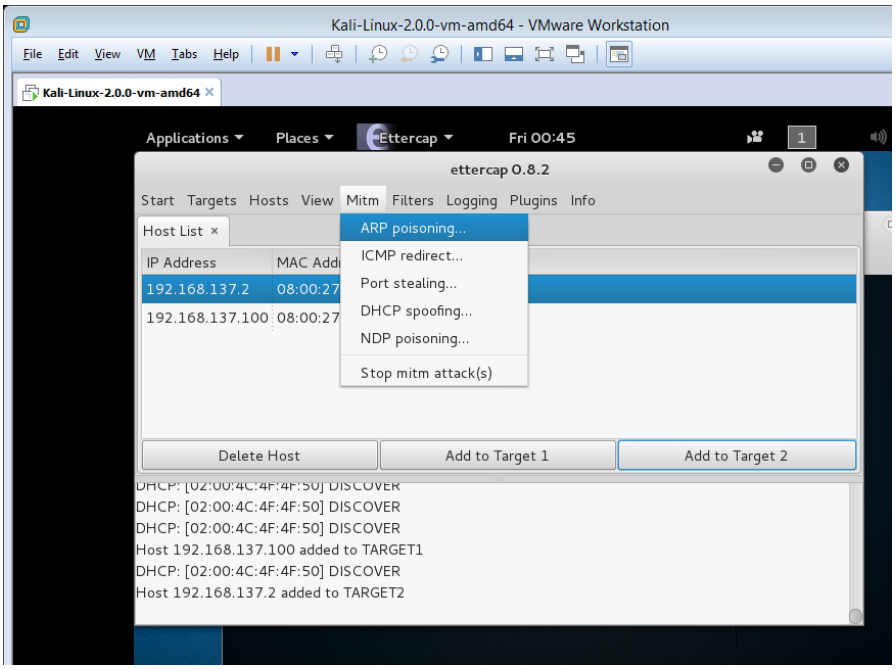


Figura 80. Objetivo 2 Pfsense

Fuente: herramienta Kali-linux

Activación del sniffer remoto como indica la figura 81

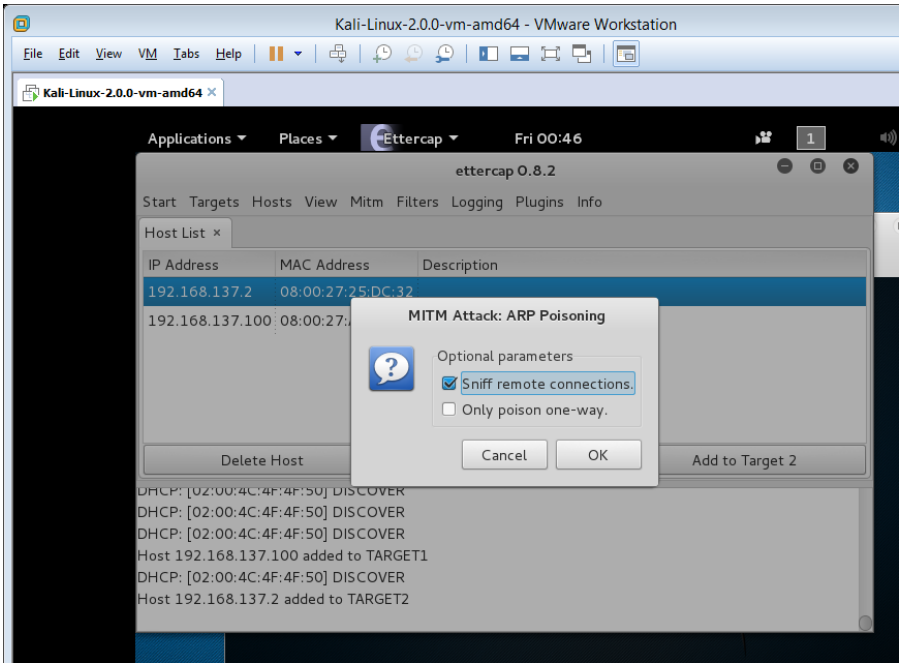


Figura 81 Activación del sniffer remoto

Fuente: herramienta Kali-linux

Activación de sniffing para realizar el envenemaniento de la red como indica la figura 82

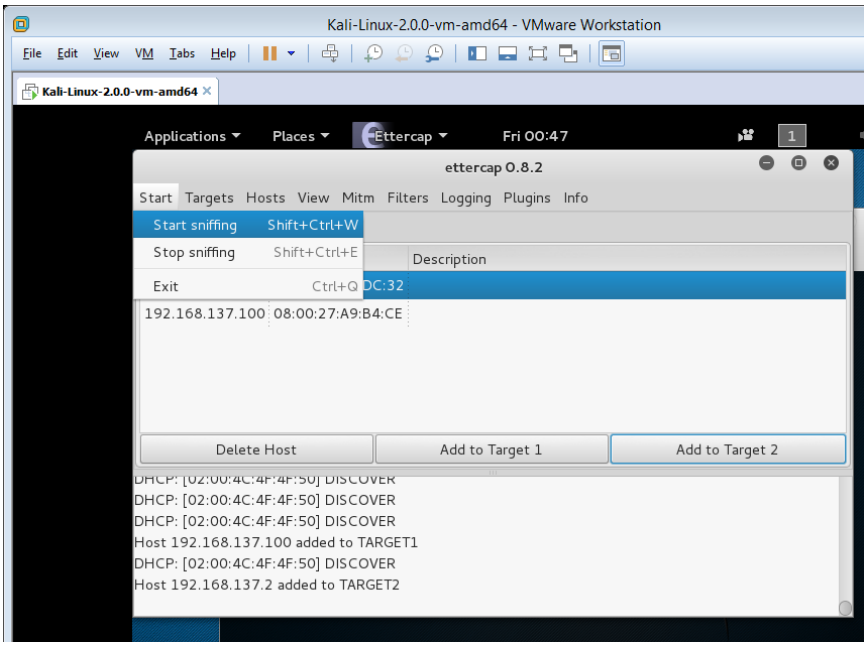


Figura 82 Activación del envenenamiento

Fuente: herramienta Kali-linux

Activación de driftnet modo escucha para la interface que se procede a escuchar como indica la figura 83

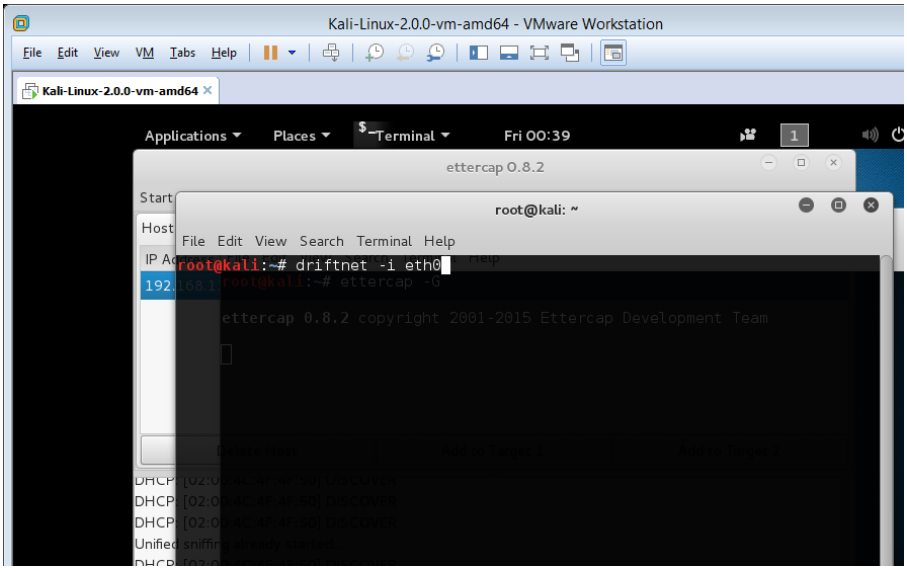


Figura 83 Activación de drifnet para la interfaz

Fuente: herramienta Kali-linux

Prueba de bloqueo por Snort de MITM (hombre en el medio) usando ettercap y Driftnet como indican las figuras 84 y 85, donde se evidencias las alertas que han sido generadas a través de Snort IPS desde el Firewall Pfsense donde no ha sido posible el ataque de envenenamiento.

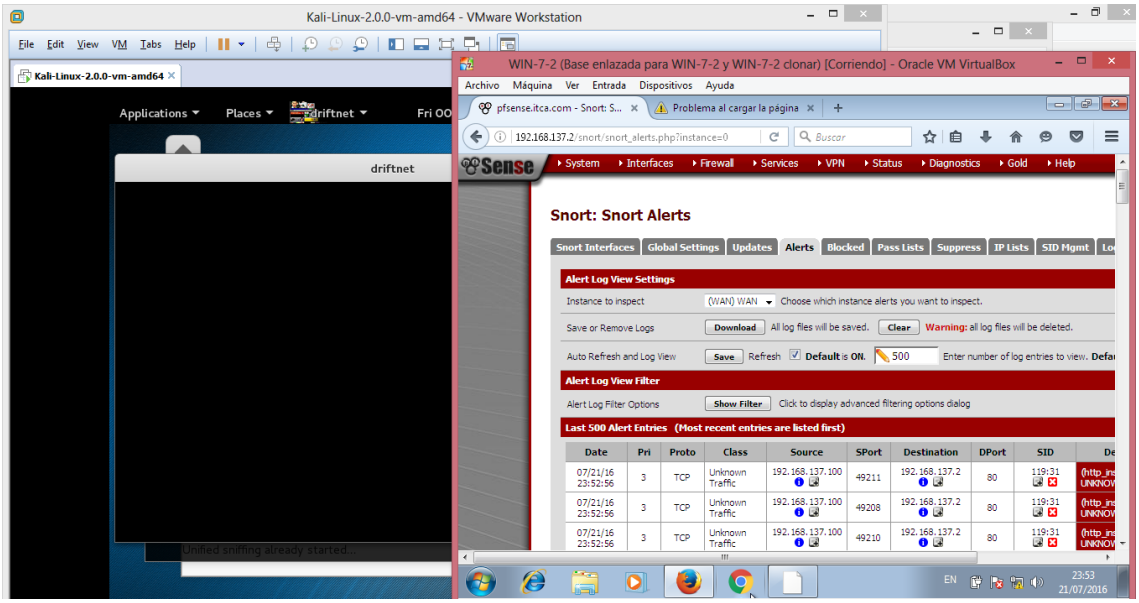


Figura 84 . Alertas generadas por Snort donde no ha sido posible el envenenamiento

Fuente: herramienta Kali-linux

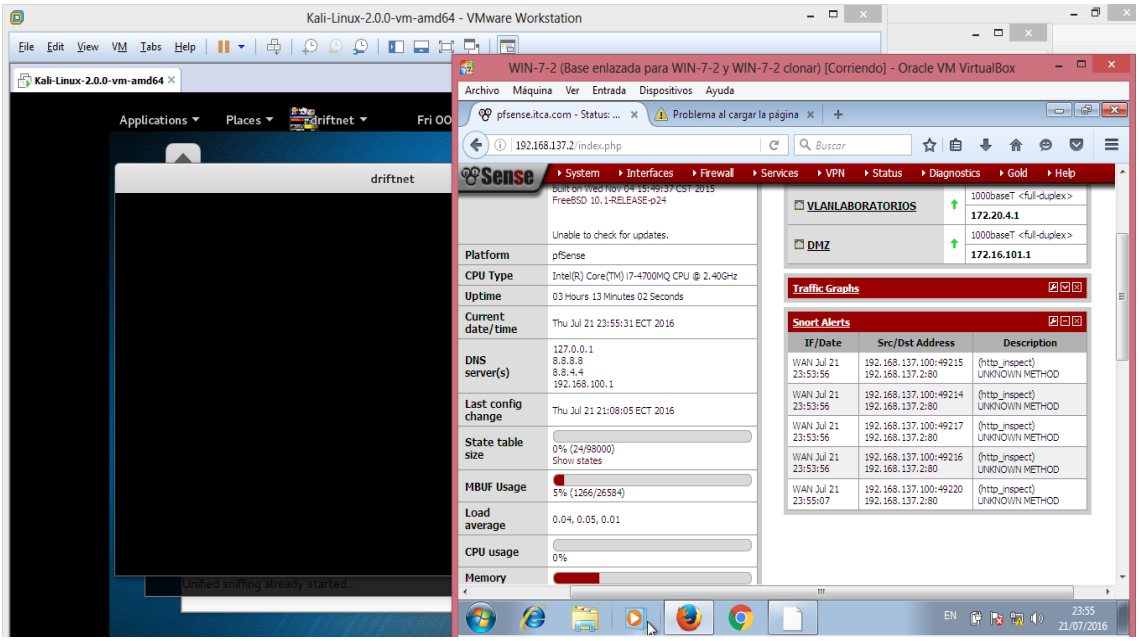


Figura 85 Resumen de Snort donde no ha sido posible el envenenamiento

Fuente: herramienta Kali-linux

6.2.1 Ataque de DoS (denegación de servicios)

La denegación de servicios tiene como objetivo imposibilitar el acceso a los servicios y recursos durante un tiempo estimado, y puede afectar a los servidores conectados a la red, no afecta los datos, sino más bien dañar la reputación e impedir el desarrollo normal de las

Para el desarrollo de esta prueba se utiliza “slowloris” que es un scrip realizado en código C++ ya existente donde se realizan miles de peticiones al servidor web de forma concurrente. Así se fuerza a mantener las conexiones abiertas las solicitudes donde el servidor llega a su límite.

Ingresar al directorio donde se encuentra el archivo con el cual enviara una gran cantidad de paquetes para cumplir con el propósito como indica la figura 87.

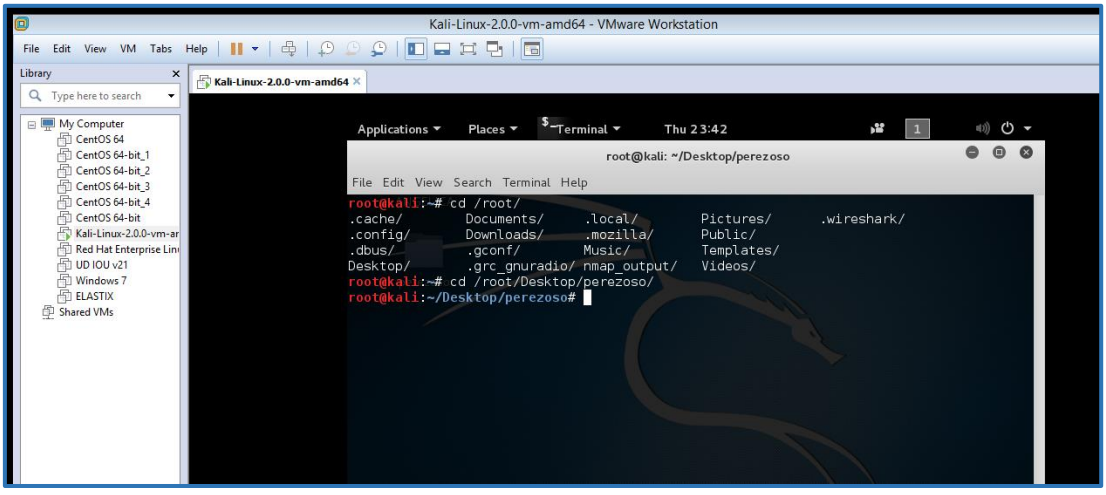


Figura 86 . Selección del archivo slowloris para realizar el ataque

Fuente: herramienta Kali-linux

A continuación se digita el comando con el cual se inicia el atque de DoS como indica la figura 88.

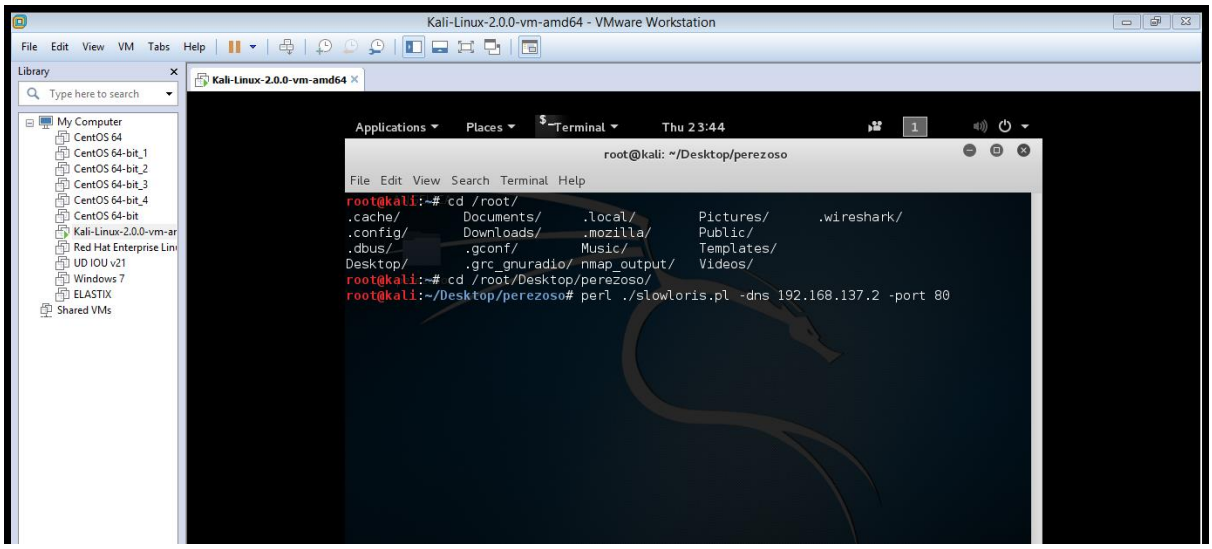


Figura 87 se inicializa el envio de peticiones mediante slowloris

Fuente: herramienta Kali-linux

Se envían las paquetes mediante slowloris hacia el firewall Pfense como indica la figura 88 y 89

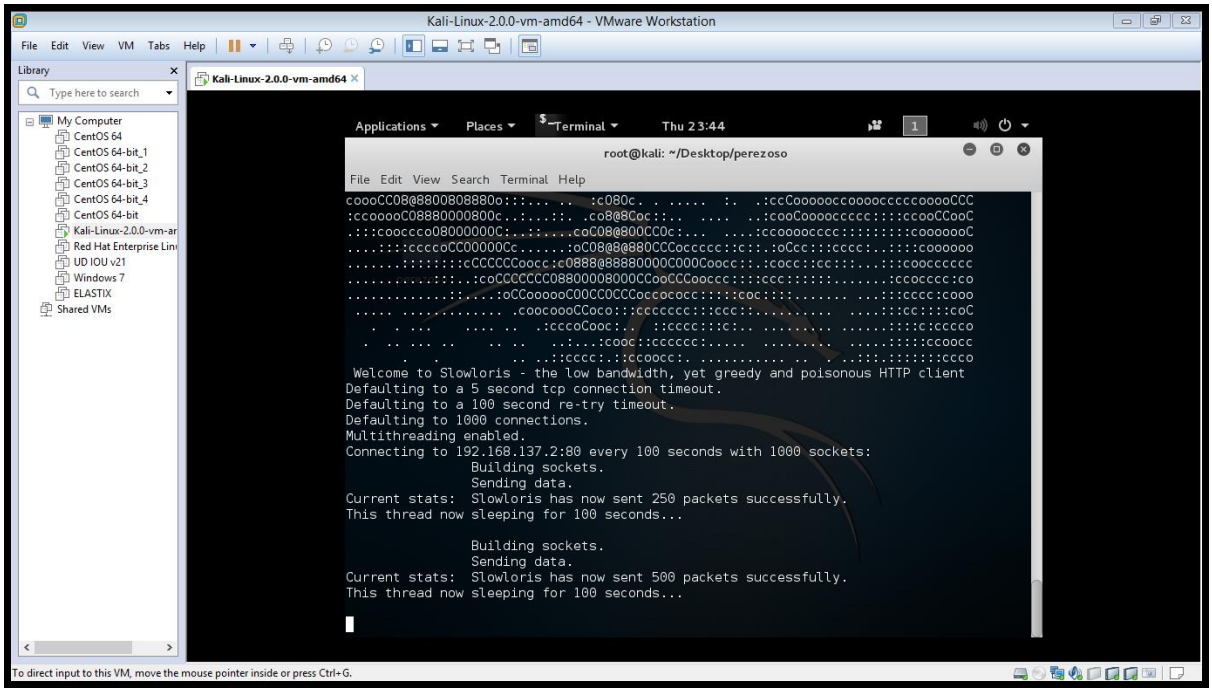


Figura 88 Envio de paquetes mediante slowloris

Fuente: herramienta Kali-linux

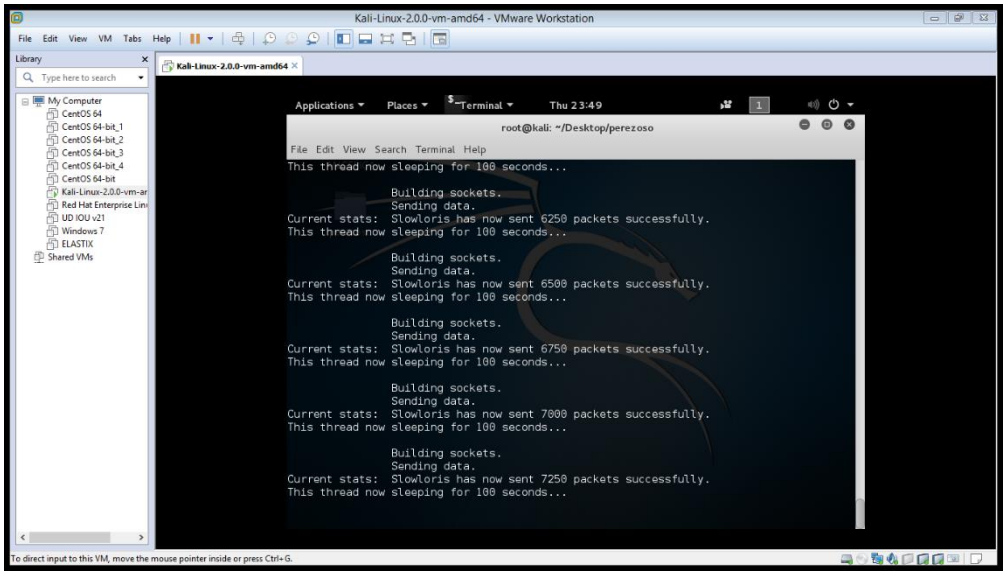


Figura 89 Envio de paquetes mediante slowloris

Fuente: herramienta Kali-linux

Se puede visualizar las aletas generadas por el ataque, mediante Snort IPS, así mismo se evita que este ataque surja efecto, esto se comprueba porque el servicio aun es accesible para el firewall como indican las figuras 90, 91 y 92

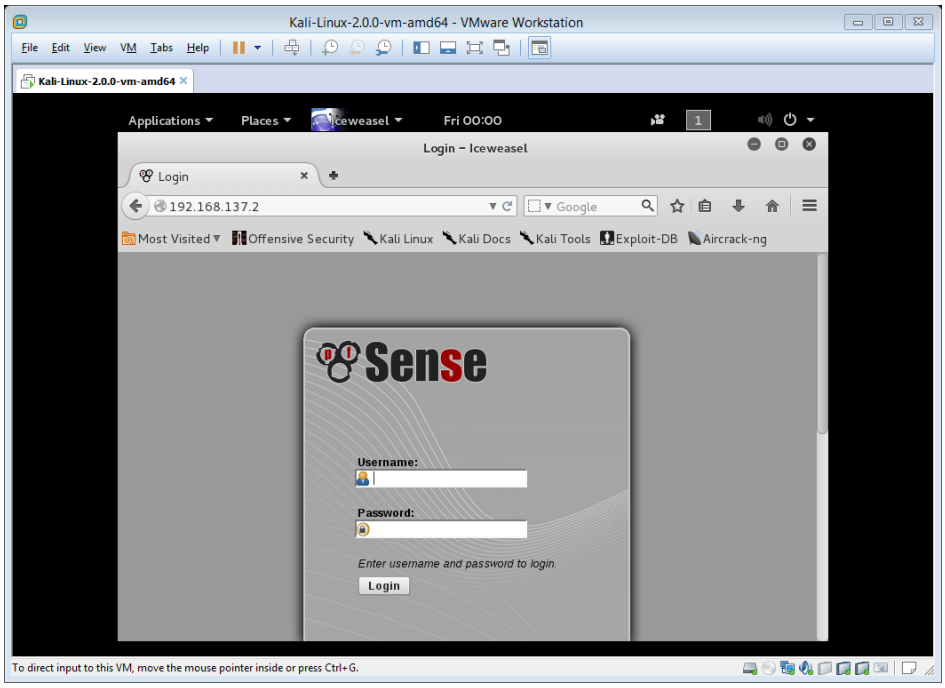


Figura 90 Firewall Pfsense es accesible después del ataque

Fuente: herramienta Kali-linux

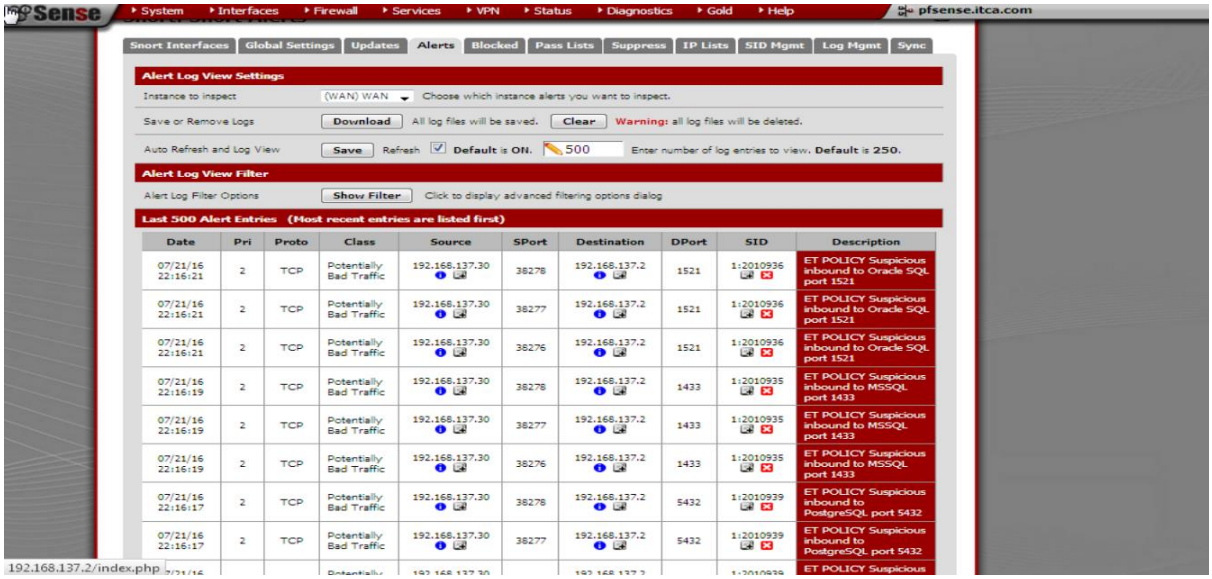


Figura 91 Alertas generadas por Snort IPS

Fuente: herramienta Kali-linux

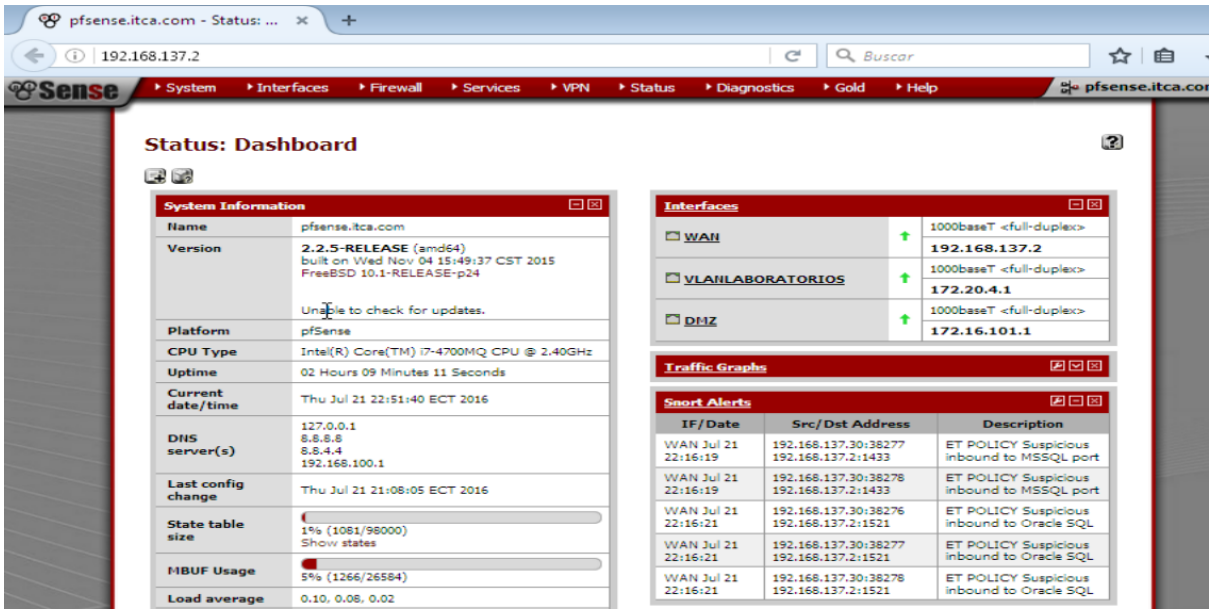


Figura 92 Resumen de las alertas generadas por el ataque DOS

Fuente: herramienta Kali-linux

CAPÍTULO VII

7 Conclusiones y recomendaciones

En este capítulo se realiza el análisis de costo beneficio entre los equipos existentes y los de la propuesta necesaria para la implementación real, para el sistema de seguridad perimetral. Y finalmente las conclusiones y recomendaciones este proyecto de titulación.

7.1 Análisis económico

Se realiza un análisis económico de los elementos utilizados en la implementación del Sistema de Seguridad Perimetral, en comparación con los equipos que la red del tecnológico ITCA, debe tener como infraestructura necesaria para la implementación real con una solución propietaria.

7.1.1 Presupuesto de software y hardware existente.

La tabla 46 se detallan los equipos de Networking con los que actualmente está diseñada la red del tecnológico ITCA, este presupuesto se ha dado para la implementación del sistema de seguridad perimetral.

Tabla 43. Costo de la infraestructura existente en el tecnológico ITCA

ITEM	Concepto	Cantidad	Precio Unitario	Precio total
1	Switch 2950 capa 3	1	$ 500,00	$ 500,00
2	Switch SG200-26	8	$ 200,00	$ 1.600,00
3	Switch SG300-28	9	$ 250,00	$ 2.250,00
4	CPU Intel core i7	1	$ 550,00	$ 550,00
5	Tarjetas Ethernet	2	$ 45,00	$ 90,00
6	Teclado	1	$ 30,00	$ 30,00
7	Pantalla	1	$ 120,00	$ 120,00
8	mouse	1	$ 20,00	$ 20,00
10	Software Pfsense	1	$ 0,00	$ 0,00
	Total			**$ 5.160,00**

Fuente: cotización de empresas para soluciones de Networking

7.1.2 Detalle del costo de los equipos de Networking necesarios para la implementación

De acuerdo al desarrollo del diseño de la seguridad perimetral, se evidencia que la infraestructura para la implementación de debe ser de una capacidad más robusta en cuanto al equipamiento de Networking, la tabla 46, muestra una comparación de los estos equipos necesarios para que pueda soportar todo el tráfico de la red.

Tabla 44. Comparación de los servidores HP Proliant .

Servidores HP Proliant de Bastidor				
N	Característica	DL320e Gen8 v2	DL360p Gen8	**DL380p Gen8**
1	Diseño Físico			
2	Procesador	Xeon E3 - 1200v3 Intel Pentium Intel Core i3	Xeon E5-2600v2	Xeon E5-2600v2 Xeon E5-2600
3	# de Procesadores	1	1 - 2	1 - 2
4	Núcleo procesador disponible	4 - 2	12 - 10 - 8 – 4	12 - 10 - 8 - 6 - 4 - 2
5	Memoria Máxima	32 GB	768 GB	768bGB
6	Ranuras de memoria	4 DIMM (máx.)	24 DIMM (máx.)	24 DIMM (máx.)
7	Descripción de unidad	2 SAS/SATA/SSD grandes 4 SAS/SATA/SSD pequeños	4 SAS/SATA/SSD grandes 10SAS/SATA/SSD pequeños 8 SAS/SATA/SSD pequeños	4 SAS/SATA/SSD grandes 10 SAS/SATA/SSD pequeños 8 SAS/SATA/SSD pequeños
8	Controladora de red	Adaptador Ethernet de 1 GB 2 puertos por controlador	Adaptador Ethernet de 1 GB 4 puertos por controlador o Adaptador Ethernet de 10 GB 2 puertos por controlador.	Adaptador Ethernet de 1 GB 4 puertos por controlador o Adaptador Ethernet de 10 GB 2 puertos por controlador.
9	Form Factor	1U	1U	2U
	Costo	$ 1.050,00	$ 1.388,00	$ 1.471,00

Fuente: cotización de empresas para soluciones de Networking

7.1.3 Detalle de las herramientas para la instalación

La tabla 47 muestra algunas de las herramientas requeridas para realizar el equipamiento necesario de infraestructura de la red de datos.

Tabla 45 herramientas necesarias para la instalación de infraestructura

Herramientas	Cantidad	Descripción	Costo unitario	Costo Total
Rollo de cable	1	Cable UTP categoría 6a	$ 220,00	$ 220,00
Conectores RJ45	1	Funda de 100 unidades cat 6	$ 34,00	$ 34,00
Adaptadores de red	1	Tarjeta de red gigabit Ethernet 10/100/1000 Mbps PCI EXPRESS x1 HP	$ 106,00	$ 106,00
Kit de Instalación	1	Ponchadora + Crimpeadora + Peladora	$ 55,00	$ 55,00
Total				**$ 415,00**

Fuente: cotización de empresas para soluciones de Networking

7.1.4 Detalle del costo de ingeniería e instalación

Para la instalación del equipamiento es necesario contratar una empresa encargada la tabla 48 muestra en resumen el costo estimado.

Tabla 46 costo estimado de ingeniería e instalación

Detalle	Horas	Costo/horas	Costo Total
Costo de Implantación	15	$ 50,00	$ 750,00
Costo de capacitación al personal	4	$ 20,00	$ 80,00
Total			**$ 830,00**

Fuente: cotización de empresas para soluciones de Networking

7.1.5 Detalle del costo total estimado

Para realizar el cálculo del costo total se toman en cuenta los valores de costo de equipos de Networking elegido, costo de herramienta necesaria, costo de instalación, véase en la tabla 49.

Tabla 47 detalle total del costo estimado

Descripción de Costos	Costo Total
Costo equipos de Networking servidor HP Proliant DL380p Gen8	1.471,00
Costo herramientas de instalación	$ 415,00
Costo ingeniería e instalación	$ 830,00
Costos del software	$ 0,00
Costo Total Estimado	**$ 2716,00**

Fuente: cotización de empresas para soluciones de Networking

7.1.6 Presupuesto de software y hardware existente.

7.1.7 Costo beneficio

Este cálculo se obtiene del análisis sobre el costo, beneficio del proyecto reflejando, así la factibilidad de la implementación del proyecto, lo que debe tender a ser igual o mayor a uno para confirmar que es viable o no.

7.1.8 Cálculo del costo-beneficio

Para esta relación matemática se toman los valores totales del presupuesto de software y hardware existentes, sobre el costo total estimado del proyecto, como establece la fórmula.

Donde:

- Beneficio: Presupuesto de software y hardware existente (1471,00USD)
- Costo: Costo total estimado. (2716,00USD)

- Si el resultado es igual o mayor a 1, el proyecto es aceptable, positivo o factible.
- Si el resultado es menor a 1, el proyecto es rechazado o negativo.

$$\frac{\text{Beneficio}}{Costo} = X \qquad \frac{2716{,}00\ USD}{1471{,}00\ USD} = 1{,}83$$

Ecuación 2. Fórmula del análisis costo beneficio

Fuente: Blank, Leland (2006). Ingeniería Económica. McGrawHill. México

Se finiquita que el proyecto es viable de ser aplicable, de acuerdo al análisis costo beneficio X = 1.8.

7.2 Conclusiones

Al culminar el proyecto de titulación se obtiene las siguientes conclusiones:

- La base teórica es de suma importancia para la realización del proyecto, se requiere la información suficiente sobre cuáles son las principales características de un Sistema de Seguridad Perimetral, de esta manera tener una idea clara de los procesos que se van a seguir para realizar un correcto diseño y finalmente la implementación del mismo de ser el caso requerido.

- El levantamiento de la información de la situación actual dela red del Tecnológico ITCA

  Permite conocer a fondo toda la infraestructura existente tanto lógica como física, esta es una parte importante aquí se evidencia los activos de la red, permite verificar y dimensionar de la red y clasificar los activos que van a ser evaluados en el riesgo.

- En el estudio de la norma de evaluación del riesgo se utiliza la Guía del Instituto Nacional de Estándares y Tecnología NIST SP 800-30, con el fin de conocer los niveles actuales de seguridad de la información e identificar tanto amenazas y vulnerabilidades en la red de datos del Tecnológico ITCA, esta evaluación permite realizar un control del nivel del riesgo, y poder realizar el mejoramiento continuo de los sistemas.

- La gestión y evaluación de riesgos conlleva un esfuerzo adicional de los propietarios o administradores de la red ya que están definidos procesos específicos que deben seguirse en conjunto, y no es una actividad sencilla además los resultados se lo ven a largo plazo, por lo tanto se requiere de un alto compromiso de todo los involucrados dentro de la institución, para llevar a cabo la evaluación de riesgos y la implantación de controles.

- El estudio de la norma de evaluación del riesgo permite evidenciar las falencias de la red de datos del Tecnológico ITCA y permite verificar y concluir que no se ha implementado ningún sistema de seguridad perimetral, es una red plana es decir no está definido un modelo jerárquico. En cualquier momento la red puede ser blanco de un ataque informático esto puede ocasionar pérdida parcial o total de la información, costo económicos y más problemas que esta clase de ataques pueda desencadenar.

- Según las recomendaciones y conclusiones de la guía de evaluación del riesgo permite plantear el diseño del sistema de seguridad perimetral, para ello se divide la red en tres zonas específicas la red LAN, la red DMZ y la red WAN. Además de realizar la segmentación lógica de la red, esto permite separar a los usuarios por la naturaleza de servicios a los que necesitan acceder dentro de la institución.

- Se desarrolla la implementación del firewall Pfsense en la red Real del Tecnológico ITCA, donde se ha realizado configuración de los equipos necesarios en este caso el Swtich de core , además se realiza la segmentación lógica de la red, con la creación de 16 Vlans que se ha clasificado de acuerdo a

los requerimientos del administrador de red al mismo tiempo se realiza la configuración de proxy Squid para incrementar la rapidez de acceso a los servidores , y finalmente el Sistema de Prevención de Intrusos IPS en este caso Snort que en paquete incluido en el software Pfsense.

- En el presente trabajo de titulación se permitió unificar dos métodos de seguridad informática basados en software libre como son los Firewall y los IPS mediante Firewall Pfsense y Snort respectivamente, para el monitoreo y detección de ataques a la red de datos del tecnológico ITCA

- El desarrollo del análisis costo beneficio permite tener un precedente tanto de la infraestructura actual y de la necesaria tanto con su costo real para desarrollar el plan de puesta en marcha del sistema de seguridad perimetral para la red de datos del tecnológico ITCA

7.3 Recomendaciones

Al culminar el proyecto de titulación se menciona las siguientes Recomendaciones:

- Para mejorar la estructura física y lógica de la red se recomienda realizar el modelo de red jerárquico contemplando el manejo de sus 3 capas: núcleo, distribución y acceso.

- En la actualidad las empresas o instituciones aún no tienen conciencia de la importancia de la implantación de una adecuada evaluación y gestión de los riesgos en los sistemas de información, la misma que va de la mano de una excelente toma de decisiones, se solicita tomar las medidas y acciones necesarias para llevar a cabo el plan de recuperación ante un ataque informático.

- En la infraestructura de red del Tecnológico ITCA, donde se evidencia que los equipos de red no posee con la capacidad necesaria para dejar el sistema de seguridad perimetral en marcha puesto que al realizar aquello la red colapsaría y se recomienda como solución viable la adquisición del equipamiento necesario de Networking para la implementación del firewall de hardware.

- Es recomendable establecer un plan de contingencia ante los riesgos, se debe tener en cuenta la importancia de respaldar las bases de datos, configuraciones esenciales, información confidencial de los dispositivos y la capacidad de recuperase en el menor tiempo posible de un ataque.

- El diseño del firewall Pfsense así como todas las configuraciones necesarias son viables para cuando la institución desee continuar con el proceso de implementación total.

- Cabe mencionar que el uso de software libre en instituciones públicas o privadas se ha convertido en un factor fundamental en la gestión, administración y seguridad de las redes de información, debido a que consume menos recursos de memoria, procesador y espacio en los equipos de red, permitiendo la reutilización de recursos y por ende disminución de gastos económicos que al utilizar un software propietario.

7.4 **Bibliografía**

Baltazar José, Campuzano Juan. (2011). *Diseño e Implemantación de un esquema de Seguridad Perimetral para redes de datos.* México, D.F: Universidad Autónoma de México.

educativo, P. (2014). *tiposde.org*. Obtenido de http://www.tiposde.org/informatica/131-tipos-de-servidores/

ITCA. (abril de 2015). *Instituti Tecnologico José Chiribiga Grijalva.* Obtenido de http://portalins.tecnologicoitca.edu.ec

MAYORGA, D. (2008). *ANALISIS,DISEÑO E IMPLEMTACIÓN DEL ESQUEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA UISEK-ECUADOR (CAMPUS MIGUEL DE CERVANTES).* QUITO.

Microsoft Develoer network. (2005). MSDN Library. *Microsoft develoer network.*

MOLINA, E. (2012). *PROPUESTA DE SEGMENTACIÓN DE REDES VIRTUALES Y PRIORIZACIÓN DEL ANCHO DE BANDA CON QoS PARA LA MEJORA DEL RENDIMIENTO Y SEGURIDA DE LA RED LAN EN LA EMPRESA EDITORA EL COMERCIO PLATA NORTE.* Chiclayo.

Sanchez, J. (2012). *Instalación de un router/Appliance con funciones de firewall, VPN,potección de ataques,antiespam y antivirus perimetral con IpCop.* Colombia: Universidad de Caldas, Manizales, Colombia.

TORRES, R. J. (2014). *SEGURIDAD PERIMETRAL EN LA RED DE DISTRIBUCIÓN DE LA UNIVERSIDAD TECNICA DEL NORTE.* Ibarra.

ZAPATA. (s.f.).

Zapata, R. D. (2012). *Estudio de las técnicas de control de acceso a internet y su aplicación en la red de datos del colegio corina parral de la ciudad de Chimbo.* RIOBAMBA: Universidad Superior Politecnica de Chimborazo.

TESIS

Alulema Chiluisa, D. (2008). Estudio y diseño de un sistema de seguridad perimetral para la red Quito Motors, utilizando tecnología UTM (Unified Threat Management). (Tesis inédita de Ingeniería). Escuela Politécnica Nacional, Quito, ECU.

Astudillo Herrera, J & Jiménez Macías, A. & Ortiz Flores, F. (2011). Adaptación del IDS/IPS Suricata para que se pueda convertir en una solución empresarial. (Tesis inédita de Ingeniería). Escuela Superior Politécnica del Litoral, Guayaquil, ECU.

Vinueza Jaramillo, T. (2012). Honeynet virtual híbrida en el entorno de red de la Universidad Técnica del Norte de la ciudad de Ibarra. (Tesis inédita de Ingeniería). Disponible en el repositorio digital de la Universidad Técnica del Norte, Ibarra, ECU.

MICHILENA, M. A. (2013). METODOLOGÍA DE SEGURIDAD INFORMÁTICA CON BASE EN LA NORMA ISO 27002 Y EN HERRAMIENTAS DE PREVENCIÓN DE INTRUSOS PARA LA RED ADMINISTRATIVA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA. Ibarra

LIBROS

PRESSMAN, S. Rogger; (2002). Ingeniería de Software. Quinta Edición. España. Mc-GRAW-HILL/Interamericana de España

SOMMERVILLE, Ian; (2002). Ingeniería de Software. Sexta Edición. México. Pearson Educación.

SOM, Cerezo Guillermo; (2002). Manual Imprescindible Visual Basic .NET. Primera Edición. España. Anaya Multimedia S.A

BALENA, Francesco; (2003). Programación Avanzada con Microsoft VISUAL BASIC .NET. Primera Edición. España. McGRAW-HILL/Interamericana de España.

ROBINSON, Ed. James; BOND, Michael; (2003). Seguridad para Microsoft Visual

Basic .NET, Primera Edición. España. McGRAW-HILL/Interamericana de España.

BOTT, Ed. Siechert; (2003). Seguridad en Microsoft Windows XP. Primera Edición. España. McGRAW-HILL/Interamericana de España.

GRATTON, Pierre; (1998). Protección Informática. Primera Edición. México. Editorial Trillas, S.A de C.V.

GROFF, James R; WEINBERG, Paul N; (1991). Aplique SQL. Primera Edición. México. McGRAW-HILL/Interamericana de México.

ANEXOS

ANEXO 1

IDENTIFICACION DE LOS USUARIOS DEL TECNOLOGICO ITCA

172.20.3.10	JORGE ACOSTA
172.20.3.11	JOSE LUIS
172.20.3.12	JUAN JARAMILLO
172.20.3.13	HUGO NARVAEZ
172.20.3.14	FER SANCHEZ
172.20.3.15	LAP JORGE
172.20.3.16	LAP JOSE
172.20.3.17	LAP JUAN
172.20.3.18	LAP HUGO
172.20.3.19	LAP FER
172.20.3.20	Henry
172.20.3.21	Reloj de huellas
172.20.3.22	lap henry
172.20.3.23	
172.20.3.24	
172.20.3.25	
172.20.3.26	
172.20.3.27	Impresora
172.20.3.28	
172.20.3.29	Impresora

INF	
172.20.3.71	Henry Guachagmira
172.20.3.72	JEANETH CALDERON
172.20.3.73	FER SANCHEZ
172.20.3.74	FREDY NARANJO
172.20.3.75	N/A
172.20.3.76	David
172.20.3.77	
172.20.3.78	
172.20.3.79	
172.20.3.80	

VINCULACION	
172.20.3.111	ERNESTO MOROCHO
172.20.3.112	Impresora
172.20.3.113	FERNANDO CARRERA
172.20.3.114	
172.20.3.115	
172.20.3.116	
172.20.3.117	
172.20.3.118	
172.20.3.119	
172.20.3.120	

ADE	
172.20.3.41	LILIANA TAPIA
172.20.3.42	FLOR RODRIGUEZ
172.20.3.43	JORGE SUAREZ
172.20.3.44	MIKAELA POSSO
172.20.3.45	GUIDO GUERRERO
172.20.3.46	MANUEL HIDALGO
172.20.3.47	
172.20.3.48	BAYARDO SALAZAR
172.20.3.49	JORGE SUAREZ
172.20.3.50	JORGE SUAREZ

DMP	
172.20.3.61	GABRIELA BARAHONA
172.20.3.62	JOSE DIAZ
172.20.3.63	MANUEL MOROCHO
172.20.3.64	
172.20.3.65	IMPRESORA
172.20.3.66	
172.20.3.67	TALLER DE MODA
172.20.3.68	ROUTER TRENDNET
172.20.3.69	
172.20.3.70	

CONTABILIDAD	
172.20.3.121	TATIANA ZAMBRANO 1
172.20.3.122	TATIANA ZAMBRANO 2
172.20.3.123	FERNANDA ORTEGA
172.20.3.124	
172.20.3.125	
172.20.3.126	
172.20.3.127	
172.20.3.128	
172.20.3.129	
172.20.3.130	Impresora RICOH

RECTORADO	
172.20.3.131	ALICIA SOTO
172.20.3.132	NURIA GALARRAGA
172.20.3.133	MARIA FERNANDA
172.20.3.134	FRANCISCO DELGADO LAP
172.20.3.135	ALEXIS PEREZ
172.20.3.136	FRANCISCO DELGADO
172.20.3.137	
172.20.3.138	
172.20.3.139	
172.20.3.140	IMPRESORA RICOH

FACTURACION	
172.20.3.141	FERNANDA ORTEGA
172.20.3.142	JESSY
172.20.3.143	
172.20.3.144	
172.20.x.x	PC1COUNTER
172.20.x.x	PC2COUNTER
172.20.x.x	Cacmu
172.20.3.148	
172.20.3.149	
172.20.3.150	172.20.3.150

INVESTIGACION	
172.20.3.181	JUAN CARLOS PINEDA
172.20.3.182	BYRON ALBAN
172.20.3.183	Juan Carlos Pineda lap
172.20.3.184	RAMIRO SOTO
172.20.3.185	Ramiro soto
172.20.3.186	
172.20.3.187	
172.20.3.188	
172.20.3.189	
172.20.3.190	

DIN	
172.20.3.31	Marcelo Paucar
172.20.3.32	Verónica Diaz
172.20.3.33	N/A
172.20.3.34	LORENA JUMA
172.20.3.35	MARIO MONTALVO
172.20.3.36	
172.20.3.37	
172.20.3.38	
172.20.3.39	AP-docentes aula 215
172.20.3.40	IMPRESORA

RRHH	
172.20.3.151	CARLA JARAMILLO
172.20.3.152	NANCY CIFUENTES
172.20.3.153	Tania Figueroa
172.20.3.154	AUDITOR
172.20.3.155	
172.20.3.156	
172.20.3.157	
172.20.3.158	
172.20.3.159	
172.20.3.160	IMPRESORA RICOH

GTG	
172.20.3.51	ROBERTO PORTILLA
172.20.3.52	NATALIA ALOMOTO
172.20.3.53	RONNY SORIANO
172.20.3.54	LAP RONNY
172.20.3.55	
172.20.3.56	
172.20.3.57	
172.20.3.58	
172.20.3.59	
172.20.3.60	IMPRESORA RICOH

INGLES	
172.20.3.81	GEOCONDA CALDERON
172.20.3.82	N/A
172.20.3.83	VACA GERMAN
172.20.3.84	
172.20.3.85	Geoconda Portatil
172.20.3.86	
172.20.3.87	
172.20.3.88	
172.20.3.89	
172.20.3.90	Impresora

DIN	
172.20.3.31	Marcelo Paucar
172.20.3.32	Verónica Diaz
172.20.3.33	N/A
172.20.3.34	LORENA JUMA
172.20.3.35	MARIO MONTALVO
172.20.3.36	
172.20.3.37	
172.20.3.38	
172.20.3.39	AP-docentes aula 215
172.20.3.40	IMPRESORA

EVALUACION	
172.20.3.171	EDISON RODRIGUEZ
172.20.3.172	
172.20.3.173	
172.20.3.174	MARIA DEL CARMEN ESTEVEZ
172.20.3.175	
172.20.3.176	Natali Roman
172.20.3.177	
172.20.3.178	
172.20.3.179	IMPRESORA RICOH MP C3000
172.20.3.180	IMPRESORA

INGLES	
172.20.3.81	GEOCONDA CALDERON
172.20.3.82	N/A
172.20.3.83	VACA GERMAN
172.20.3.84	
172.20.3.85	Geoconda Portatil
172.20.3.86	
172.20.3.87	
172.20.3.88	
172.20.3.89	
172.20.3.90	Impresora

INVESTIGACION	
172.20.3.181	JUAN CARLOS PINEDA
172.20.3.182	BYRON ALBAN
172.20.3.183	Juan Carlos Pineda lap
172.20.3.184	RAMIRO SOTO
172.20.3.185	Ramiro soto
172.20.3.186	
172.20.3.187	
172.20.3.188	
172.20.3.189	
172.20.3.190	

UBI	
172.20.3.101	SANDRA LUNA
172.20.3.102	MONICA GOMEZ
172.20.3.103	
172.20.3.104	
172.20.3.105	
172.20.3.106	
172.20.3.107	
172.20.3.108	
172.20.3.109	IMPRESORA RICOH MP C4000
172.20.3.110	IMPRESORA

ANEXO 2

DISTRIBUCION DE LAS VLANS EN L TENOLOGICO ITCA

#	SWITCH	IP	PUERTO IINCIO	PUERTO FIN
1	CISCO SG200 26 PUERTOS	172.20.0.5	P1D49	D72
2	CISCO SG200 26 PUERTOS	172.20.0.6	P1D25	D48
3	CISCO SG300 28 PUERTOS	172.20.0.7	PB-D01	D24
4	CISCO SG300 28 PUERTOS	172.20.0.8	D25	D48
5	CISCO SG300 28 PUERTOS	172.20.0.9	D49	D72
6	CISCO SG300 28 PUERTOS	172.20.0.10	D73	D96
7	CISCO SG500 28 PUERTOS	172.20.0.11	D97	D120
8	CISCO SG200 26 PUERTOS	172.20.0.12	D121	D144
9	CISCO SG200 26 PUERTOS	172.20.0.13	A1--01	A2--02
10	CISCO SG200 26 PUERTOS	172.20.0.14	A2--03	A3--04
11	CISCO SG200 26 PUERTOS	172.20.0.15	A3--05	A4--06
12	CISCO SG200 26 PUERTOS	172.20.0.16	A4--07	A5--08
13	ADVANTEK NETWORK 24 PUERTOS - UTILIZADOS 14	172.20.0.17	A5--09	A5--22

SWICTH	PLANTA	PUERTO	HOST	DEPARTAMENTO	RESPONSABLE
8	PB	D121	PC	INFORMATICA	ING. HUGO NARVAEZ
8	PB	D122	TELEFONO, PC	INFORMATICA	ING. HUGO NARVAEZ
8	PB	D119	-	INFORMATICA	SIN CONEXIÓN
8	PB	D120	-	INFORMATICA	SIN CONEXIÓN
7	PB	D118	ROUTER	INFORMATICA	-
7	PB	D117	-	INFORMATICA	SIN CONEXIÓN
7	PB	D116	-	INFORMATICA	SIN CONEXIÓN
7	PB	D114	-	INFORMATICA	SIN CONEXIÓN
7	PB	D115	IMPRESORA	INFORMATICA	SIN CONEXIÓN
7	PB	D112	TELEFONO, PC	INFORMATICA	ING FERNANDA SANCHEZ
7	PB	D113	-	INFORMATICA	ING FERNANDA SANCHEZ
8	PB	D124	-	INFORMATICA	-
8	PB	D123	-	INFORMATICA	-

8	PB	D139	PC	SISTEMAS	ING. JUA CARLOS JARAMILLO
8	PB	D138	-	SISTEMAS	ING. JUA CARLOS JARAMILLO
8	PB	D144	PC	SISTEMAS	ING.JOSE LUIS RODRIGUEZ
13	PB	A_523	-	SISTEMAS	ING.JOSE LUIS RODRIGUEZ
8	PB	D142	PC	SISTEMAS	ING. HENRI GUACHIMIR
8	PB	D143	IMPRESORA	SISTEMAS	ING. HENRI GUACHIMIR
4	PB	D140	-	SISTEMAS	ING. JORGE ACOSTA
4	PB	D141	TELEFONO, PC	SISTEMAS	ING. JORGE ACOSTA
6	PB	D88	PC	SECRETARIADO EJECUTIVO	LORENA PERUGACHI
6	PB	D89	PC	SECRETARIADO EJECUTIVO	PILAR TATES
6	PB	D90	-	SECRETARIADO EJECUTIVO	-
6	PB	D91	-	SECRETARIADO EJECUTIVO	-

6	PB	D93	PC	GESTION TURISTICA	NATALY ALIMOTO
6	PB	D94	PC	GESTION TURISTICA	ING. MONICA ANDRADE
6	PB	D95	PC	GESTION TURISTICA	ING RONI
6	PB	D96	-	-	-
7	PB	D97	TELEFONO, PC	GESTION TURISTICA	ING. ROBERTO PORTILLA
7	PB	D102	PC	GESTION TURISTICA	RUBEMN HERNANDEZ
7	PB	D98	IMPRESORA	GESTION TURISTICA	-
7	PB	D99	PC	MERCADOTECNIA	JORGE SUAREZ
7	PB	D101	PC	ADMINISTRACION Y MERCADOTECNIA	ING. FLOR ALBA
7	PB	D104	PC	MERCADOTECNIA	JORGE SUAREZ
7	PB	D105	-	ADMINISTRACION	-
7	PB	D106	PC	ADMINISTRACION	DOC. SANDRA MORA
7	PB	D107	PC	ADMINISTRACION	MAG. ISABEL MORILLO
7	PB	D108	PC	ADMINISTRACION	GUIDO GUERRERO

3	PB	D01	IMPRESORA	GOLDEN	-
3	PB	D02	PC	GOLDEN	TANIA FIGUEROA
3	PB	D04	TELEFONO, PC	GOLDEN	MG. YOCONDA
3	PB	D03	-	GOLDEN	-
3	PB	D05	-	GOLDEN	-
3	PB	D06	PC	GOLDEN	TEACHERS
3	PB	D07	-	GOLDEN	-
3	PB	D08	-	GOLDEN	-

12	PA1	D23			
13	PA1	D33	PC,TELEFONO	Direccion Académica	ALEXIS PEREZ
14	PA1	D37	PC,TELEFONO	Rectorado	SECRETARIA AUTORIDADES
15	PA1	D42			
16	PA1	D44		Aula 2015	AP CISCO DOCENTES
17	PA1	D46	PC	Aula 2016	EDISON RODRIGUEZ
18	PA1	D27	PC,TELEFONO	Rectorado	FRANCISCO DELGADO
19	PA1	D14			
20	PA1	D16			
21	PA1	D18			
22	PA1	D20			
23	PA1	D22	PC,TELEFONO	Vicerrectorado	DR. ALICIA SOTO

ANEXO 3

CONFIGURACIÓN BÁSICA DEL SWITCH CORE

```
ESW1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
ESW1(config)#hostname SW-ITCA-CORE
SW-ITCA-CORE(config)#banner motd "ITCA BIENVENIDOS"
SW-ITCA-CORE(config)#ip domain-name tecnologicoitca.edu.ec
SW-ITCA-CORE(config)#crypto key generate rsa
The name for the keys will be: SW-ITCA-CORE.tecnologicoitca.edu.ec
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW-ITCA-CORE(config)#
*Mar  1 00:07:48.675: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-ITCA-CORE(config)#ip ssh version 2
SW-ITCA-CORE(config)#ip ssh time-out 30
SW-ITCA-CORE(config)#ip ssh authentication-retries 3
SW-ITCA-CORE(config)#username itca privilege 15 password itca@2016
SW-ITCA-CORE(config)#line vty 0 4
SW-ITCA-CORE(config-line)#transport input ssh telnet
SW-ITCA-CORE(config-line)#login local
SW-ITCA-CORE(config-line)#exit
SW-ITCA-CORE(config)#line console 0
SW-ITCA-CORE(config-line)#password cisco
SW-ITCA-CORE(config-line)#login
SW-ITCA-CORE(config-line)#exit
SW-ITCA-CORE(config)#enable password cisco
SW-ITCA-CORE(config)#enable secret class
SW-ITCA-CORE(config)#service password-encryption
SW-ITCA-CORE(config)#exit
SW-ITCA-CORE#
*Mar  1 00:08:29.499: %SYS-5-CONFIG_I: Configured from console by console
SW-ITCA-CORE#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-ITCA-CORE#
```

CONFIGURACION DE VTP SERVER

```
SW-ITCA-CORE#vlan database
SW-ITCA-CORE(vlan)#vtp server
Device mode already VTP SERVER.
SW-ITCA-CORE(vlan)#vtp domain itca
Changing VTP domain name from NULL to itca
SW-ITCA-CORE(vlan)#vtp password itca
Setting device VLAN database password to itca.
SW-ITCA-CORE(vlan)#apply
APPLY completed.
SW-ITCA-CORE(vlan)#exit
APPLY completed.
Exiting....
SW-ITCA-CORE#
```

COMPROBACION DE VTP SERVER

```
SW-ITCA-CORE#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 256
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : itca
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x16 0xA6 0x88 0xE5 0x13 0xF2 0x71 0xA4
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
SW-ITCA-CORE#
```

CREACION DE VLANS EN SWITCH DE CORE:

```
SW-ITCA-CORE#vlan database
SW-ITCA-CORE(vlan)#vlan 2 name servidores
VLAN 2 added:
    Name: servidores
SW-ITCA-CORE(vlan)#vlan 3 name Administrativos
VLAN 3 added:
    Name: Administrativos
SW-ITCA-CORE(vlan)#vlan 4 name Sistemas
VLAN 4 added:
    Name: Sistemas
SW-ITCA-CORE(vlan)#vlan 5 name Laboratorios
VLAN 5 added:
    Name: Laboratorios
SW-ITCA-CORE(vlan)#vlan 6 name Wireless
VLAN 6 added:
    Name: Wireless
SW-ITCA-CORE(vlan)#vlan 7 name Vigilancia
VLAN 7 added:
    Name: Vigilancia
SW-ITCA-CORE(vlan)#vlan 8 name Coordinadores
VLAN 8 added:
    Name: Coordinadores
SW-ITCA-CORE(vlan)#vlan 9 name Internet
VLAN 9 added:
    Name: Internet
SW-ITCA-CORE(vlan)#vlan 10 name Laboratorio3
VLAN 10 added:
    Name: Laboratorio3
SW-ITCA-CORE(vlan)#vlan 10 name W_Estudiantes
VLAN 10 modified:
    Name: W_Estudiantes
SW-ITCA-CORE(vlan)#vlan 10 name Laboratorio3
VLAN 10 modified:
    Name: Laboratorio3
SW-ITCA-CORE(vlan)#vlan 11 name W_Estudiantes
VLAN 11 added:
    Name: W_Estudiantes
SW-ITCA-CORE(vlan)#vlan 12 name W_Docentes
VLAN 12 added:
    Name: W_Docentes
SW-ITCA-CORE(vlan)#vlan 13 name W_Administrativos
VLAN 13 added:
    Name: W_Administrativos
SW-ITCA-CORE(vlan)#vlan 14 name W_Invitados
VLAN 14 added:
    Name: W_Invitados
SW-ITCA-CORE(vlan)#vlan 15 name Cyber
VLAN 15 added:
    Name: Cyber
SW-ITCA-CORE(vlan)#vlan 16 name CACMU
```

CONFIGURACION DE ENLACES TRONCALES EN SWITCH CORE:

```
SW-ITCA-CORE(config)#interface fastEthernet 0/1
SW-ITCA-CORE(config-if)#swi
SW-ITCA-CORE(config-if)#switchport mo
SW-ITCA-CORE(config-if)#switchport mode tru
SW-ITCA-CORE(config-if)#switchport mode trunk
SW-ITCA-CORE(config-if)#
*Mar  1 00:06:36.275: %DTP-5-TRUNKPORTON: Port Fa0/1 has become dot1q trunk
SW-ITCA-CORE(config-if)#sw
SW-ITCA-CORE(config-if)#switchport trun
SW-ITCA-CORE(config-if)#switchport trunk encap
SW-ITCA-CORE(config-if)#switchport trunk encapsulation do
SW-ITCA-CORE(config-if)#switchport trunk encapsulation dot1q
SW-ITCA-CORE(config-if)#exit
SW-ITCA-CORE(config)#interface fastEthernet 0/0
SW-ITCA-CORE(config-if)#switchport mode trunk
SW-ITCA-CORE(config-if)#switchport trunk encapsulation dot1q
SW-ITCA-CORE(config-if)#
*Mar  1 00:06:52.935: %DTP-5-TRUNKPORTON: Port Fa0/0 has become dot1q trunk
SW-ITCA-CORE(config-if)#exit
SW-ITCA-CORE(config)#
```

CONFIGURACION DE ENLACES TRONCALES EN OTRO SWITCH:

```
SW2(config)#interface fastEthernet 0/0
SW2(config-if)#swi
SW2(config-if)#switchport mo
SW2(config-if)#switchport mode tru
SW2(config-if)#switchport mode trunk
SW2(config-if)#swi
SW2(config-if)#switchport
*Mar  1 00:07:13.491: %DTP-5-TRUNKPORTON: Port Fa0/0 has become dot1q trunk
SW2(config-if)#switchport trun
SW2(config-if)#switchport trunk enca
SW2(config-if)#switchport trunk encapsulation do
SW2(config-if)#switchport trunk encapsulation dot1q
SW2(config-if)#end
SW2#show
```

CONFIGURACION DE VTP CLIENTE EN SWITCH:

```
ESW2#vlan database
ESW2(vlan)#vtp client
Setting device to VTP CLIENT mode.
ESW2(vlan)#vtp domain itca
Changing VTP domain name from NULL to itca
ESW2(vlan)#vtp password itca
Setting device VLAN database password to itca.
ESW2(vlan)#apply
Apply not allowed when device is in CLIENT state.
ESW2(vlan)#exit
In CLIENT state, no apply attempted.
Exiting....
ESW2#
```

COMPROBACIÓN VTP CLIENTE:

```
ESW2#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 256
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : itca
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x16 0xA6 0x88 0xE5 0x13 0xF2 0x71 0xA4
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

COMPROBACION DE PROPAGACION DE VLANS EN SWITCH CLIENTE

```
SW2#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15
2    servidores                       active
3    Administrativos                  active
4    Sistemas                         active
5    Laboratorios                     active
6    Wireless                         active
7    Vigilancia                       active
8    Coordinadores                    active
9    Internet                         active
10   Laboratorio3                     active
11   W_Estudiantes                    active
12   W_Docentes                       active
13   W_Administrativos                active
14   W_Invitados                      active
15   Cyber                            active
16   CACMU                            active
1002 fddi-default                     active

SW2#_
```

CONFIGURACION DE VLAN DE MODO ACCESO EN EL SWITCH DE CORE

```
SW-ITCA-CORE(config)#interfac fast
SW-ITCA-CORE(config)#interfac fastEthernet 0/10
SW-ITCA-CORE(config-if)#switchpo
SW-ITCA-CORE(config-if)#switchport mode access
SW-ITCA-CORE(config-if)#switchport  access vlan 4
SW-ITCA-CORE(config-if)#no shutdown
SW-ITCA-CORE(config-if)#exit
```

ANEXO 4

ISTALACIÓN DE FIREWALL PFSENSE

Manual de usuario e Instalación de Pfsense

Acerca de este manual

Este manual es una compilación de varios tutoriales, videos y documentación oficial cuyas fuentes serán citadas al final de este manual, es un trabajo de carácter académico y no representa ninguna violación a los derechos de autor. Este manual mostrara la descripción general del software, su casa de software desarrolladora, requerimientos de hardware, instalación, funcionalidades haciendo énfasis a la configuración de las reglas de firewall, conclusiones y por último se citaran las fuentes bibliográficas de donde fue extraída la información.

Contenido:

1. Introducción a Pfsense

2. Requerimientos de hardware

3. Acerca de BSD

4. Funcionalidades de Pfsense

5. Instalación de Pfsense

6. Configuración de reglas de firewall en Pfsense

7. Conclusiones

8. Material de Referencia

Introducción a Pfsense:

| Pfsense es una distribución personalizada de FreeBSD para usarlo en servicios de redes LAN y WAN tales como firewall, enrutador, servidor de balanceo de carga, entre otras las cuales serán mencionadas más adelante. El proyecto es comercialmente sostenido por BSD perimeter LLC. Este proyecto nació el año 2004 por Chris Buechler y Ullrich Scott en instalaciones para PC y servidores. El modelo de desarrollo de pfsense es de código abierto, la última versión estable es la versión 1 2 3, el núcleo de pfsense es basado en el sistema operativo libre llamado BSD, el tipo de nucleo de pfsense es de tipo monolítico. De acuerdo al portal oficial de pfsense para el 2010 pfsense ha tenido más de un millón de descargas donde ha sido instalado con éxito en ambientes desde redes domésticas hasta grandes corporaciones. Pfsense cuenta con un gestor de paquetes desde su interfaz gráfica accedida remotamente para ampliar sus funcionalidades, al elegir el paquete deseado el sistema lo descarga y lo instala automáticamente. Existen 60 modulos disponibles para descargar al pfsense e instalarlos entre estos son el proxy squid IMinspector, Snort, ClamAV entre otros. Para manejar pfsense no es necesario tener conocimientos avanzados sobre línea de comandos de BSD. Pfsense puede ser instalado en cualquier ordenador PC o servidor independientemente de su arquitectura que cuente con un mínimo de 2 tarjetas de red. Al poseer software de código abierto, la comunidad de desarrolladores pueden dar soporte y asistencia con costo por parte de BSD Perimeter. Cada persona es libre de modificar y vender su propia distribución con ciertas condiciones.

Requerimientos de Hardware

Para la instalación de pfsense sobre arquitectura i386 los requerimientos de hardware son los siguientes.

1. Procesador Intel Pentium III, hasta un Intel Xeon, nada de AMD.
2. Memoria RAM desde 256 Mb hasta 3 Gb.
3. Disco Duro de 2 Gb hasta 80 Gb, IDE, SCSI, SATA Y SAS-SATA.

4. Tarjetas de red cableadas Intel y Realtek (la red inalambrica solamente funcionan las tarjetas de red marca Atheros).

5. Debido a que este software será instalado sobre un servidor o PC dedicado única y exclusivamente, este PC o servidor no necesitara un mouse, solo un teclado y monitor ya que este servidor será administrado remotamente.

Acerca de BSD

BSD Es la abreviatura de Berkeley Software Distribution que traducido al español es llamado Distribución de software Berkeley el cual es un sistema operativo derivado de Unix nacido a partir de un proyecto de la universidad de California en Berkeley. En sus primeros años los laboratorios Bell autorizaron a esta universidad a trabajar el código fuente de Unix y adaptarlo a sus necesidades, esto se realizó entre los años sesenta y ochenta pero luego AT&T retiro este permiso por motivos comerciales. Sin embargo la universidad haciendo uso de sus investigaciones con el código fuente de Unix creo una distribución de sistema operativo llamado BSD con fines académicos y reduciendo algunas restricciones legales en cuanto a su uso. Entre los sistemas operativos desarrollados por Berkeley son SunOS, FreeBSD, NetBSD, PC-BSD, OpenBSD Y MacOS. Y BSD ha contribuido en el desarrollo en los sistemas operativos en general en cuanto a implementaciones de TCP que derivan de la versión 4.4 BSD lite, el manejo de memoria virtual paginada por demanda, control de trabajos, y el sistema de archivos FFS.

Funcionalidades del PFSense

Pfsense es una aplicación que se instala como un sistema operativo ya que tiene varias funcionalidades entre estos servicios de redes LAN y WAN, con detalle estos servicios son los siguientes:

Firewall: Pfsense se puede configurar como un cortafuego permitiendo y denegando determinado tráfico de redes tanto entrante como saliente a partir de una dirección ya sea de red o de host de origen y de destino, también haciendo filtrado avanzado de paquetes por protocolo y puerto.

Servidor VPN: Pfsense se puede se puede configurar como un servidor VPN usando protocolos de tunneling tales como IPSec, PPTP, entre otras.

Servidor de Balanceo de Carga: Pfsense puede ser configurado como servidor de balanceo de carga tanto entrante como saliente, esta característica es usada comúnmente en servidores web, de correo, de DNS. También para proveer estabilidad y redundancia en él envió de tráfico a través del enlace WAN evitando los cuellos de botella.

Portal Cautivo: Este servicio consiste en forzar la autenticación de usuarios redirigiéndolos a una página especial de autenticación y/o para aceptar los términos de uso, realizar un pago etc. para poder tener acceso a la red. El portal cautivo es usado comúnmente para control de accesos a la red en los puntos de accesos inalámbricos de los hoteles, restaurantes, parques y kioscos.

Tabla de estado: PFSense es un stateful firewall, el cual como característica principal guardad el estado de las conexiones abiertas en una tabla. La mayoría de los firewall no tienen la capacidad de controlar con precisión la tabla de estado. Pfsense tiene un enorme número de características que permiten una granularidad muy fina para el manejo de la tabla de estado.

Servidor DNS y reenviador de cache DNS: Pfsense se puede configurar como un servidor DNS primario y reenviador de consultas de DNS.

Servidor DHCP: Tambien funciona como servidor de DHCP, se puede también implementar VLAN desde Pfsense.

Servidor PPPoE: Este servicio es usado por los ISP para la autenticación de usuarios que puedan ingresar a internet, por una base local o via radius.

Enrutamiento estatico: Pfsense funciona como un enrutador ya que entrega direccionamiento IP y hace el nateo hacia afuera.

Redundancia: Pfsense permite configurar dos o más cortafuegos a través del protocolo CARP (Common Address Redundancy Protocol) por si uno de los cortafuegos se cae el otro se declara como cortafuegos primario.

Reportes Y Monitoreo: A través de los graficos RDD Pfsense muestra el estado de los siguientes componentes:

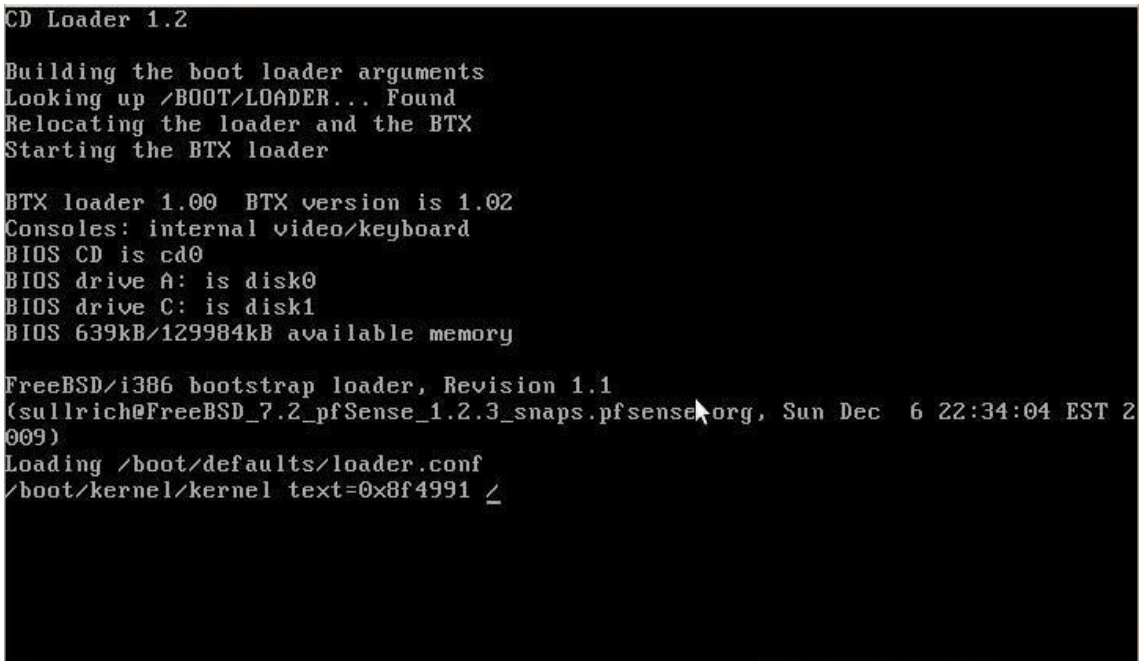
-

- Utilización de CPU
- Rendimiento Total
- Estado del Firewall
- Rendimiento individual por cada interface
- Paquetes enviados y recibidos por cada interface
- Manejo de tráfico y ancho de banda.

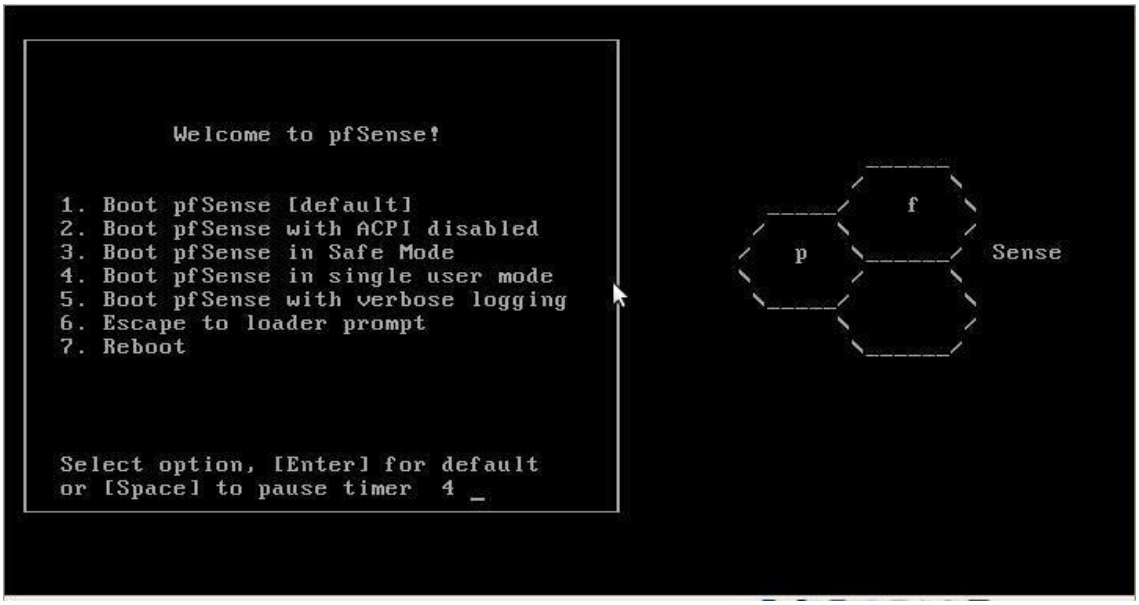
Instalacion del pfsense

El proceso de instalación del pfsense se realiza de la siguiente manera:

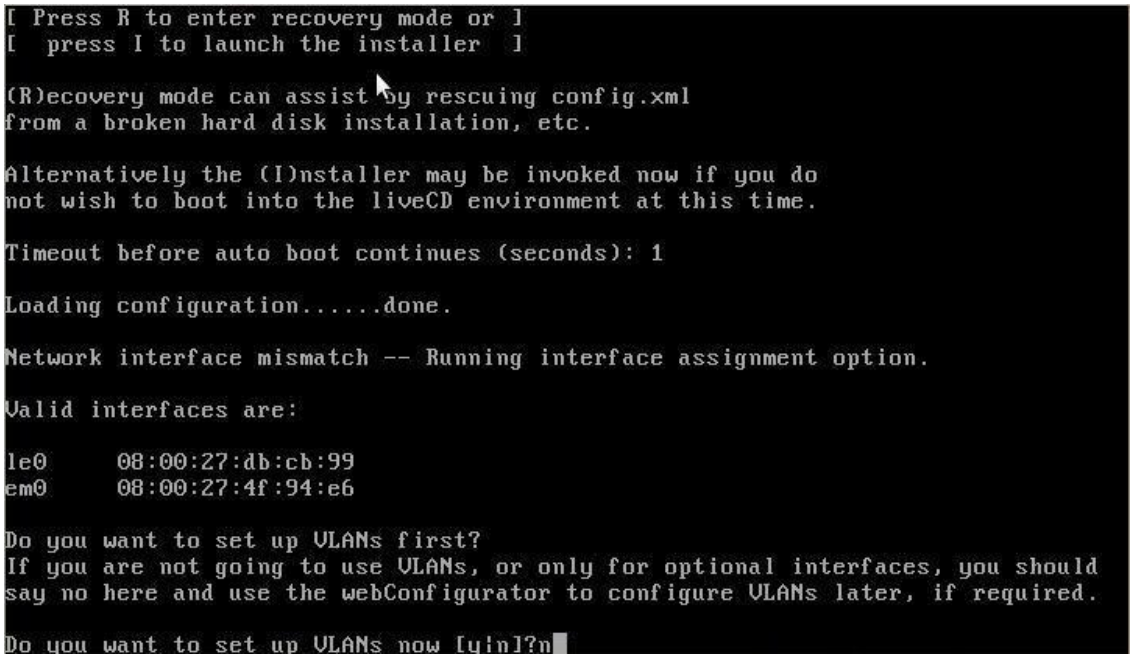
1. Se arranca el PC o el servidor desde la unidad de CD verificando arranque tal y como se muestra en esta pantalla.



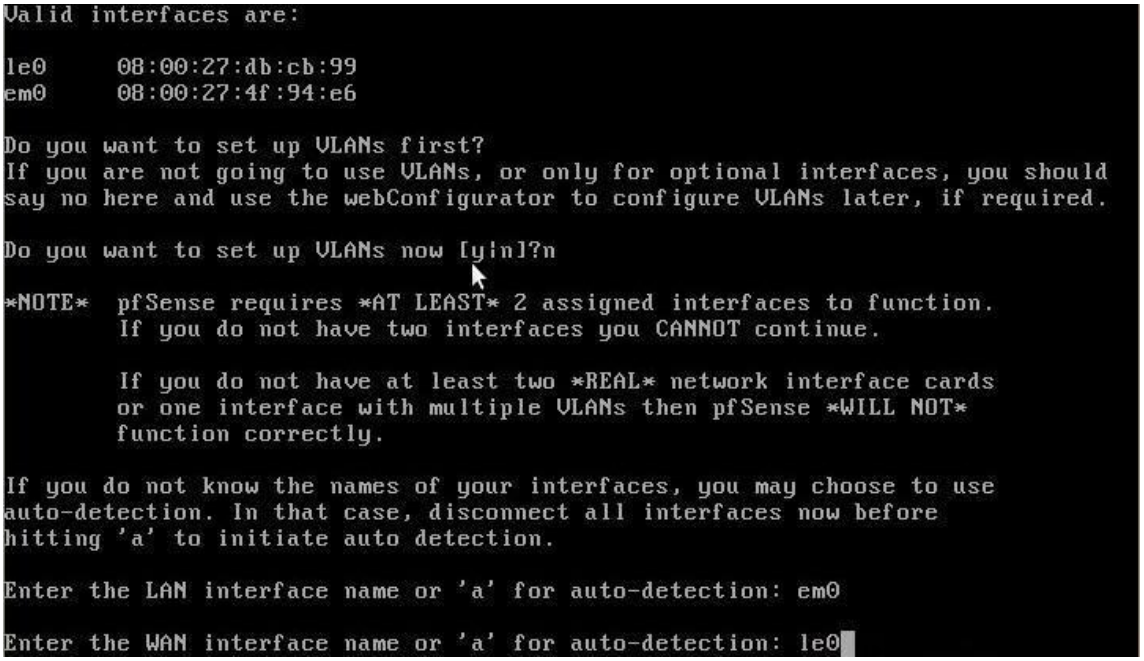
2. Se visualizara luego la siguiente pantalla mostrando el menú de arranque del pfsense como tal donde seleccionamos la opción 1



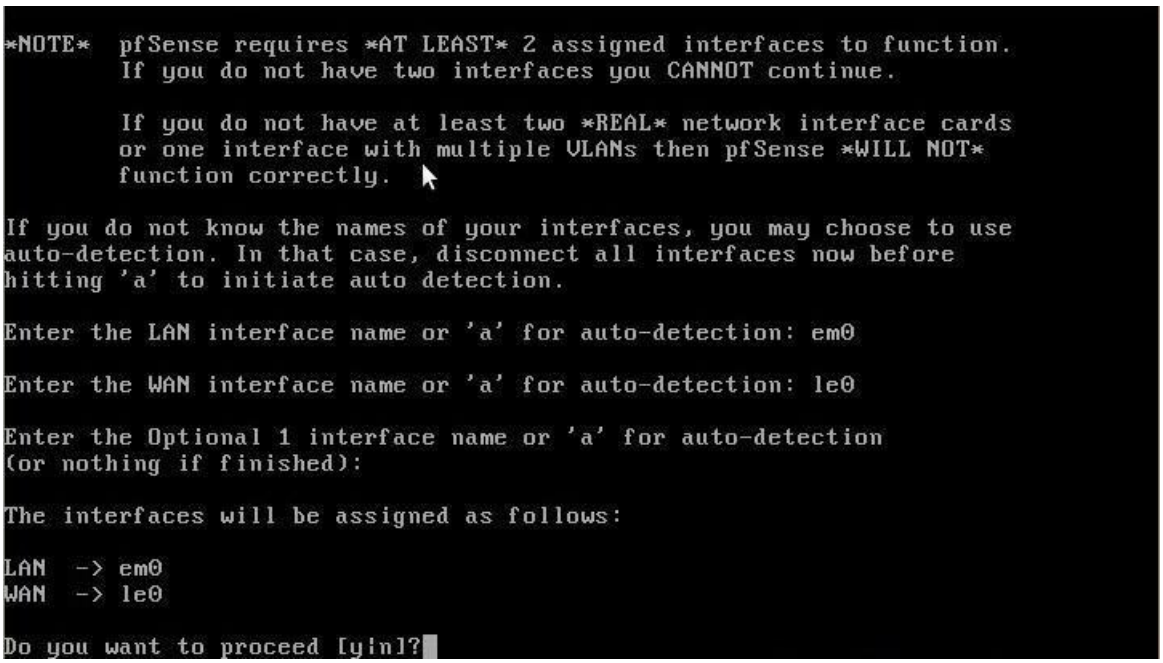
3. Después saldrá un pantallazo tal cual como se muestra a continuación indicándonos que identificador le daremos a las tarjetas de red que se encuentran instaladas y reconocidas por el pfsense, las cuales se identifican por el fabricante de la tarjeta de red y pregunta que si queremos configurar vlan para la red LAN en este caso le decimos que no.



4. Enseguida le damos el identificador de las tarjetas de red para diferenciar cual será LAN y WAN respectivamente así. Los identificadores pueden varias dependiendo del fabricante de las tarjetas de red

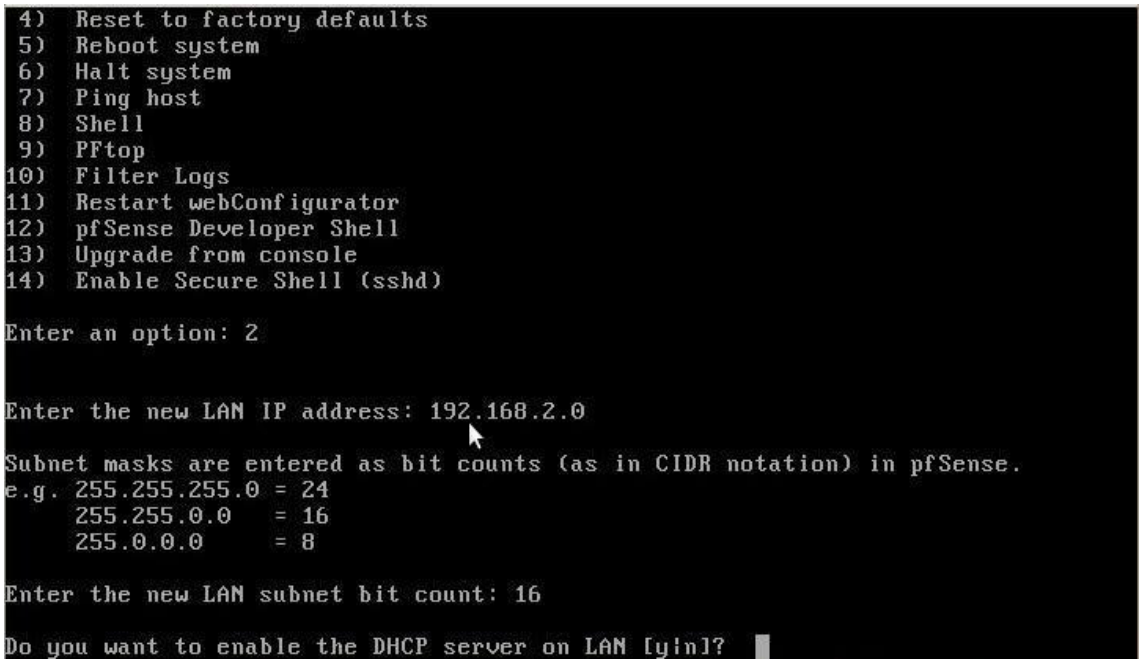


5. Luego de configurar el identificador de las tarjetas de red el sistema nos preguntara si esta configuración es correcta para proceder con la carga de archivos de instalación del pfsense donde damos "Y"

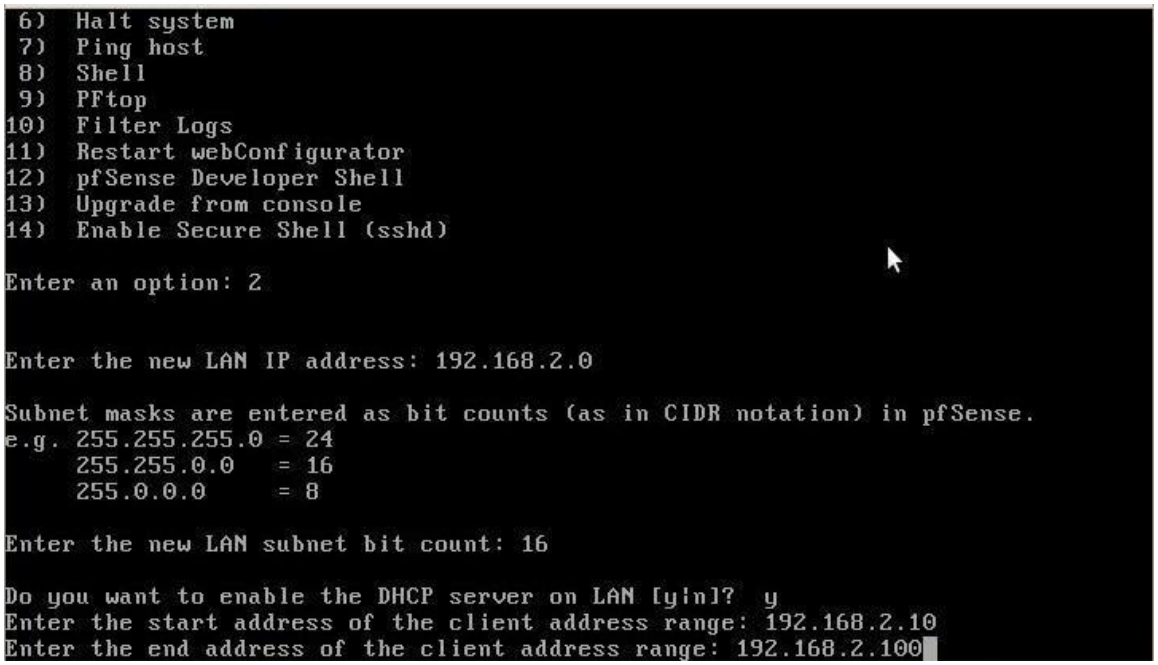


6. En este momento nos saldrá una pantalla como esta con 16 opciones de configuración previa antes de iniciar la instalación, lo recomendable es configurar primero la ip fija para la red LAN de acuerdo al rango que se tenga en la topología existente

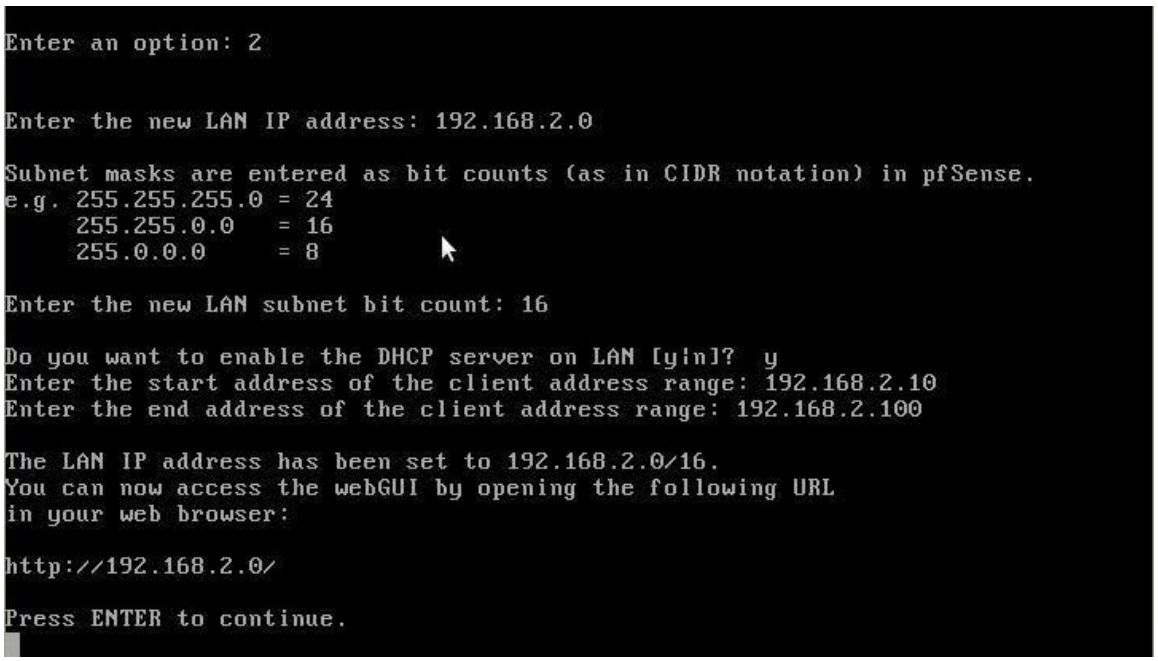
7. Esta configuración se realiza en dos campos, primero la dirección IP ejemplo 192.168.2.1 y segundo se configura la longitud de la máscara de acuerdo a las que aparecen en la siguiente pantalla.



8. y por último el sistema nos pregunta si queremos habilitar el servicio DHCP le damos que si para indicar la ip inicial y la ip final de la siguiente forma:



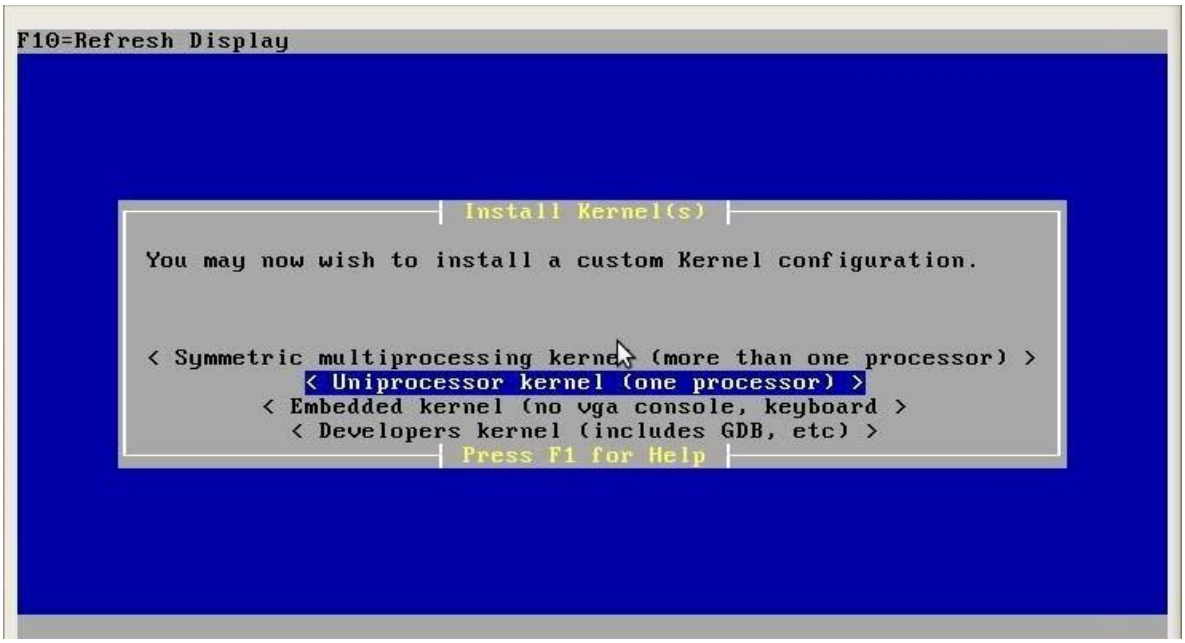
9. resultado de esta configuración será el siguiente, aquí el sistema nos indicara la ip por la cual accederemos a la consola por web y la configuración dhcp que fue realizada.



10. El siguiente paso será digitar el número 99 para dar inicio a la instalación del pfsense en el disco duro donde saldrá la siguiente pantalla. En esta pantalla seleccionaremos la opción “Accept these settings”. Aquí el sistema empezara a formatear el disco duro y copiar los archivos del sistema.

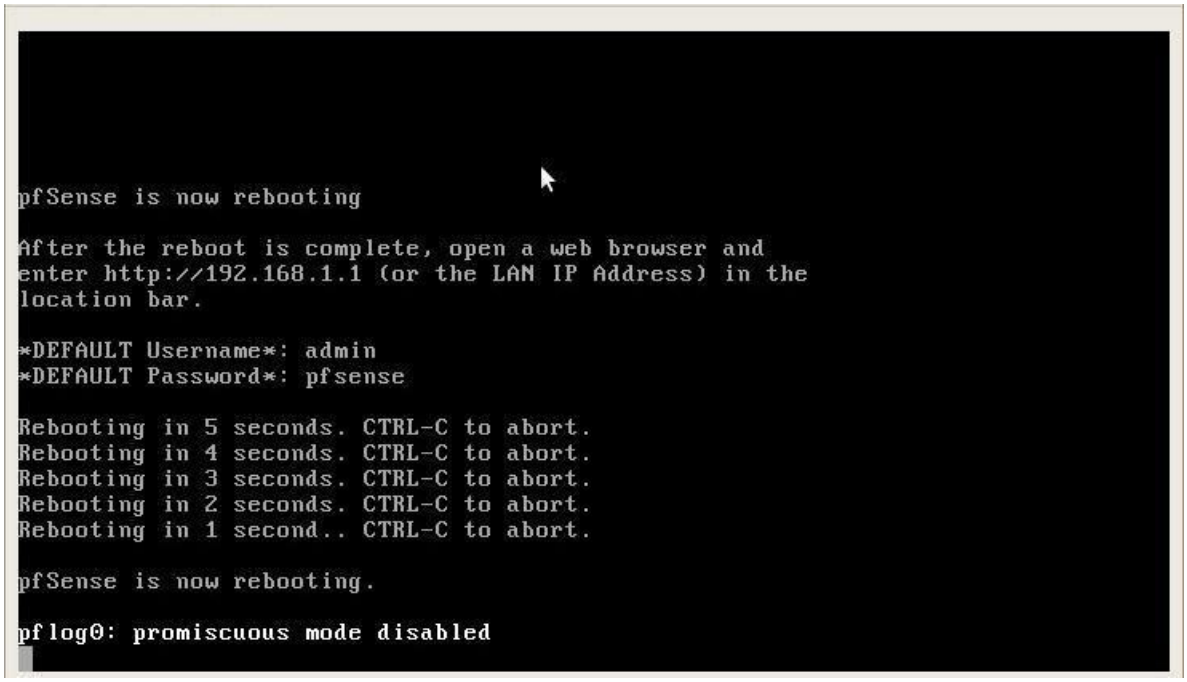
11. Luego nos saldrá la siguiente pantalla en donde nos preguntara que tipo de instalación queremos aplicar a nuestro servidor, o si queremos recuperar el archivo de config.xml. Seleccionamos la opción Quick/Easy install.

12. En el siguiente paso seleccionamos el kernel para el procesador que estemos utilizando, en la mayoria de casos “uniprocessor kernel” las otras opciones se reservan para otros usos como programadores, o dispositivos que se manejan via cable Serial.

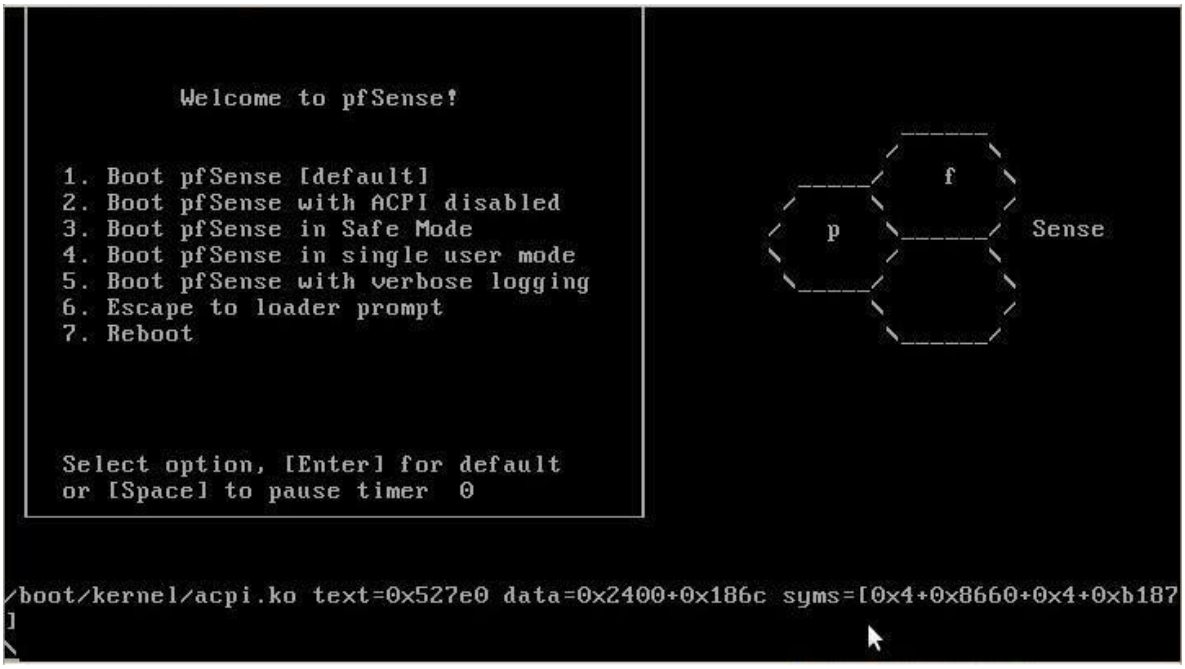


13. Por ultimo seleccionamos OK para dar por terminado el proceso de instalación del pfsense en el servidor dedicado y seleccionamos “reboot”

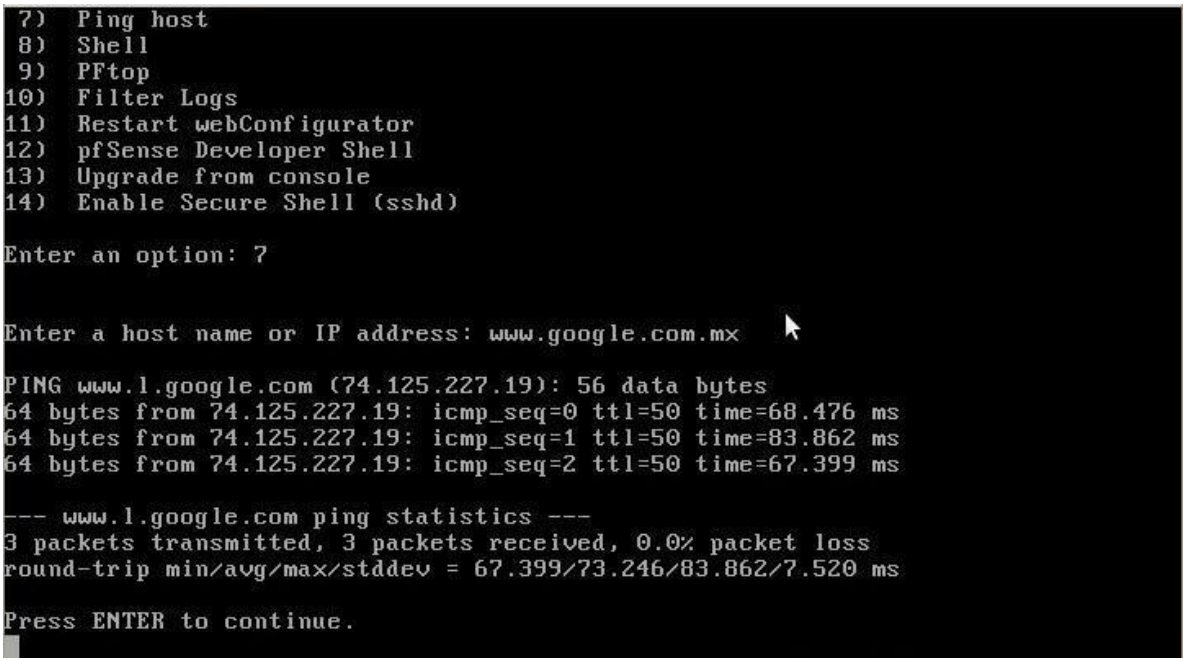
14. Luego antes de reiniciar por HDD saldrá esta pantalla con el usuario y contraseña de ingreso a la consola web.



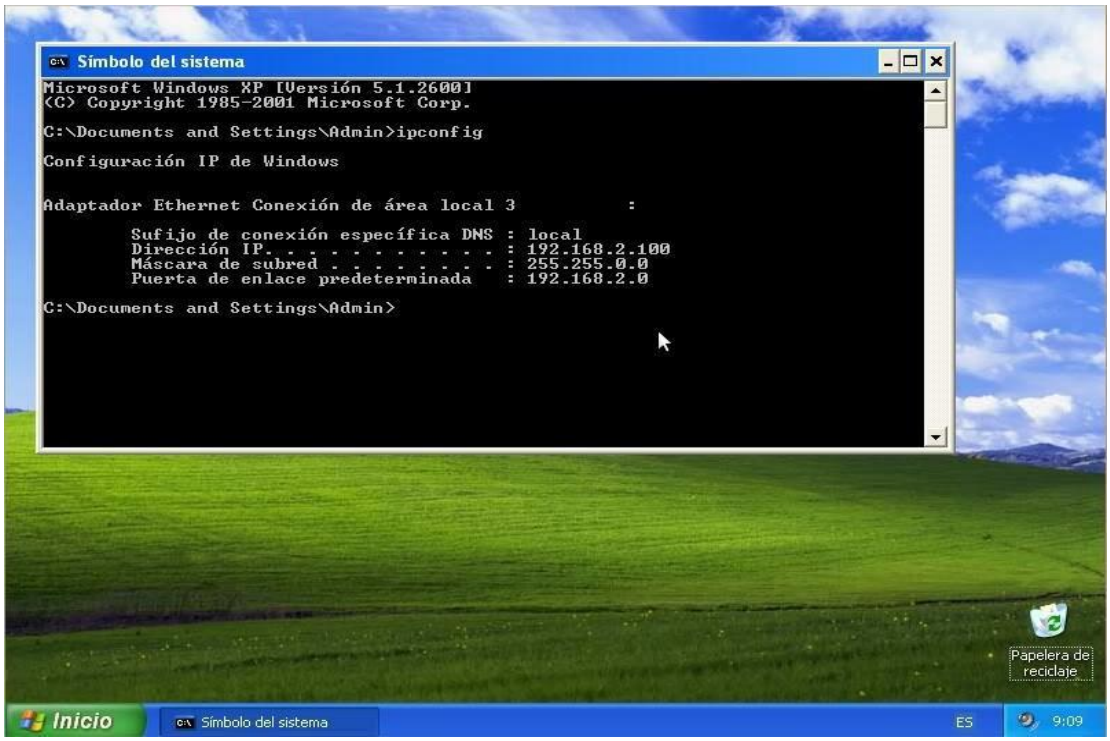
15. Arrancamos el servidor dedicado desde el disco duro



16. Comprobamos el acceso a internet del pfsense a través de un ping a una página web ejemplo www.google.com esto se hace con la opción 7.



17. En la misma red lan nos ubicamos en un equipo diferente con sistema operativo windows o Linux verificando que este tenga una ip entregada del servidor pfsense para poder acceder a la consola web.



18. Comprobamos acceso a internet a través del servidor pfsense.

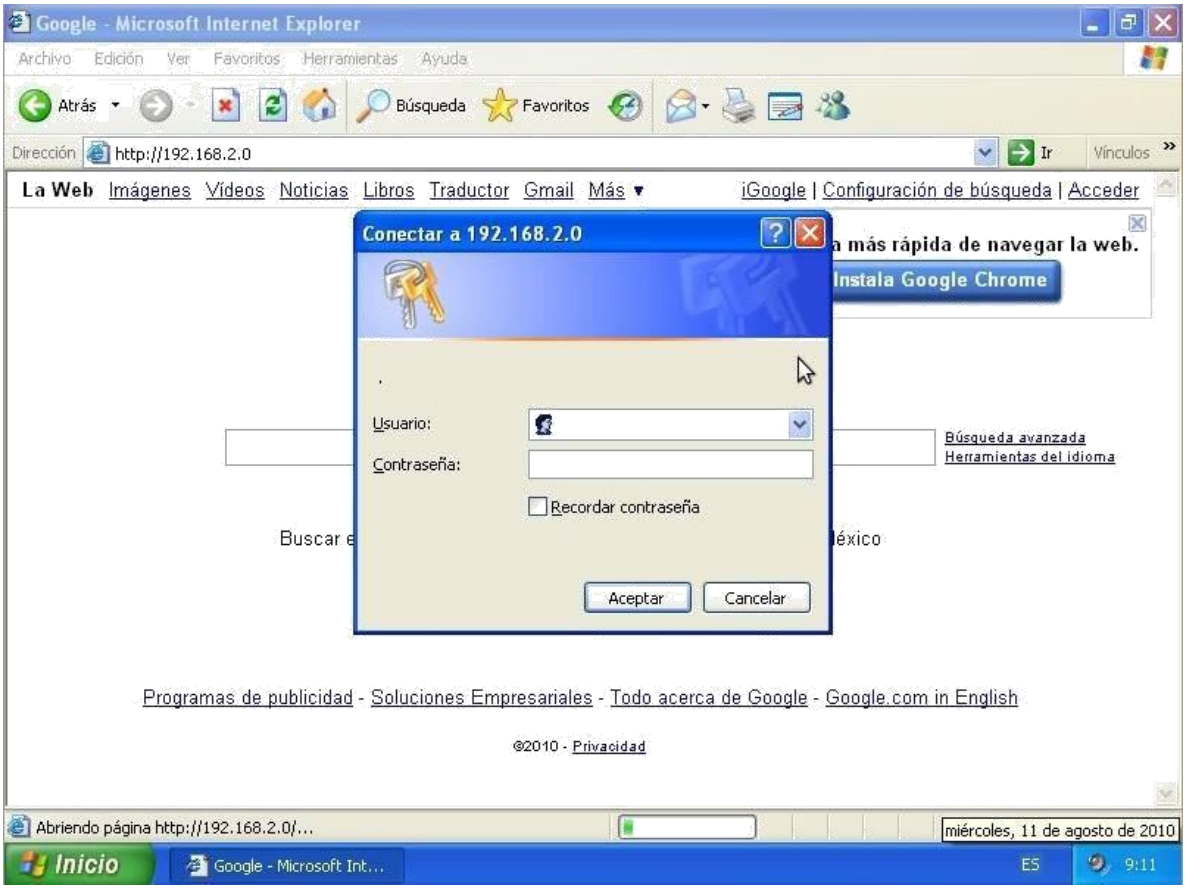
19. Para ingresar a la consola web ingresamos la ip que configuramos previamente para la interfaz LAN http://192.168.2.1 y nos saldrá una ventana para ingresar usuario y contraseña:

    Usuario: admin

    contraseña:

    pfsense

Esta ip es la puerta de enlace que será entregada a los equipos cliente a través de dhcp,

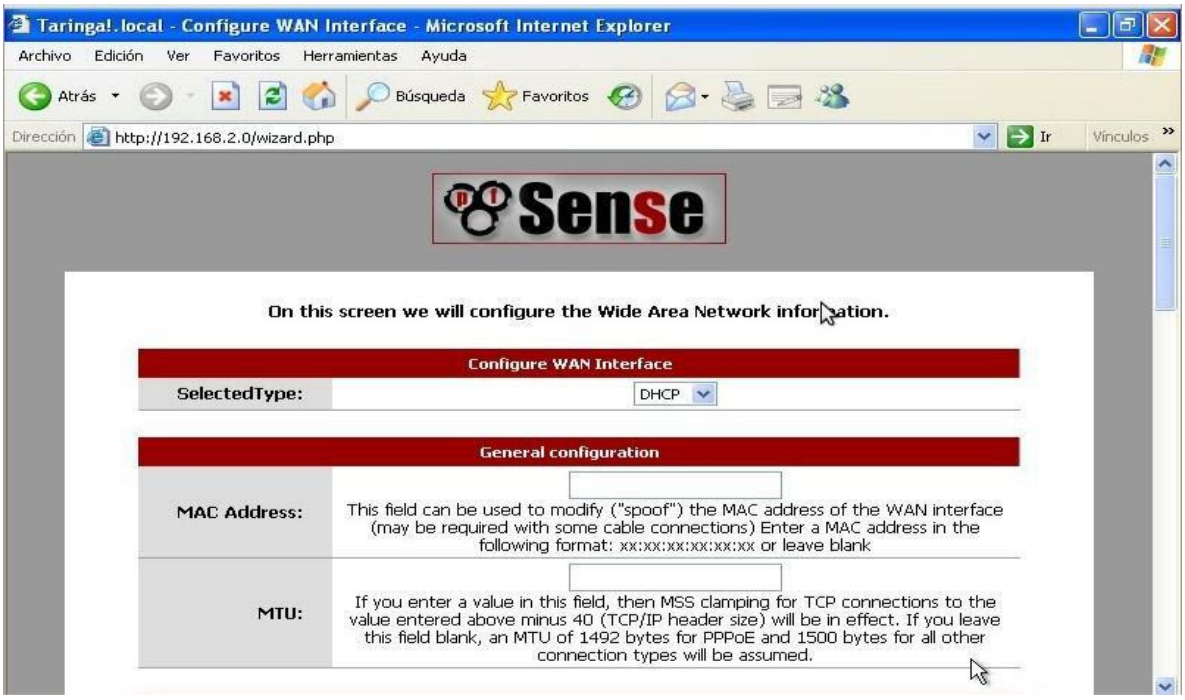


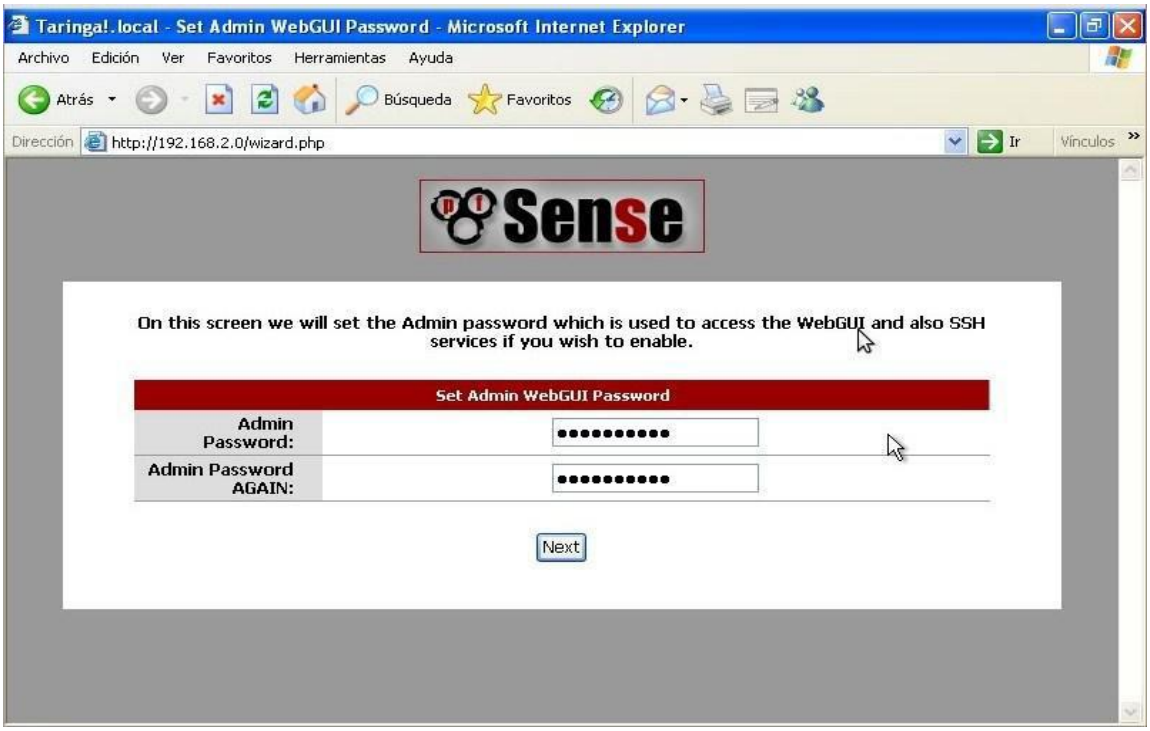
20. pues de ingresar las credenciales de ingreso nos saldrá una serie de pantallazos con los siguientes parámetros de configuración:

- Servidores DNS ya sean de otro servidor en la topología, o los entregados por el ISP o los propios del sistema operativo.
- Nombre del host como todo equipo en una red. Nombre del dominio si existe en el sistema.

21. En la configuración de la interfaz WAN se modifica cuando en la topología existen IP´s fijas públicas entregadas por el ISP

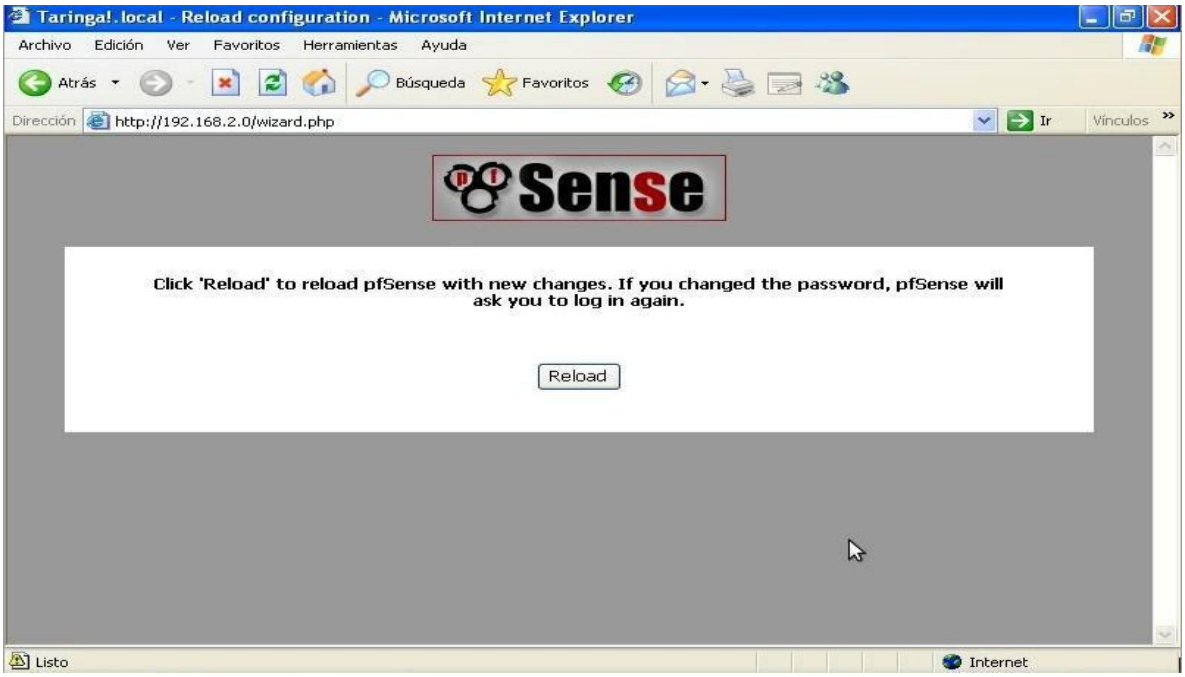
En esta pantalla se configura la nueva contraseña para ingresar a la consola web del pfsense.





23. Por último saldrá la pantalla de reiniciar el sistema con los cambios guardados.

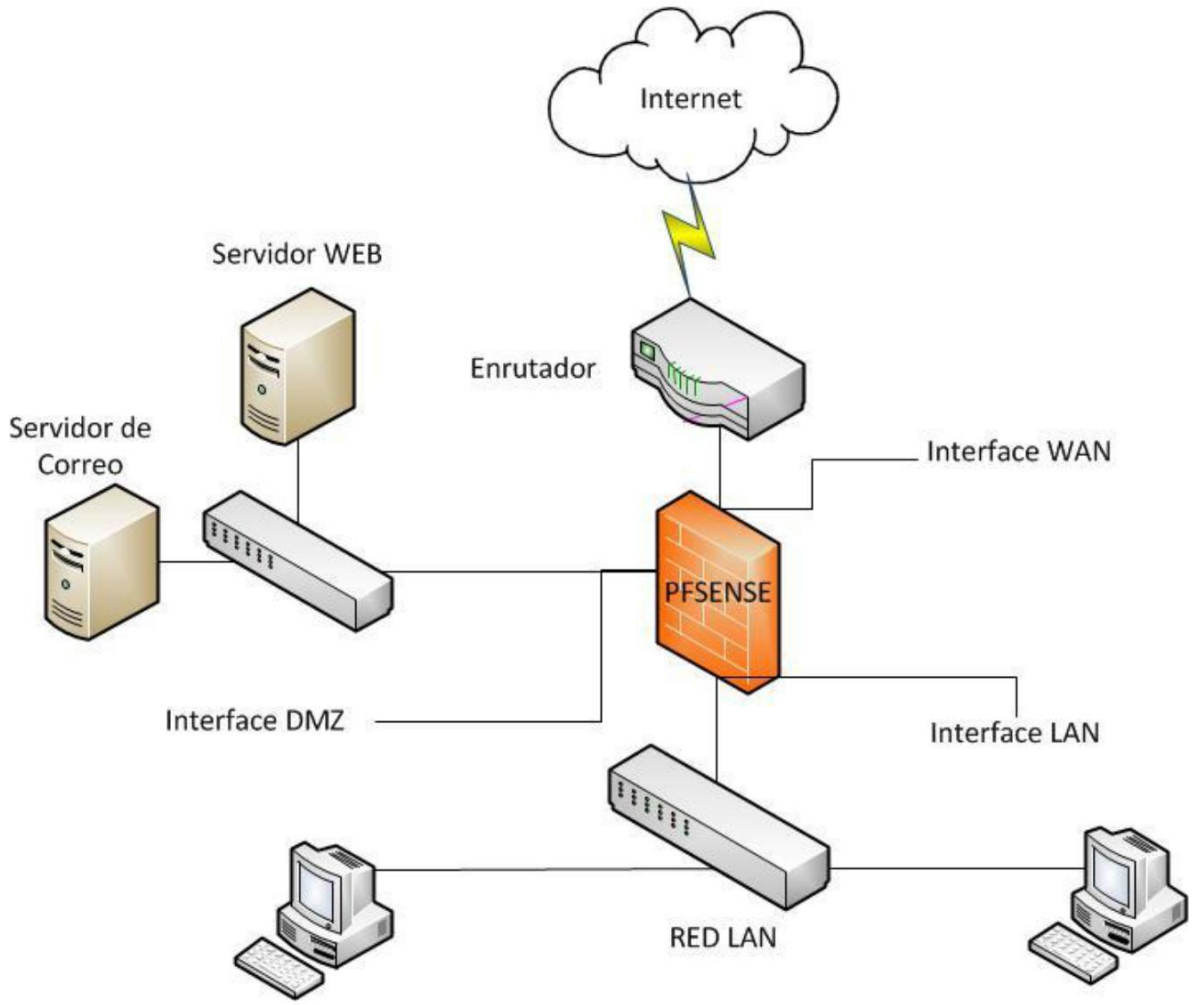
24. Por último saldrá la pantalla de inicio del Firewall listo para configurar las reglas de filtrado.



Configuración de reglas de Firewall en Pfsense

Despues de haber instalado el Pfsense en el disco duro y haber configurado los parámetros iniciales, procederemos a configurar las reglas de firewall las cuales se aplican a las interfaces configuradas previamente.

Antes de empezar a configurar las reglas de firewall es necesario tener clara la topología de la red donde está participando el Pfsense y de qué forma, ejemplo:



- La red LAN se refiere a la red interna de la organización la cual está conectada a la interfaz LALa red DMZ que significa zona desmilitarizada es donde se ubican

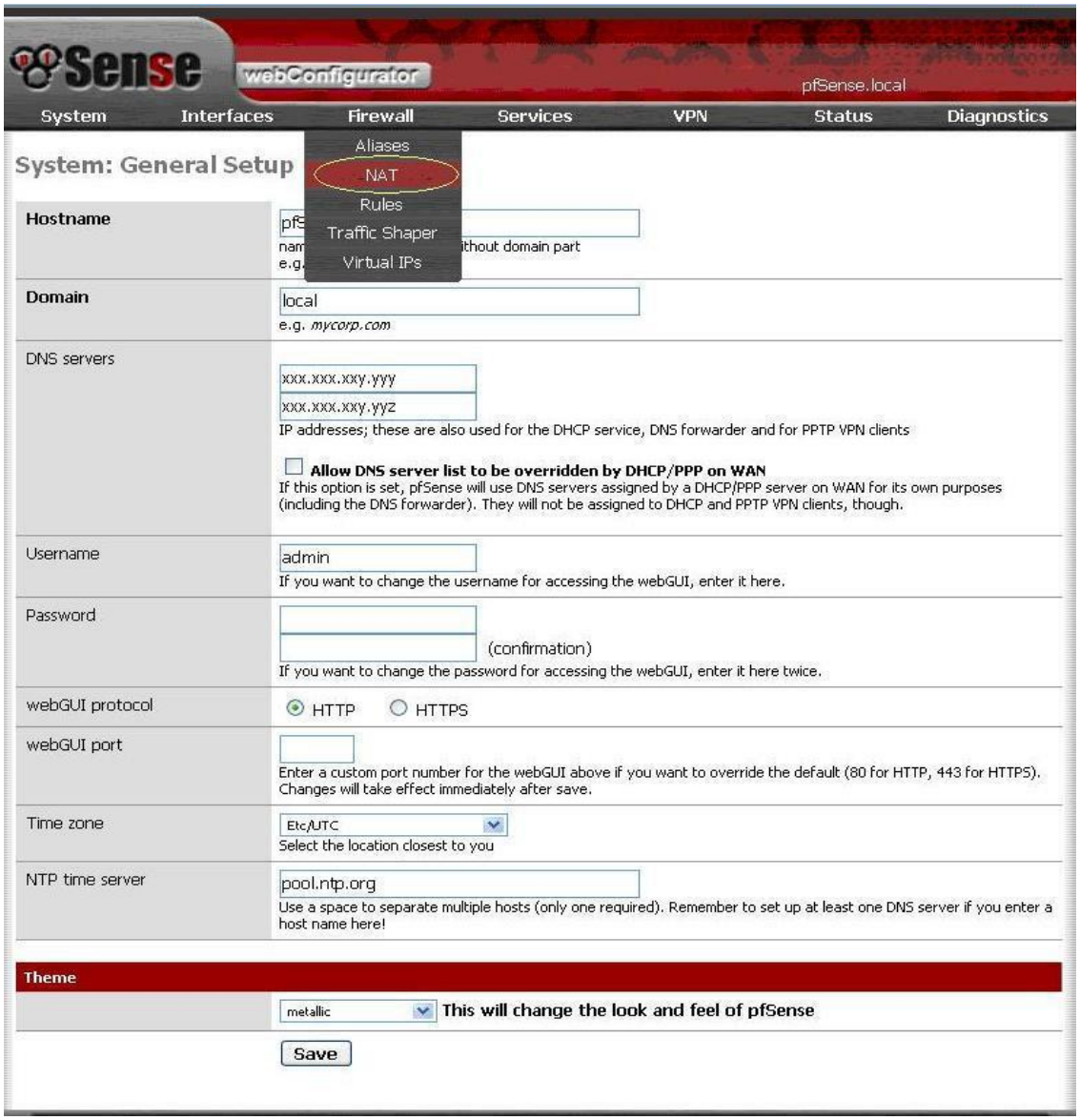
los servidores los cuales se puede tener acceso desde internet como servidores web y de correo con ciertos parámetros.

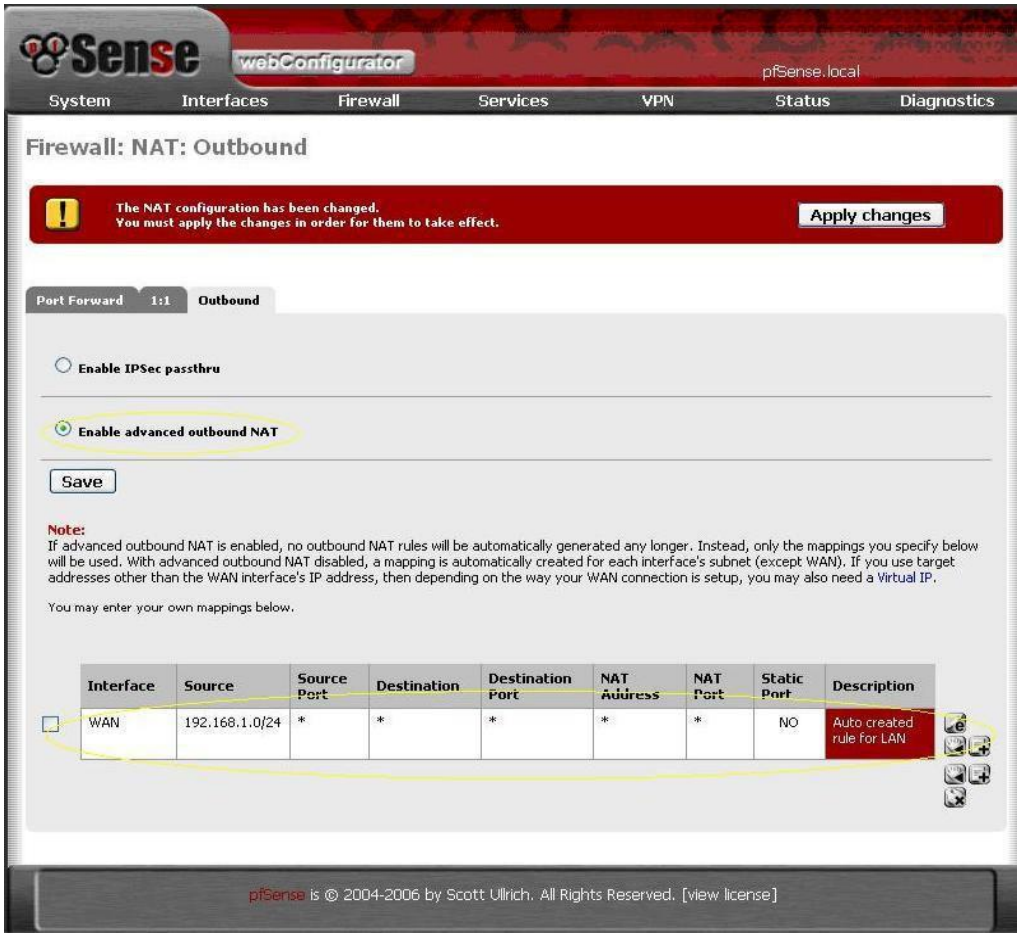
- La red WAN que es básicamente internet está conectada a la interfaz WAN del Pfsense el cual también deniega tráfico desde la red la hacía internet y viceversa

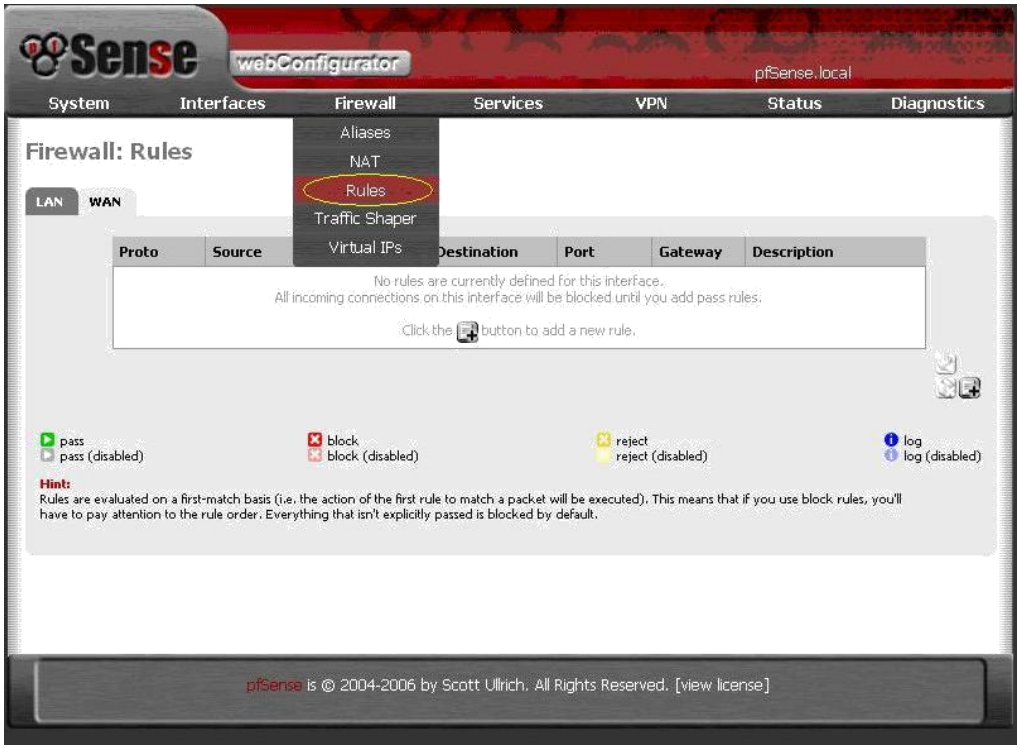
En PFSense las reglas de firewall se configuran de la siguiente manera:

1. Nos ubicamos en la pestaña Firewall y en la opción NAT en la barra de menú ubicado en la parte superior de la pantalla del browser de internet:
   N la cual debe estar protegida de ataques desde internet.

2. En esta pantalla habilitaremos la opción de Enable Advanced Outbound NAT luego borrar todas las reglas de firewall que hay por defecto esto con el objetivo de que el firewall quede transparente como un bridge y configurar las reglas sin ningún problema.


pfSense
webConfigurator
pfSense.local
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Aliases
NAT
Rules
Traffic Shaper
Virtual IPs
System: General Setup
Hostname
pfS
ithout domain part
e.g.
Domain
local
e.g. mycorp.com
DNS servers
xxx.xxx.xxy.yyy
xxx.xxx.xxy.yyz
IP addresses; these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients
Allow DNS server list to be overridden by DHCP/PPP on WAN
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). They will not be assigned to DHCP and PPTP VPN clients, though.
Username
admin
If you want to change the username for accessing the webGUI, enter it here.
Password
(confirmation)
If you want to change the password for accessing the webGUI, enter it here twice.
webGUI protocol
HTTP
HTTPS
webGUI port
Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.
Time zone
Etc/UTC
Select the location closest to you
NTP time server
pool.ntp.org
Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!
Theme
metallic
This will change the look and feel of pfSense
Save


pfSense
webConfigurator
pfSense.local
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Firewall: NAT: Outbound
The NAT configuration has been changed.
You must apply the changes in order for them to take effect.
Apply changes
Port Forward
1:1
Outbound
Enable IPSec passthru
Enable advanced outbound NAT
Save
Note:
If advanced outbound NAT is enabled, no outbound NAT rules will be automatically generated any longer. Instead, only the mappings you specify below will be used. With advanced outbound NAT disabled, a mapping is automatically created for each interface's subnet (except WAN). If you use target addresses other than the WAN interface's IP address, then depending on the way your WAN connection is setup, you may also need a Virtual IP.
You may enter your own mappings below.
Interface
Source
Source Port
Destination
Destination Port
NAT Address
NAT Port
Static Port
Description
WAN
192.168.1.0/24
*
*
*
*
*
NO
Auto created rule for LAN
pfSense is © 2004-2006 by Scott Ullrich. All Rights Reserved. [view license]


pfSense
webConfigurator
pfSense.local
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Aliases
NAT
Rules
Traffic Shaper
Virtual IPs
Firewall: Rules
LAN
WAN
Proto
Source
Destination
Port
Gateway
Description
No rules are currently defined for this interface.
All incoming connections on this interface will be blocked until you add pass rules.
Click the button to add a new rule.
pass
pass (disabled)
block
block (disabled)
reject
reject (disabled)
log
log (disabled)
Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.
pfSense is © 2004-2006 by Scott Ullrich. All Rights Reserved. [view license]

3. Despues ingresamos al submenú Rules desde el menú Firewall ubicado en la barra de menús de la interfaz gráfica de configuración del PFSense.

4. Al ver que no tenemos ninguna regla configurada podemos visualizar que están las dos interfaces LAN y WAN, en la parte inferior se encuentran las convenciones que indican cada uno de los estados de la regla:

PASS Permitir

PASS (Disabled) Permitir Deshabilitado

BLOCK Bloquear

BLOCK (Disabled) Bloquear Deshabilitado

Reject Rechazar

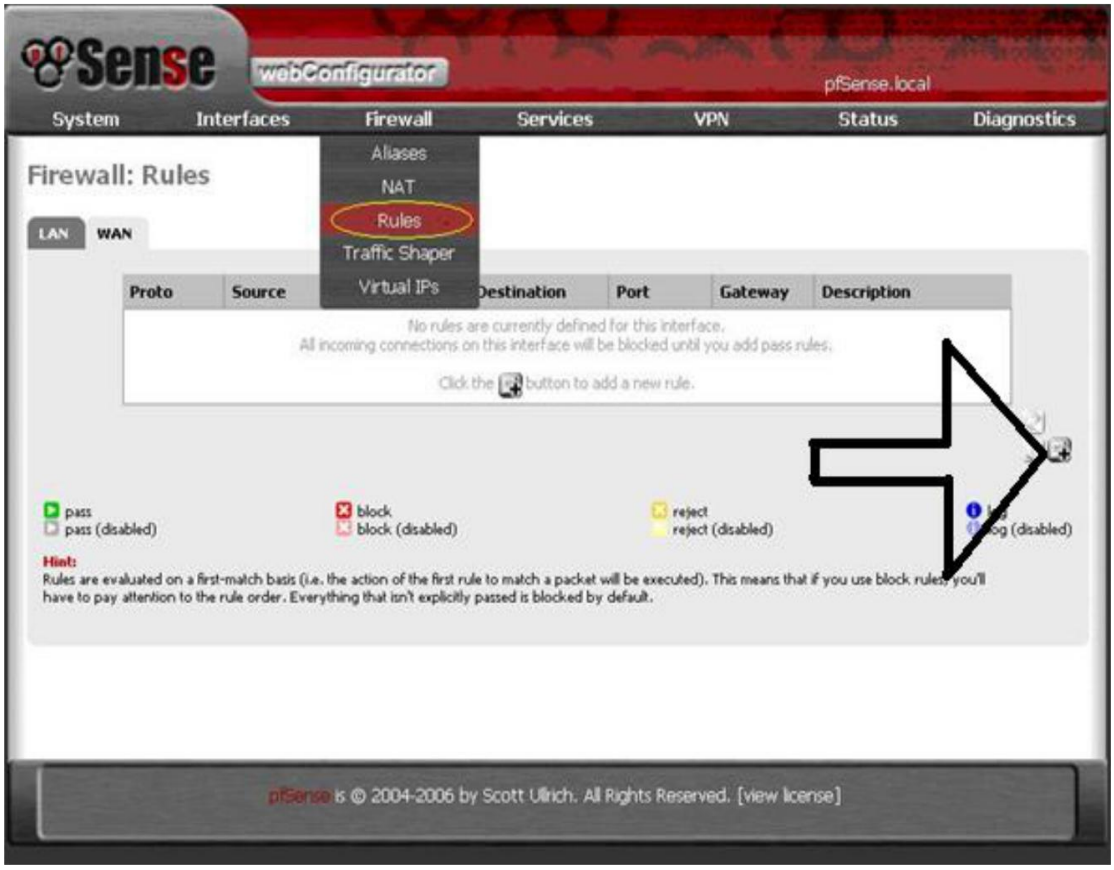
Reject (Disabled)

Log Hacer seguimiento en archivo de log

Log (Disabled) Hacer seguimiento en archivo de log deshabilitado

Si se bloquea, simplemente se ignora el paquete de información que se está recibiendo. Si se rechaza, se comunica al emisor que no se quiere el paquete. Por tanto, normalmente se bloquea. ¿Por qué? Pues porqué bloquear es silencioso, es no hacer caso al emisor y nada más.

5. la parte derecha de la pantalla de pfsense hay un icono que dice agregar nueva regla con la siguiente forma damos clic ahí para crear una nueva regla de firewall



6. Luego nos saldrá una pantalla con los siguientes parámetros los cuales serán definidos a continuación:

Action: Permite seleccionar que hacer con los paquetes que coinciden con el criterio seleccionado debajo en las siguientes opciones de filtrado (pass, blocked, Reject)

Disabled: Permite deshabilitar temporalmente esta regla sin ser eliminada, esto con el objetivo de administración de la red y gestión de servicios de red.

Interface: En este campo se configura a que interfaz ira aplicada la regla de firewall ya sea LAN, WAN, O DMZ

Protocol: Especifica que protocolo de capa 4 se va a utilizar en el filtrado de paquetes en la regla de firewall (TCP, UDP, ICMP)

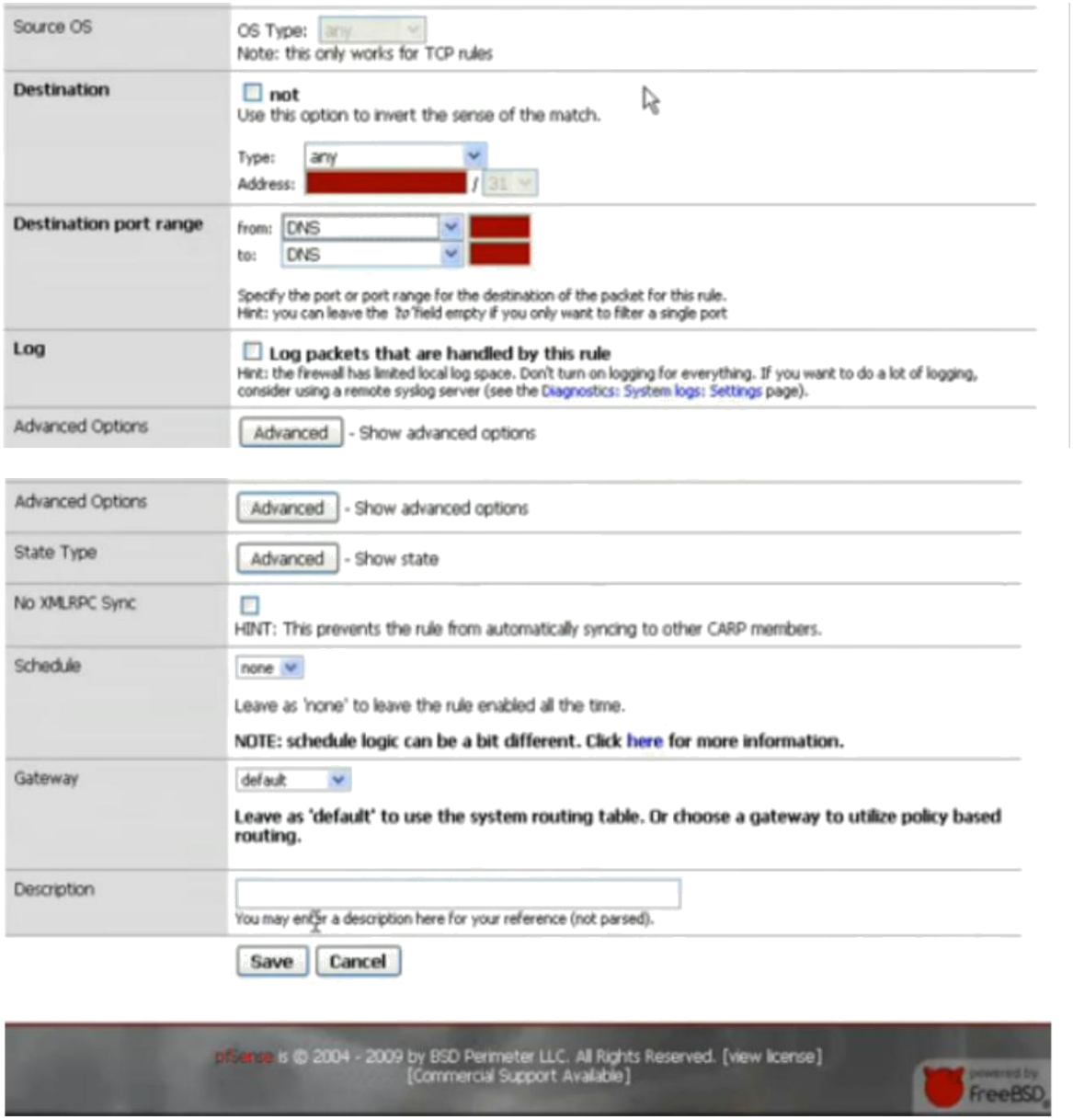
Source: Aquí se configura la dirección de red, o de host origen y en avanzadas se coloca el puerto de origen adicional al origen

Source OS: En esta opción se puede filtrar el sistema operativo el cual solo funciona con el protocolo TCP

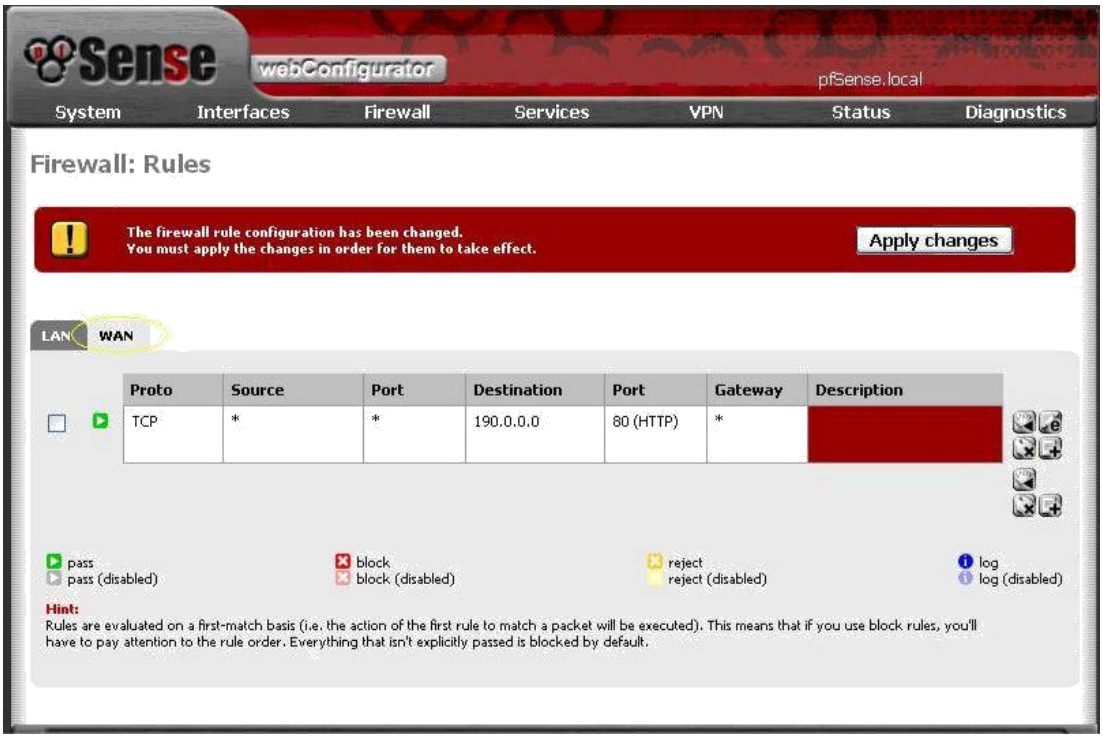
Destination: Es la dirección de red, o de host de destino donde llegara el paquete y también tiene las mismas opciones avanzadas de configuración por puerto.

Destination Log: Selecciona los rangos de puertos para la entrega de paquetes en esta regla por protocolo de capa 7


System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Firewall: Rules: Edit
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
LAN
Choose on which interface packets must come in to match this rule.
Protocol
TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.
Source
not
Use this option to invert the sense of the match.
Type:
any
Address:
/ 31
Advanced
- Show source port range
Source OS
OS Type:
any
Note: this only works for TCP rules
Destination
not



7. Por ultimo damos clic en el botón Save y nos saldrá esta pantalla indicándonos el resumen de los parámetros de configuración de la regla, después damos clic en guardar en la parte superior de la pantalla. En el botón que dice Apply Changes. Aquí podemos apreciar los parámetros mencionados anteriormente con el estado de la regla que en este caso está en color verde.


pfSense
webConfigurator
pfSense.local
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Firewall: Rules
The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.
Apply changes
LAN
WAN
Proto
Source
Port
Destination
Port
Gateway
Description
TCP
*
*
190.0.0.0
80 (HTTP)
*
pass
pass (disabled)
block
block (disabled)
reject
reject (disabled)
log
log (disabled)
Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.