



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE INFORMÁTICA Y ELECTRÓNICA
ESCUELA DE INGENIERÍA EN SISTEMAS

**“ANÁLISIS COMPARATIVO DE HERRAMIENTAS N.A.C OPENSOURCE Y
SU APLICACIÓN A LA DIRECCIÓN PROVINCIAL DEL CONSEJO DE LA
JUDICATURA DE CHIMBORAZO”**

TESIS DE GRADO

**Previa la obtención del título de
INGENIERO EN SISTEMAS INFORMÁTICOS**

**Presentado por:
CARLOS MIGUEL PADILLA CEVALLOS**

RIOBAMBA – ECUADOR

2012

AGRADECIMIENTO

Agradezco infinitamente a Dios por ser la luz y la fuerza de mi vida, a mis padres por su apoyo incondicional y el sacrificio que han hecho por darme una educación; a mis hermanos y amigos por sus consejos y aprecio.

DEDICATORIA

A Dios y a mis padres por los buenos valores, hábitos y enseñanzas que me han ayudado a salir adelante y alcanzar mis sueños y objetivos. A mi novia por sus consejos, comprensión y apoyo. También a mis hermanos por siempre darme fuerza para seguir adelante.

NOMBRE

FIRMA

FECHA

Ing. Iván Ménes

**DECANO FACULTAD DE
INFORMÁTICA Y
ELECTRÓNICA**

.....

.....

Ing. Raúl Rosero

**DIRECTOR ESCUELA
INGENIERÍA EN
SISTEMAS**

.....

.....

Ing. Alberto Arellano

DIRECTOR DE TESIS

.....

.....

Ing. Diego Ávila

**MIEMBRO DEL
TRIBUNAL**

.....

.....

Ing. Carlos Rodríguez

**DIRECTOR DPTO.
DOCUMENTACIÓN**

.....

.....

NOTA DE LA TESIS

.....

Yo Carlos Miguel Padilla Cevallos, soy responsable de las ideas vertidas en esta tesis y el patrimonio intelectual pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

Carlos Miguel Padilla Cevallos

ÍNDICE GENERAL

AGRADECIMIENTO

DEDICATORIA

CAPITULO I

MARCO REFERENCIAL.....	16
1.1 ANTECEDENTES.....	16
1.2 JUSTIFICACIÓN DEL PROYECTO DE TESIS.....	20
1.2.1 Justificación Teórica.....	20
1.2.2 Justificación Aplicativa	21
1.3 OBJETIVOS	22
1.3.1 Objetivo General	22
1.3.2 Objetivos Específicos	23
1.4 HIPÓTESIS.....	23
1.5 MÉTODOS Y TÉCNICAS	23
1.5.1 Métodos	23
1.5.2 Técnicas.....	24

CAPITULO II

MARCO TEÓRICO CONCEPTUAL.....	25
2.1 INTRODUCCIÓN	25
2.2 HERRAMIENTAS NAC OPENSOURCE.....	27
2.2.1 Redes De Autodefensa	28
2.2.2 Control De Admisión A La Red.....	29
2.2.3 Objetivos De NAC.	30
2.2.4 Conceptos De NAC.	30
2.2.5 Características De NAC.	32
2.2.6 Arquitectura General De NAC.	33
2.2.7 CICLO DE NAC.	37
2.3 HERRAMIENTAS OPENSOURCE NETWORK ADMISSION CONTROL	51

2.3.1 FREENAC.....	51
2.3.2 PACKETFENCE.....	58
2.4 POLÍTICAS DE SEGURIDAD	70
2.4.1 Políticas De Seguridad Local	70
2.4.2 Objetivos De Las Políticas De Seguridad	70
2.4.3 Componentes De Las Políticas De Seguridad	71
2.4.4 Elementos De Una Política De Seguridad Informática	72
2.4.5 Parámetros Para Establecer Políticas De Seguridad.....	72
2.5 ACERCAMIENTO A LAS POLÍTICAS DE SEGURIDAD.....	73
2.5.1 Análisis De Riesgo	75
2.5.2 Identificación De Los Recursos.....	75
2.5.3 Identificación De Amenazas.....	76
2.5.4 Cálculo Del Riesgo.....	76
2.6 USO Y RESPONSABILIDADES EN LA RED.....	77
2.6.1 Identificando A Quien Es Permitido El Uso De Recursos De La Red.....	78
2.6.2 Identificando El Uso Apropiado De Un Recurso.	78
2.6.3 Determinando Quien Está Autorizado Para Otorgar Acceso Y Aprobar El Uso.....	79
2.6.4 Determinando Las Responsabilidades De Los Usuarios.....	81
2.6.5 Determinando Las Responsabilidades Del Administrador Del Sistema.	81
2.7 PLAN DE ACCIÓN CUANDO LAS POLÍTICAS DE SEGURIDAD SON VIOLADAS	82
2.7.1 Respuesta A Violaciones Por Parte De Usuarios Internos	82
2.7.2 Respuesta A Violaciones Por Parte De Usuarios Externos	83
2.7.3 Estrategias De Respuesta.....	83
2.7.4 Contactos Y Responsabilidades Con Organizaciones Externas.	86

CAPITULO III

ANÁLISIS COMPARATIVO DE	87
HERRAMIENTAS NAC OPENSOURCE	87
3.1 ANÁLISIS DE LA INFRAESTRUCTURA DE RED DE LA INSTITUCIÓN.	87
3.1.1 Subredes	89
3.1.2 Equipos de la Institución	90
3.2 IMPLEMENTACIÓN DE HERRAMIENTAS NAC OPENSOURCE EN UN AMBIENTE DE PRUEBAS	92
3.2.1 Pruebas Con La Herramienta FreeNAC	92
3.2.2 Pruebas Con La Herramienta Packetfence	111
3.3 DEFINICIÓN DE LOS PARÁMETROS DE COMPARACIÓN	118
3.4 DEFINICIÓN DE ESCALAS	119
3.5 Análisis Comparativo de Herramientas NAC	119

CAPITULO IV

POLÍTICAS DE RED E IMPLEMENTACIÓN DE LA HERRAMIENTA NAC OPENSOURCE EN LA DIRECCIÓN PROVINCIAL DEL CONSEJO DE LA JUDICATURA DE CHIMBORAZO.	133
4.1 Políticas de Red	133
4.1.2 Análisis de Riesgo	136
4.1.3 Conclusiones del Análisis de Riesgos.	139
4.1.4 Usos y Responsabilidades de la Redes Institucionales	140
4.1.5 Plan de acción ante violación de políticas de seguridad	144
4.1.6 Conclusiones	147
4.2 Implementación De La Herramienta Y Su Aplicación A La Dirección Provincial Del Consejo De La Judicatura De Chimborazo.	148
4.2.1 Administración de la Herramienta	148
4.3 COMPROBACIÓN DE LA HIPÓTESIS	177
4.3.1 Hipótesis de investigación	177

4.3.2 Tipo de Hipótesis.....	177
4.3.3 Población y Muestra	177
4.3.4 Determinación de Variables	177
4.3.5 Comprobación de la hipótesis de investigación	179

CONCLUSIONES

RECOMENDACIONES

RESUMEN

ABSTRACT

ABREVIATURAS Y ACRÓNIMOS

ANEXOS

BIBLIOGRAFÍA DE INTERNET

ÍNDICE DE FIGURAS

Figura II.01: Arquitectura General de NAC	36
Figura II.02: Ciclo de NAC	38
Figura II.03: NAC en línea.	48
Figura II.04: NAC fuera de banda.	49
Figura II.05: Arquitectura de FREENAC.	52
Figura II.06: Arquitectura de Packetfence.	63
Figura III.01: Infraestructura de Red Actual para la Institución.....	88
Figura III.02: Ambiente de Pruebas de NAC.....	92
Figura III.03: Ejecución de interfaz de Escritorio	92
Figura III.04: Configuración de Ingreso a FreeNac.....	93
Figura III.05: Interfaz para la administración de FreeNac.....	93
Figura III.06: Pantalla inicial de FreeNac.....	94
Figura III.07: Edición de Dispositivos Finales.	94
Figura III.08: Administración de Switchs.....	95
Figura III.09: Administración de Puertos de los Switchs.	95
Figura III.10: Registro de Acceso a la interfaz de Administración.	96
Figura III.11: Registro de Sucesos del Servidor.	96
Figura III.12: Administración dinámicas de Vlans.....	97
Figura III.13: Reinicio de la Herramienta.....	97
Figura III.14: Configuración de la Herramienta.	98
Figura III.15: Escaneo de Subredes.	98
Figura III.16: Configuración de Ubicaciones Físicas.	99
Figura III.17: Configuración de tipos de Dispositivos.	99
Figura III.18: Configuración de la Herramienta.	100
Figura III.19: Configuración de Usuarios.....	100
Figura III.20: Reportes de la Herramienta.	101
Figura III.21: Enlaces para Soporte Web.....	101
Figura III.22: Página de Inicio de FreeNac.....	102
Figura III.23: Reporte Inicial de Dispositivos Detectados.	102
Figura III.24: Agregación de Dispositivos.	103
Figura III.25: Búsqueda de Dispositivos Finales.....	103
Figura III.26: Grafica de Dispositivos Detectados.	104

Figura III.27: Grafica de Sistemas Operativos Detectados.....	104
Figura III.28: Grafica de Hardware Detectado.	105
Figura III.29: Configuración de los Puertos del Switch.	105
Figura III.30: Configuración del Switch.....	106
Figura III.31: Configuración de Vlans para Administración Dinámica.	106
Figura III.32: Listado de Usuarios.....	107
Figura III.33: Búsqueda de Ubicaciones.....	107
Figura III.34: Configuración de Nmap.	108
Figura III.35: Configuración de los Tipos de Dispositivos.	108
Figura III.36: Reporte de Sucesos de la herramienta.....	109
Figura III.37: Reporte de Sucesos de Ingreso al Sistema.	109
Figura III.38: Reporte de Sucesos Generales.....	110
Figura III.39: Reporte de Información del Sistema.	110
Figura III.40: Página de Ingreso a PacketFence.	111
Figura III.41: Página de Inicio de PacketFence.....	111
Figura III.42: Estado de Nodos de la Red LAN.....	112
Figura III.43: Grafico del Estado de los Nodos en la Red LAN.....	112
Figura III.44: Grafica del Total de Nodos.	113
Figura III.45: Grafica del Total de Nodos No Registrados.....	113
Figura III.46: Grafica de Violaciones Detectadas por Día.	114
Figura III.47: Página de Usuarios Registrados.	114
Figura III.48: Agregar Usuarios.....	115
Figura III.50: Importación de Nodos.	116
Figura III.51: Reporte de Violaciones (abiertas o cerradas).....	116
Figura III.52: Administración de Servicios que utiliza PacketFence.	117
Figura III.53: Configuración de Todas las Opciones PacketFence.	117
Fig.III.54 Grafica de Resultados de Usabilidad.....	120
Fig.III.55 Grafica de Resultados de Gestión y Administración de Usuarios.....	122
Fig.III.56 Grafica de Resultados de Administración de Switchs.....	123
Fig.III.57 Grafica de Resultados de Auto Descubrimiento de Dispositivos.....	124
Fig.III.58 Grafica de Resultados del Analisis de Politicas de Red.	126
Fig.III.59 Grafica de Resultados del Analisis yDetección de Vulnerabilidades.....	127

Fig.III.60 Grafica de Resultados del Analisis de Sporte.....	129
Figura III.61: Grafico Comparativo de Herramientas NAC.	131
Figura IV.1: Backbone Edificio Principal de la Institución.....	138
Figura IV.2: Interfaz principal para la administración de usuarios.	149
Figura IV.3: Añadir usuarios.	149
Figura IV.4: Información detallada de usuarios.	150
Figura IV.5: Interfaz principal para la administración de dispositivos.....	151
Figura IV.6: Categorías de dispositivos finales.	152
Figura IV.7: Edición de Categorías.	152
Figura IV.8: Edición de Categorías.	153
Figura IV.9: Eliminación de Categorías.	153
Figura IV.10: Visualización de información de los dispositivos.....	154
Figura IV.11: Agregación manual de los dispositivos.....	155
Figura IV.12: Visualización navegadores utilizados por los dispositivos finales.	155
Figura IV.13: Página para la edición de dispositivos.	156
Figura IV.14: Interfaz principal de violaciones de seguridad.....	157
Figura IV.15: Añadir violaciones de forma manual.	157
Figura IV.16: Administración de Servicios.	158
Figura IV.17: Configuraciones de Alertas.	159
Figura IV.18: Configuraciones ARP.	159
Figura IV.19: Configuración de la dirección del Portal Captivo.	160
Figura IV.20: Configuración de la conexión a la Base de Datos.....	160
Figura IV.21: Configuración del servicio DHCP.	161
Figura IV.22: Configuración de parámetros de red.	161
Figura IV.23: Configuración de puertos de Red.....	162
Figura IV.24: Configuración de dirección de antivirus.	162
Figura IV.25: Configuración de las opciones de registro.	163
Figura IV.26: Configuración de las opciones de Escaneo.....	163
Figura IV.27: Configuración de ubicaciones de servicios.....	164
Figura IV.28: Configuración del servicio de vigilancia.....	164
Figura IV.29: Configuración del servicio de captura de dispositivos.....	165
Figura IV.30: Configuración de la administración de Vlans.....	165

Figura IV.31: Configuración de las interfaces de red.	166
Figura IV.32: Configuración de redes de cuarentena y registro.	166
Figura IV.33: Edición de configuración de la red de cuarentena.	167
Figura IV.34: Edición de configuración de la red de registro.	167
Figura IV.35: Interfaz principal de configuración de switchs.	168
Figura IV.36: Interfaz principal de configuración de switchs.	169
Figura IV.37: Configuración de dispositivos de acceso móvil.	170
Figura IV.38: Configuración de políticas de seguridad.	170
Figura IV.39: Actualización de firmas de sistemas operativos.	171
Figura IV.40: Interfaz de agentes de usuario.	171
Figura IV.41: Configuración de plantillas del portal captivo.	172
Figura IV.42: Pantalla principal de reportes.	172
Figura IV.43: Reporte de direcciones IP's asignadas a una dirección MAC.	173
Figura IV.44: Reporte de localización de un equipo por dirección MAC.	173
Figura IV.45: Reporte de dispositivos activos.	174
Figura IV.46: Reporte de dispositivos inactivos.	174
Figura IV.47: Reporte de tipo de conexiones.	175
Figura IV.48: Grafico de dispositivos totales.	175
Figura IV.49: Grafico de nodos no registrados.	176
Figura IV.50: Grafico de violaciones.	176

ÍNDICE DE TABLAS

Tabla II.I: Arquitecturas de NAC	34
Tabla II.II: Métodos de Evaluación de NAC	39
Tabla II.III: Métodos de Autenticación NAC	44
Tabla II.I: Formato para establecer Políticas de Seguridad.	74
Tabla II.II: Recursos de la Red	77
Tabla II.III: Recursos de la Red.....	80
Tabla III.I: Subredes de la Red de la Institución	89
Tabla III.II: Rangos de Direccionamiento de la Institución	90
Tabla III.III: Servidores de NAC.	90
Tabla III.IV: Dispositivos de Conectividad de la Institución Ed. Principal.	91
Tabla III.V: Dispositivos de Conectividad de la Institución Ed. Nuevo.	91
Tabla III.VI: Parámetros de Comparación.....	118
Tabla III.VII: Definición de Escalas.....	119
Tabla III.VIII: Valoración del Parámetro Usabilidad.	119
Tabla III.IX: Valoración del Parámetro Gestión y Administración de Usuarios.....	121
Tabla III.X: Valoración del Parámetro Administración de Switchs.	122
Tabla III.XI: Autodescubrimiento Dispositivos y Recolección de Información en Tiempo Real.....	123
Tabla III.XII: Valoración del Parámetro Administración de Switchs.	125
Tabla III.XIII: Valoración del Parámetro Análisis y Detección de Vulnerabilidades..	126
Tabla III.XIV: Valoración del Parámetro Soporte.....	128
Tabla III.XV: Valoración del Parámetro Reportes.	129
Tabla III.XVI: Resumen Comparativo de Herramientas.	130
Tabla IV.I: Tabla de Terminología.	137
Tabla IV.II: Resultados del Análisis de Riesgo del Backbone.	138
Tabla IV.II: Usuarios autorizados para utilizar los recursos.	142
Tabla IV.IV: Operacionalización Conceptual.....	178
Tabla IV.V: Operacionalización metodológica.	178
Tabla IV.VI: Distribución de X.	180
Tabla IV.VII: Resultados de Factibilidad.	181
Tabla IV.VIII: Resultados de Gestión.	181

Tabla IV.IX: Resultados de Usabilidad.	181
Tabla IV.X: Resultados de Seguridad.....	181
Tabla IV.XI: Resultados de Productividad.	182
Tabla IV.XII: Matriz de resultados totales de la encuesta.	182
Tabla IV.XIII: Matriz de resultados esperados.....	183
Tabla IV.XII: Frecuencia observada sobre frecuencia esperada.	183

CAPITULO I.

MARCO REFERENCIAL

1.1 ANTECEDENTES

Control de acceso a red (del inglés NAC) es un enfoque de seguridad en redes de computadoras que intenta unificar las tecnologías de seguridad (tales como antivirus, prevención de intrusión en hosts, informes de vulnerabilidades, etc.) en los equipos finales, usuarios o sistemas de autenticación y reforzar la seguridad de la red.

NAC es usado para definir como asegurar los nodos de la red antes de que estos accedan a esta; Este mecanismo de protección abarca varias tecnologías que permiten a las empresas garantizar la imposición de las políticas de seguridad corporativas a los puntos finales conectados a sus redes. Estas políticas de seguridad para puntos finales, pueden exigir, por ejemplo, que los dispositivos tengan completamente actualizados los parches de seguridad o las herramientas antivirus.

También pueden haber sido definidas para prevenir la utilización de determinadas aplicaciones, como la compartición de ficheros peer-to-peer (P2P) o la mensajería instantánea. Es decir, determinan el estado y el comportamiento permitido por la empresa a los puntos finales conectados a sus redes.

Las instituciones públicas como la Dirección Provincial del Consejo de la Judicatura de Chimborazo cada vez necesitan métodos más eficaces para proteger sus operaciones de amenazas como hackers externos e internos, para combatir virus y gusanos que infectan los dispositivos finales a través de la red, y para controlar el acceso de sus empleados, clientes y asociados a los datos y las aplicaciones internas; también se debe tener en cuenta que las instituciones manejan ahora la política de software libre para mejorar los costes y gestión de la tecnología.

Es algo común, ya sea por política interna, por la tolerancia al riesgo, porque trabajemos en un sector regulado o por cualquier otra razón: las instituciones públicas deben aprender a elegir entre un elevado nivel de seguridad, o una mayor usabilidad.

Anteriormente la institución contaba con el suficiente cableado estructurado de tipo Ethernet, pero actualmente con la creciente demanda de servicios por parte de la ciudadanía ha surgido la necesidad de aumentar el número de dependencias de justicia y por ende el número de equipos finales lo que ha llevado al uso de Switchs no manejados que ofrecen poca seguridad, los cuales dan más facilidades para la conexión de dispositivos no autorizados.

La mayoría de sistemas que se manejan dentro de la institución utilizan servicios y recursos de la red como son: El sistema SATJE que es el sistema que registra las acciones de todos los funcionarios judiciales para llevar un registro de los trámites judiciales;

El sistema de Pensiones que maneja el registro de las transacciones bancarias referentes a las pensiones alimenticias. El Sistema de Activos Fijos para llevar el control contable de la institución.

El Sistema de Control de Personal que maneja las entradas, salidas, permisos y vacaciones mediante relojes biométricos conectados a un servidor que registra toda las acciones del personal. Otro recurso de red que utilizan es el correo institucional que también sirve para

comunicaciones internas debido a una política de ahorro de recursos sobre todo de papelería y de impresión, además este servicio también funciona para enviar mensajes externos.

También poseen sistemas de información de juicios y de pensiones alimenticias que utilizan los usuarios para consultar el estado de sus trámites judiciales. La institución cuenta también con el servicio de internet que se da a los funcionarios judiciales para que hagan consultas de leyes a través del sistema FIELWEB que es una base de datos de leyes que se encuentra publicada a nivel nacional.

Por estas razones, las personas encargadas de la unidad informática desean saber qué es lo que se conecta a su red, dónde, cuándo, que servicios y protocolos utilizan con el fin de prevenir riesgos eventuales de seguridad introducidos por usuarios ya sean inconscientes o maliciosos, utilizar programas que consumen muchos recursos de red (descargas, música por internet, chat, etc.), introducir un virus ya sea intencionalmente o no, para perturbar el funcionamiento de la red, ver los datos que transitan por la red, o acceder a datos o recursos internos confidenciales;

Este problema crea una brecha de seguridad importante para la redes de la institución puesto que de estos equipos se puede ingresar a servicios y equipos sensibles como servidores además pueden tener mucho tiempo para realizar un ataque interno y capturar los datos críticos de sistemas y servicios (información de juicios, tramites, sentencias, correo, etc.) de la red; además la institución se encuentra conectada a las redes de los cantones y provincias del resto del país por lo cual puede tener acceso a la red WAN comprometiendo aún más la seguridad;

Los virus y gusanos informáticos que ingresan por medio de memorias flash utilizadas por los usuarios la mayor parte continúan la infección por medio de las redes LAN a las que tienen acceso; Se pretende evitar esto con la tecnología NAC. Las seguridades

implementadas en la Unidad Informática de la institución como son firewalls y proxys son implementados para evitar los ataques externos, más para evitar los ataques internos.

Para solucionar este problema de seguridad dentro la institución se plantea analizar y aplicar la tecnología NAC con herramientas OpenSource en la plataforma Linux para seguir la política gubernamental de SW libre y así cumplir con los requisitos que rigen en las instituciones públicas para tratar de reducir costos en el área informática. Para aplicar NAC en la institución se debe elegir la herramienta adecuada para poder controlar el acceso a la LAN.

Algunas herramientas NAC OpenSource son:

FreeNAC.- es una solución de Open Source (GLP) para el control de acceso LAN y administración dinámica de VLAN's. Ofrece asignación simplificada de redes virtuales, control de acceso a redes (para todo tipo de dispositivos de red tales como Servidores, Estaciones de trabajo, Impresoras, Teléfonos IP, Webcams, etc.), inventario de dichos dispositivos de red, y permite también documentar el cableado.

PacketFence.- es totalmente compatible, confiable, libre y de código abierto para el control de acceso de red (NAC). Con un impresionante sistema incluyendo un portal cautivo para el registro y la habilitación de usuarios, la gestión centralizada de redes cableadas e inalámbricas, soporte 802.1X, dispositivos de capa 2, aislamiento de problemas, integración con el IDS Snort y el escáner de vulnerabilidades Nessus; PacketFence se puede utilizar con eficacia en seguridad de redes desde pequeñas a grandes redes heterogéneas.

Hupnet.- es para uso en redes inalámbricas (WLAN), pero funciona también en redes Ethernet cableadas. Cualquier método de autenticación de WWW se pueden utilizar en el programa de entrada cgi, especialmente Shibboleth, pero otros métodos de autenticación tales como PubCookie, LDAP y RADIUS también se pueden utilizar, la opción más simple

es "htpasswd" contraseñas de Apache (útil para probar la puerta de entrada Hupnet sin los debidos métodos de autenticación, puede ser complicado de configurar).

NetReg.- proporciona a los administradores una plataforma central para la gestión y administración del direccionamiento IP y la información relacionada con la red. NetReg mantiene una base de datos de información de la subred, zonas DNS, las opciones de DHCP, los registros de la máquina, y mucho más. Tiene un mecanismo de control de acceso de refinado para proporcionar a los administradores la flexibilidad máxima en la delegación de acceso.

1.2 JUSTIFICACIÓN DEL PROYECTO DE TESIS

1.2.1 Justificación Teórica

Network Admission Control es una tecnología relativamente nueva que está tomando fuerza en el ámbito de las seguridades de redes informáticas para asegurar, controlar y administrar los servicios y recursos críticos de las redes LAN tomando en cuenta políticas de seguridad de las instituciones y empresas sin tomar en cuenta el tamaño de las mismas.

La empresa líder en redes de computadoras Cisco creo e impulso el desarrollo de la tecnología NAC para el aseguramiento de ambientes LAN. Gracias a la liberación del código fuente de esta tecnología por parte de Cisco han nacido algunas herramientas de OpenSource para la utilización de esta tecnología. Por esta razón no se tiene una adecuada documentación para instalar, configurar y administrar apropiadamente esta tecnología.

NAC es una tecnología importante en el ámbito de las seguridades informáticas, permite mitigar ataques de día cero a equipos finales por la falta de antivirus, parches, o software de prevención de intrusión de hosts y acceder así a la red poniendo en riesgo a otros equipos de contaminación y expansión de gusanos informáticos. Permite a los

operadores de red definir políticas, tales como tipos de computadores o roles de usuarios con acceso permitido a ciertas áreas de la red, y forzarlos en switches y routers. Permite controlar los servicios y aplicaciones que acceden a los recursos de la red LAN.

Se plantea el análisis de herramientas NAC en ambientes LAN para así realizar una investigación completa y adecuada de esta tecnología y así poder recopilar y generar la información necesaria para la aplicación de esta tecnología.

1.2.2 Justificación Aplicativa

La Dirección Provincial del Consejo de la Judicatura de Chimborazo para brindar un mejor servicio a la ciudadanía actualmente cuenta con algunos sistemas que utilizan la red para realizar las transacciones correspondientes; los cuales son: Sistemas para el Registro de todos los trámites de la Administración de Justicia y para la consulta de causas que ingresan a la institución denominado SATJE, el sistema para el cobro de pensiones alimenticias, sistema de proveeduría, sistema de activos fijos, Sistema de Control de Personal además de poseer el servicio de correo institucional y páginas web informativas.

En algunas ocasiones la red institucional ha sufrido congestión de servicios y aplicaciones debido al gran número de usuarios que utilizan el sistema y las aplicaciones que instalan en su tiempo libre para mejorar el control y la administración de la institución se desea implementar la tecnología NAC con herramientas OpenSource. Aunque parece no haber registro de algún ataque externo o interno a los servicios o datos la institución nunca está por demás prevenir cualquier problema en el futuro sobre todo cuando se trata de seguridad.

La institución no ha realizado estudios referentes al uso de herramientas de Administración y Control de la red y cabe reiterar que las tendencias actuales apuntan a que los sistemas de seguridad para redes se constituyen en una parte esencial de las arquitecturas de redes empresariales, al contar la institución con varias aplicaciones que

utilizan servicios de red, hace que su administración sea una pieza clave para garantizar la disponibilidad y el grado de servicio requerido para la red.

En este sentido, se realizara el Análisis e Implementación de Herramientas NAC OpenSource para la administración y control de acceso a la red LAN de la Dirección Provincial del Consejo de la Judicatura de Chimborazo, que sirva para ayudar a controlar y asegurar los dispositivos de red, dando seguimiento a todos los eventos ocurridos en los dispositivos de red, garantizando así la explotación eficiente de los recursos de la institución y así lograr mejorar el servicio.

Para elegir la herramienta NAC OpenSource adecuada se plantea realizar un ambiente de pruebas en la propia institución mediante el uso de VLANs. Se creará una VLAN especial donde se realizara las pruebas de las herramientas en la red de la institución, los datos tomados del análisis comparativo de las herramientas serán los más cercanos a la realidad puesto que al tener una VLAN dentro de la red institucional se podrá usar sistemas y equipos propios de la institución, además de utilizar los recursos de la red. De esta manera se podrá elegir adecuadamente la herramienta que satisfaga las necesidades de la institución y sin interferir con el trabajo diario de los funcionarios públicos.

1.3 OBJETIVOS

1.3.1 Objetivo General

- Realizar un análisis comparativo de herramientas NAC OpenSource para aplicar a la Dirección Provincial del Consejo de la Judicatura de Chimborazo para mejorar el control de acceso a los recursos de información institucionales.

1.3.2 Objetivos Específicos

- Investigar en qué consiste NAC y las herramientas OpenSource que permita entender el funcionamiento de la tecnología en una red LAN.
- Elegir la herramienta NAC OpenSource más adecuada para aplicar en la red de la Institución mediante la realización de un ambiente de pruebas.
- Aplicar la herramienta NAC seleccionada para administrar y mejorar el acceso y control a la red LAN de la institución.
- Determinar las políticas de seguridad que se deben incorporar en la institución para asegurar los ambientes LAN.

1.4 HIPÓTESIS

La utilización de herramientas Network Admission Control OpenSource en la Dirección Provincial del Consejo de la Judicatura de Chimborazo mejorara el control de admisión a los recursos críticos de la LAN.

1.5 MÉTODOS Y TÉCNICAS

1.5.1 Métodos

El método utilizado como guía para la presente investigación es el método Científico, el cual contempla los siguientes puntos:

1. El planteamiento del problema que es objeto principal de nuestro estudio.
2. El apoyo del proceso previo a la formulación de la Hipótesis.
3. Levantamiento de información necesaria.
4. Análisis e interpretación de Resultados.
5. Proceso de Comprobación de la Hipótesis, etc.

Además, se aplicará el método analítico que permitirá dividir el objeto de estudio en partes de información de sus componentes.

1.5.2 Técnicas

Para la recopilación de la información necesaria que sustente el presente trabajo de investigación, se ha establecido como técnicas las siguientes:

- Revisión de Documentos
- Observación
- TFA'S (Técnicas que facilitan la especificación de aplicaciones)
- Técnicas de Comprobación de hipótesis.

CAPITULO II.

MARCO TEÓRICO CONCEPTUAL

2.1 INTRODUCCIÓN

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan han llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para

establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

La seguridad informática va adquiriendo una importancia creciente con el aumento del volumen de información importante que se halla en las computadoras distribuidas. En este tipo de sistemas resulta muy sencillo para un usuario experto acceder subrepticamente a datos de carácter confidencial. La norma Data Encryption System (DES) para protección de datos informáticos, implantada a finales de los años setenta, se ha visto complementada recientemente por los sistemas de clave pública que permiten a los usuarios codificar y descodificar con facilidad los mensajes sin intervención de terceras personas.

Actualmente existe una creciente dependencia de las redes de computadoras para las transacciones de negocios. Como resultado, las nuevas prácticas en los negocios llevan una multitud de cambios en todas las facetas de las redes de una empresa. Por ello prevalece la seguridad en la red mientras, las empresas intentan comprender y administrar los riesgos asociados con el rápido desarrollo de las aplicaciones de negocios y de las prácticas que se despliegue en relación a las infraestructuras de la red. Con el flujo libre de información y la gran disponibilidad de muchos recursos, los administradores de las empresas deben conocer todas las amenazas posibles para sus redes. Dichas amenazas toman muchas formas pero el resultado es siempre la pérdida de la privacidad y posibilidad de destrucción de la información.

Es necesario el uso restringido del equipo de infraestructura de la red y de los recursos críticos. Limitar el acceso a la red a solo los que tengan permitido, es una manera inteligente de detener muchas amenazas que pueden abrir una brecha en la seguridad de las redes de computadoras. No todas las amenazas tienen porque ser dañinas, pero pueden tener el mismo comportamiento y causar el mismo daño. Es importante comprender que tipos de ataques y vulneraciones son comunes, y que se pueden hacer al nivel de la naturalización para garantizar la seguridad en la red.

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. “Hackers”, “crackers”, entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes. Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red.

2.2 HERRAMIENTAS NAC OPENSOURCE

La industria de las TIC trabajan intensamente en encontrar soluciones a un problema cada vez más crítico para todo tipo de organizaciones: garantizar que cualquiera que se conecte a la red corporativa sea no sólo identificado y autorizado apropiadamente, sino también que está usando un dispositivo seguro. Un objetivo que, bajo diversas denominaciones y enfoques, representa el cambio más significativo en la seguridad de redes desde la invención de los cortafuegos.

Desde una perspectiva física, en todas las organizaciones hay puntos de acceso por donde las personas autorizadas entran y salen. Las dificultades comienzan cuando esto pasa a un plano lógico, pues los accesos dejan de ser evidentes y sencillos.

Las compañías cuentan con redes cada vez más distribuidas para que los empleados, clientes y proveedores tengan conectividad desde una gran variedad de dispositivos y plataformas. El entorno de la interconexión, por lo tanto, se ha vuelto complejo.

Por si esto fuera poco, a futuro, el aumento de los puntos de acceso expondrá aún más la infraestructura y los activos digitales de las empresas.

La respuesta incipiente frente a este ecosistema de conectividad notoriamente más complicado, consiste en un conjunto de iniciativas tecnológicas agrupadas en torno a nuevos modelos de seguridad. Su nombre genérico es: Control de Acceso a la Red (Network Access Control: NAC, por sus siglas en inglés) o también se lo puede conocer como Network Admission Control.

2.2.1 Redes De Autodefensa

Son las redes típicamente protegidos por una combinación de dispositivos y software que detecta y elimina las amenazas, este tipo de protección trabajó durante muchos años, se hizo más fuerte y más seguro con el tiempo, pero la industria de la seguridad siguió creciendo debido a que las amenazas también estaban cada vez son más fuertes y más inteligentes, y a veces van un paso por delante de la comunidad de seguridad.

No es muy claro cuando el primer virus informático en marcha, pero se sabe que durante los 80's las computadoras de IBM fueron los primeros en verse afectados por un virus de arranque.

En la siguiente etapa de los virus se convirtieron en virus de macros, ataques a DoS, de auto-codificación y transformación, como el virus polimórfico "Camaleón" que apareció en los años 90's. Hoy en día los virus incluyen gusanos, virus troyanos, todo en uno y se pueden propagar en cuestión de minutos. Aquí es cuando las antiguas técnicas de mantener los virus a distancia con sólo dejarlos entrar y la eliminación de ellos tenían que cambiar.

Dado que los virus y los ataques evolucionaron y se diversificaron una nueva necesidad para los dispositivos de seguridad inteligente surgió. Estos así llamados dispositivos y software de "auto-defensa" para tratar de adaptar y cambiar, incluso cuando los ataques se han transformado manteniendo siempre la comunicación y asegurando los datos críticos.

En las redes de Auto-defensa cada dispositivo individual rige su propia seguridad y es capaz de responder a un mundo siempre cambiante de los ataques. En el futuro vamos a tener amenazas que se desplegará en segundos, impulsado por los gusanos masivos, es por eso que necesitamos dispositivos más inteligentes y de adaptación para protección de nuestras redes.

2.2.2 Control De Admisión A La Red.

El Control de Admisión a la Red o Network Admission Control (NAC) es un componente principal de la estrategia global de seguridad denominada Redes de Auto-defensa o Self-Defending Networks. Su objetivo principal es la comprobación del estado de salud del equipo desde el que un usuario intenta acceder a la red, de forma que se permita el acceso sólo a los dispositivos "seguros" y se bloquee la entrada a aquellos equipos que no cumplan con los requisitos mínimos de protección exigidos por la política de seguridad corporativa. Los elementos de red y las aplicaciones utilizadas para comprobar y garantizar el estado adecuado del dispositivo realizan una labor conjunta de protección de la infraestructura, permitiendo o restringiendo el acceso de los dispositivos en función de su identidad y nivel de protección. La solución es aplicable a todos los métodos de acceso: red de área local, red inalámbrica, red de área extensa y accesos remotos ya que se ha desarrollado para los accesos a través de cualquier dispositivo de red: conmutadores, equipos Wi-Fi, routers y concentradores VPN respectivamente.

2.2.3 Objetivos De NAC.

El control de acceso a red (NAC) representa una categoría emergente en productos de seguridad, su definición es controvertida y está en constante evolución.

Los objetivos principales de este concepto se pueden resumir en:

- **Mitigar ataques de día cero.-** El propósito clave de una solución NAC es la habilidad de prevenir en los equipos finales la falta de antivirus, parches, o software de prevención de intrusión de hosts y acceder así a la red poniendo en riesgo a otros equipos de contaminación y expansión de gusanos informáticos.
- **Refuerzo de políticas.-** Las soluciones NAC permiten a los operadores de red definir políticas, tales como tipos de computadores o roles de usuarios con acceso permitido a ciertas áreas de la red, y forzarlos en switches y routers.
- **Administración de acceso e identidad.-** Donde las redes IP's convencionales refuerzan las políticas de acceso con base en direcciones IP, los dispositivos NAC lo realizan basándose en identidades de usuarios autenticados, al menos para usuarios finales de equipos portátiles y escritorio.

2.2.4 Conceptos De NAC.

- **Pre-admisión y Post-admisión.-** Existen dos filosofías de diseño predominantes en NAC, basadas en políticas de refuerzo antes de ganar acceso a la red o después de hacerlo. En el primer caso denominado NAC pre-admisión, las estaciones finales son inspeccionadas antes de permitirles el acceso a la red. Un caso típico de NAC pre-admisión sería el prevenir que equipos con antivirus no actualizados pudieran conectarse a servidores sensibles. Alternativamente, el NAC post-admisión crea decisiones de refuerzo basadas en acciones de usuario después de que a estos usuarios se les haya proporcionado el acceso a la red.

- **Con agente vs sin agente.-** La idea fundamental de la tecnología NAC es permitir a la red tomar decisiones de control de acceso basadas en inteligencia sobre los sistemas finales, por lo que la manera en que la red es informada sobre los sistemas finales es una decisión de diseño clave. Una diferencia clave entre sistemas NAC es si requieren agentes software para informar de las características de los equipos finales, o si por el contrario utilizan técnicas de escaneo e inventariado para discernir esas características remotamente.
- **Solución, cuarentena y portal cautivo.-** Los administradores de sistemas y redes despliegan productos NAC con la esperanza de que a algunos clientes legítimos se les denegará el acceso a la red (si los usuarios nunca tuvieron antivirus desactualizados y sus sistemas están siempre actualizados, NAC no sería necesario). Por ello las soluciones NAC requieren de un mecanismo para remediar el problema del usuario final que le ha sido denegado el acceso a la red.

Las dos estrategias comunes para este remedio son redes de cuarentena y portales cautivos.

Cuarentena:

Una red en cuarentena es una red IP restringida que proporciona a los usuarios acceso encaminado sólo a determinados hosts y aplicaciones.

La cuarentena es a menudo aplicado en términos de asignación de VLAN's, y cuando un producto NAC determina que un usuario final no cumple con las políticas de seguridad, su puerto de switch se asigna a una VLAN que se dirige sólo a los servidores de revisión y actualización, pero no con el resto de la red. Otras soluciones de usan técnicas de gestión direcciones (por ejemplo, Address Resolution Protocol (ARP) o Neighbor Discovery Protocol (NDP)) para la cuarentena, evitando la sobrecarga de la gestión de VLAN de cuarentena.

Portales cautivos:

Un portal cautivo intercepta el acceso HTTP a páginas web, redirigiendo a los usuarios a una aplicación web que proporciona instrucciones y herramientas para la actualización de su computador. Hasta que su equipo pasa la inspección automatizada, sin uso de la red. Esto es similar a la manera de pagar las obras de acceso inalámbrico en los puntos de acceso público.

Portales cautivos externos permiten a las organizaciones descargar controladores inalámbricos y intercambiadores de portales web de los hosting. Un portal único externo ofrecido por un dispositivo NAC para la autenticación inalámbrica y por cable, elimina la necesidad de crear varios portales, y consolida los procesos de políticas de gestión.

2.2.5 Características De NAC.

La primera tarea de NAC es decidir a qué clientes se autoriza a acceder y permanecer en la red. Los criterios para tomar estas decisiones pueden variar ampliamente, en función de múltiples parámetros de la máquina cliente, como disponer de un software antivirus debidamente actualizado, un sistema operativo con los parches adecuados o un cortafuegos configurado apropiadamente, por citar sólo algunos.

El objetivo es prevenir que los dispositivos que hayan sido contaminados en otras redes accedan a la red corporativa. Los dispositivos móviles y los utilizados por visitantes o socios comerciales que acceden a los recursos de la empresa son buenos ejemplos de clientes potencialmente peligrosos.

NAC puede también volver a ejecutar periódicamente los chequeos de seguridad mientras los clientes permanecen conectados a la red para cerciorarse de su buen comportamiento. Asimismo, algunos equipos comprueban si los dispositivos intentan explotar recursos no autorizados, restringiendo el acceso cuando violan las políticas.

Pese a sus ventajas, la adopción de NAC está lejos de ser agresiva, ni en número de despliegues ni en sus primeras aplicaciones en los negocios. Según Nemertes Research, en la mayoría de los casos, el uso del control de accesos se limita a las conexiones VPN; sólo una minoría emplea hoy NAC en las LAN corporativas. Un estudio realizado por la consultora hace algo menos de un año concluye que sólo alrededor del 14% de los entrevistados chequeaban en los puntos extremos los parches del sistema operativo y las aplicaciones; la presencia de cortafuegos, antivirus o antispyware; dispositivos USB conectados; y contraseñas. Sin embargo, un 60% desearía poder disponer, al menos, de chequeo de cortafuegos, antivirus y antispyware. Al 40% le gustaría además disponer de chequeo de sistema operativo y contraseñas. Y menos de un tercio deseaba chequear la actualización de las aplicaciones.

2.2.6 Arquitectura General De NAC.

Tres componentes básicos se encuentran en todos los productos NAC: el solicitante de acceso (Access Requestor o AR), la política de Punto de Decisión (Policy Decision Point o PDP) y el punto de aplicación de políticas (The Policy Enforcement Point o PEP). Los vendedores tienen sus propios nombres para ellos, pero vamos a utilizarlos términos definidos por el Trusted Computing Group Conexión de Red de Confianza (Trusted Network Connect) porque sus ideas son suficientemente claras.

Tabla II.I: Arquitecturas de NAC

	Cisco Network Access Control	Network Admission Protection de Microsoft	Trusted Computing Group, Trusted Network Connect
Evaluación de Host	El agente de confianza de Cisco (Cisco Trust Agent) será usado por Windows pre-Longhorn, Vista, Seven y Red Hat Enterprise 3 and 4.	EL agente NAP de Microsoft y el suplicante 802.1X son parte de Windows Longhorn y Vista. Los API's están disponibles para otros proveedores para crear e integrar los agentes del sistema de salud (SHA) en el marco de NAP. El vendedor es responsable de qué y cómo SHA se comunica con el cliente NAP. Por ejemplo, la auto-evaluación y notificación de cambios en tiempo real no son necesarias.	Las especificaciones TNC de acuerdo con la comunicación entre el AR y el PDP, así como el software pueden comunicarse con el AR TNC. Otros sistemas realizan la evaluación.
Validación	Credenciales y los datos de evaluación se envía al Servicio de Control de Acceso (ACS) para la validación. El ACS los envía al Servidor de Políticas de Red de Microsoft. El ACS selecciona una política basada en la respuesta del Servidor de Políticas de Red (NPS).	El Servidor de Políticas de Seguridad (NPS) se integra con los servidores de la política externa, tales como Servidores para evitar virus (avoid virus o AV) y sistemas de gestión de parches, para evaluar la salud de un host.	Los protocolos y API's desarrollados por TNC especifican como se comunicaran los componentes.
Ejecución	El hardware de Cisco se encarga de hacer cumplir la política de acceso enviada por el servidor de control de acceso.	La Cuarentena puede ser lograda permitiendo o denegando el acceso a un host a una VPN o la integración con sistemas externos.	Los protocolos y API's desarrollados por TNC especifican como se comunicaran los componentes.

Programas Asociados	Cisco tiene un programa de socios de gran población con una serie de proveedores de productos bien conocidos. Cisco y Microsoft alegan que se van a apoyar en sus programas de socios propios, así como el programa NAC/NAP. Microsoft está planeando la migración de sus socios a la nueva API para Longhorn y Vista.	Microsoft tiene un programa de socios grandes, y a diferencia de Cisco, también tiene una serie de proveedores de infraestructura en el campo.	Las especificaciones están disponibles para su descarga. Los miembros del TCG pueden participar en el trabajo de grupo. Microsoft ha liberado su protocolo de declaración de salud para las especificaciones TNC.
Pruebas de Interoperabilidad	Cisco utiliza AppLabs, que adquirió de KeyLabs, para las pruebas de interoperabilidad en el programa NAC. Los socios NAC están a la espera para desarrollar y probar sus productos.	Microsoft no tiene planes para un programa de pruebas de interoperabilidad.	El TNC está planificando a futuro programas de cumplimiento, pero por lo demás solo hay silencio sobre la cuestión.

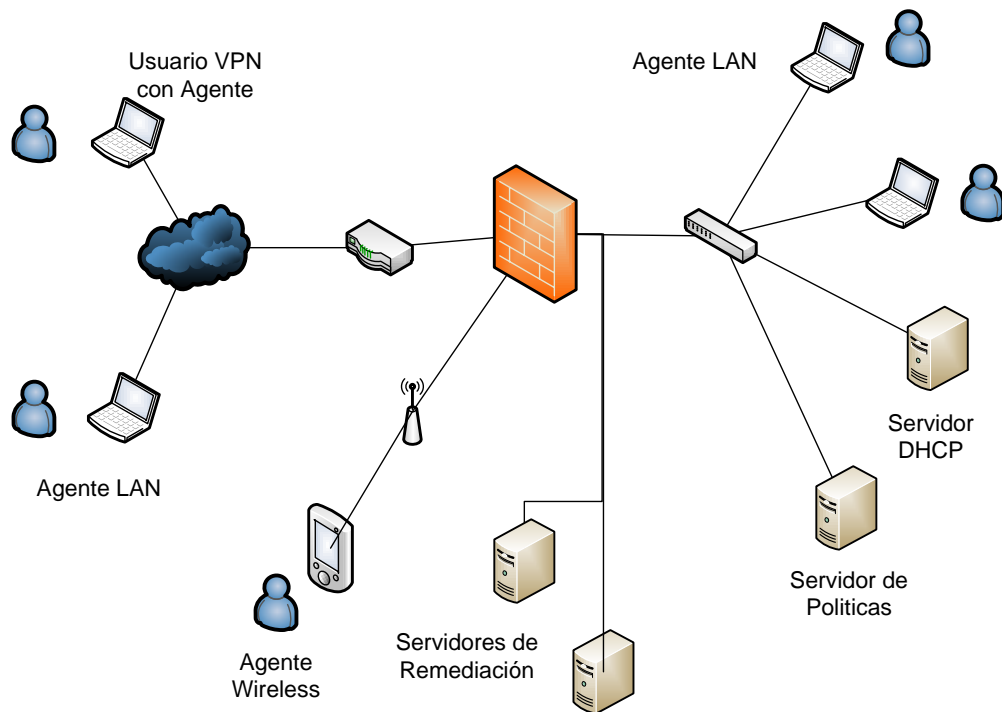


Figura II.01: Arquitectura General de NAC

Las funciones individuales de la PDP y el PEP pueden estar contenidas en un servidor o propagarse a través de múltiples servidores, dependiendo de la implementación de los proveedores, pero en general, las peticiones de acceso AR, el PDP asigna una política, y el PEP hace cumplir la política.

La AR es el nodo que está intentando acceder a la red y puede ser cualquier dispositivo que se gestiona por el sistema NAC, incluyendo estaciones de trabajo, servidores, impresoras, cámaras y otros dispositivos habilitados para IP.

La AR puede llevar a cabo su evaluación propia de host, o algún otro sistema puede evaluar el host. In either case, the AR's assessment is sent to the PDP. En cualquier caso,

la evaluación de la AR se envía al PDP. Sobre la base de la postura del AR y la definición de políticas de una empresa, el PDP determina cual acceso debería permitirse.

En muchos casos, el sistema de gestión del producto NAC puede funcionar como el PDP. El PDP se basa a menudo en los sistemas back-end, incluyendo antivirus, gestión de parches o directorios de usuarios, para ayudar a determinar la condición del host.

Una vez que el PDP determina la política a aplicar, esta comunica al control de acceso la decisión para la PEP realice su ejecución. El PEP puede ser un dispositivo de red, como un Switch, firewall o Router, un dispositivo fuera de la banda que maneje DHCP o ARP, o un agente del propio AR.

2.2.7 CICLO DE NAC.

Cuando un host intenta conectarse a una red habilitada para NAC, normalmente hay tres fases: pre-admisión o la evaluación posterior a la admisión, la selección de políticas y aplicación de políticas. Los criterios que rigen cada paso se basan en la política de su empresa y las capacidades de su sistema de NAC.

Antes de seleccionar un producto, determine con exactitud cuáles son los objetivos de su empresa. Por ejemplo, ¿Qué tan lejos fuera de la fecha puede un host tener parches o firmas AV antes de que ya no pueda acceder a la red? ¿Cuál es la condición aceptable antes de que un host invitado pueda tener acceso? ¿Quiere acceso a la base con un ID de usuario o no?

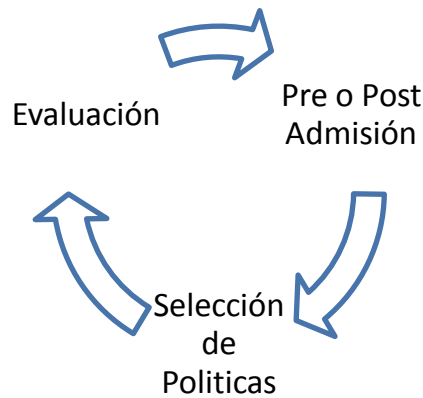


Figura II.02: Ciclo de NAC

El ciclo de NAC comienza y termina con la evaluación. La evaluación de pre-ingreso se produce antes de que conceda un acceso total a la red. La evaluación posterior a la admisión, después de que el acceso ha sido concedido, permite al host reevaluarlo periódicamente para asegurarse de que no representa una amenaza.

La evaluación de host recopila información como los sistemas operativos de los hosts, niveles de los parches, aplicaciones que se ejecutan o se instalan, la postura de seguridad, la configuración del sistema, la conexión del usuario, y más; y lo pasa a un PDP. Qué información es recogida es una función de las políticas definidas y las capacidades del producto NAC.

2.2.7.1 NAC MÉTODOS DE EVALUACIÓN

La evaluación de host es una parte fundamental de determinar el estado de este y el tipo de acceso que debe recibir. Estos son los métodos de evaluación más comunes usados hoy en día. Muchos proveedores de NAC soportan al menos dos de estos métodos. En la tabla II.II podemos observar detalladamente los métodos de evaluación.

Tabla II.II: Métodos de Evaluación de NAC

MÉTODO	¿COMO FUNCIONA?	VENTAJAS	DESVENTAJAS
Agentes Persistentes	Un agente software se instala y realiza las evaluaciones. El agente podría ser parte de un paquete más grande, como un cortafuegos de escritorio, o un corredor similar al Cisco Trust Agent	Una instalación única que trabaja con el equipo. Una vez instalado el software, el usuario nunca tiene que interactuar con él de nuevo. Ofrece una inspección profunda en el host.	No todos los sistemas, especialmente los sistemas de evaluación, pueden instalar un agente. El agente necesita los privilegios adecuados para evaluar el host. El agente debe ser compatible con todos los sistemas operativos y aplicaciones.
Agente Disolvente	Al igual que un agente persistente, el agente disolvente está escrito en un lenguaje móvil como Java o ActiveX y es descargado y ejecutado. La evaluación se realiza generalmente por el agente, en lugar de descargarlos de otras fuentes.	Puede ser instalado en cualquier máquina, y el código móvil es más probable el apoyo de múltiples sistemas operativos. Estos agentes suelen ser pequeños, en virtud de un megabyte de tamaño, para que puedan ser enviados a través de enlaces lentos.	No todos los sistemas soportan el código móvil. El usuario necesita los permisos adecuados para ejecutar el código, en Windows, este es a menudo el administrador local o un usuario avanzado.
Llamada a Procedimientos Remotos	Un servidor de la red ejecuta análisis mediante RPC o WMI en el equipo de destino. El servidor necesita credenciales de administrador del host para ejecutar la exploración, así como acceso al host.	No requiere instalación del agente, sin embargo, tiene el potencial para excavar muy profundamente en un host.	No todos los usuarios tienen acceso como administrador local, y el concepto de a los usuarios con más privilegios se debe limitar este acceso. Los invitados son difíciles de apoyar. Los chequeos no son tan completos como los enfoques de agente.
Análisis de Vulnerabilidad	Un servidor lleva a cabo una evaluación de la vulnerabilidad con un análisis en el	Ninguna instalación del agente y, a menudo, sin necesidad de tener	Visión limitada del host, si las credenciales de administrador

	host. El Servidor trata de analizar identificando el sistema operativo, servicios que se ejecutan y cualquier vulnerabilidad.	credenciales para un análisis sencillo. Proporciona una visión detallada de los puntos de ataque en un host.	no están disponibles. Los análisis pueden tardar mucho tiempo y, potencialmente, puede bloquear los servicios. Los hosts con firewalls interferirán con la capacidad de exploración. Los falsos positivos o falsos negativos son los problemas potenciales.
Monitoreo Pasivo	En lugar de evaluar el estado de un host, Monitores del host detectan un mal comportamiento, como la exploración o la infección de un gusano. Se puede realizar la detección de intrusos y supervisar las solicitudes de autenticación y las respuestas.	Detecta el comportamiento malicioso, independientemente de la condición de un host. Vigilancia pasiva puede utilizar la detección por firmas o basada en anomalías. Ofrece detección en tiempo real de las actividades no cumplen las normas.	Los únicos datos disponibles en el estado de un host es lo que se transmite de nuevo a la red. El Sistema operativo y la detección de servicios pueden no ser exactos. Necesitas tener una visión del tráfico de red, que puede ser difícil de lograr.

Las evaluaciones pueden utilizar un agente de instalación permanente, comúnmente en host basados en NAC. o agentes disolubles mas probablemente, llamada así porque se basan en Java o ActiveX y desaparecen después de ser utilizados. Los agentes disolubles a veces se llaman NAC sin agente, pero este método implica de hecho que los agentes deben ser descargados e instalados en el computador del host.

El problema es que los modelos de seguridad en Windows, Mac OS X y Linux a menudo requieren agentes, ya sean permanentes o disolubles, y para esto debemos tener derechos de administrador local para ejecutarlos.

Esto se convierte en un problema en las organizaciones que (sabiamente) no permiten que los computadores portátiles y de escritorio se ejecuten con privilegios de administrador local. En algunos casos, los agentes pueden necesitar privilegios de administrador sólo la primera vez que es instalado, esto puede permitir trabajar evitando esta limitación.

Pero ¿qué pasa si usted no puede poner un agente en un sistema? En ese caso, las evaluaciones se llevan a cabo sin agente remoto a través de métodos de exploración o análisis, como ejecutar un escaneo de vulnerabilidades, o utilizando RPC (Remote Procedure Call) o WMI (Windows Management Instrumentation) para consultar un host. Por otra parte, el escaneo pasivo, mediante la detección de intrusiones y detección de anomalías de red, busca hosts maliciosos basados en el tráfico actual de la red. Una evaluación, incluso se podría definir como obligar a un usuario establecerse en una Política de Uso Aceptable (Acceptable Use Policy) antes de ser concedido el acceso a la red.

Reevaluaciones posteriores a la conexión se producen después de que se concede el acceso al host. Estos se pasan por alto a su cuenta y riesgo, porque la condición de un hosts puede cambiar mientras se está conectado. Un gusano puede ser activado, o un usuario malintencionado podría empezar a atacar. La evaluación posterior a la

conexión puede iniciarse automáticamente después de establecer un período de tiempo, por un administrador, según sea necesario, o basado en un cambio en el host, como un cortafuegos de escritorio o el AV este deshabilitado. Nuevas evaluaciones se comparan con la política actual, y se toman acciones definidas.

Un giro interesante a las evaluaciones posterior a la conexión son los productos que utilizan la red de vigilancia pasiva, ya sea dentro del sistema de NAC o mediante la integración con un sistema de detección de intrusiones existentes o un sistema de la red de detección de anomalías, para alertar sobre la actividad maliciosa. Estos monitores externos alertan sobre el tráfico de red y pueden detectar problemas de pérdidas por las evaluaciones basadas en host.

2.2.7.2 Política De Selección

Una definición robusta de políticas es fundamental para una implementación exitosa de NAC. Definiendo reglas que son lo suficientemente flexibles como para no poner una carga desproporcionada a los usuarios finales y suficientemente estrictas para proteger la red se llevará a la planificación y las pruebas. Una política de binaria, tal como: "Cumplir con la política actual o se les niega el acceso," suena bien en el papel, pero a menudo no en el mundo real. Un computador portátil que no ha estado en línea, por ejemplo, mientras que un usuario se fue de vacaciones, no puede estar al día con su firma AV, pero eso no quiere decir que esté infectado. ¿Estás seguro que quieres sacar un empleado fuera, o sería mejor tener el portátil actual en segundo plano mientras el usuario continúa trabajando?

Afortunadamente, los motores de política de NAC ayudan en la creación de políticas. Encontrar un motor que se adapte a sus necesidades en términos de facilidad de uso y la granularidad es especialmente vital, los vendedores NAC añaden más características a sus productos, y las interfaces de política reflejan el creciente número de opciones. Al igual que cualquier interfaz de usuario para la gestión de un sistema

complejo, las características como agrupamiento, la capacidad de crear objetos personalizados y conjuntos de reglas de fácil lectura son importantes.

Cómo se integran los sistemas externos es igualmente crucial. Por ejemplo, si el sistema NAC utiliza Active Directory para la autenticación de usuario, el sistema de gestión debe ser capaz de sincronizar los objetos como usuarios y grupos dentro de AD, en lugar de tener que volver a recrearlos. De manera similar, los productos antivirus, cortafuegos gestionados y sistemas de gestión de parches también debe alimentar a la gestión de la interfaz de usuario sin problemas.

Una palabra en la política: Es un negocio arriesgado para la IT para tomar decisiones de política relacionadas con la alta gerencia. Pero resistir la tentación de tratar a los ejecutivos de otra manera. El computador portátil del director financiero no es menos vulnerable a los ataques que la de un representante del área. Educar acerca de las prácticas conocidas y, en su caso, señalando los efectos del cumplimiento de las normas puede ayudar.

2.2.7.3 Aplicación

La ejecución es la acción definida en una política en respuesta a un estado del host. Puede variar desde no hacer nada, para registrar un evento o quitar a un computador de la red. Típicamente el control de acceso se refuerza usando 802.1X, DHCP, y la gestión de ARP, la redirección de DNS a una zona protegida, un sistema de actualización y configuración y el radio de alterar el tráfico o el acceso de un usuario de la red. En la tabla II.III se puede revisar detalladamente los Métodos de Autenticación.

Tabla II.III: Métodos de Autenticación NAC

Los métodos de ejecución son las acciones que se aplican a los equipos. En muchos casos, su aplicación es automática. Muchos vendedores soportan varios métodos de aplicación al mismo tiempo, así pueden seleccionar la mejor para cada situación.			
MÉTODO	¿COMO FUNCIONA?	VENTAJAS	DESVENTAJAS
802.1X	Se trata de un protocolo de Capa 2, significa que la autorización se produce antes de la asignación de las direcciones IP. Los puertos inician en un estado no autorizado. Un cliente, llamado suplicante, envía las credenciales al switch. El switch envía las credenciales a un servidor a través de RADIUS. Tras una autenticación correcta, el puerto del switch es activado.	Autenticación y autorización ocurre antes que el host, tenga acceso a la red. Múltiples esquemas de autenticación son compatibles, y 802.1X está diseñado para ser extensible como la llegada de una nueva tecnología.	Todos los computadores necesitan tener configurado correctamente los suplicantes, y los usuarios, o las computadoras, necesitan tener cuentas. Muchos Switchs ponen un puerto en un estado u otro, así que si hay varios hosts en un puerto, todos ellos son tratados como el mismo.
Direccionamiento VLAN	Los segmentos de redes VLANs están dentro de redes lógicas, y el direccionamiento mueve los hosts a una VLAN particular. El direccionamiento sucede aprovechando un cambio de sistema de gestión de VLAN nativa o a través de otros protocolos, como SNMP.	Las VLANs se conocen bien, y muchas empresas las utilizan ya. Prácticamente cualquier puerto puede estar en cualquier VLAN, por lo que la movilidad se logra fácilmente.	Una arquitectura VLAN puede ser compleja y la asignación dinámica de VLANs puede hacer que la solución de problemas sea difícil. Algunos Switchs son vulnerables a los ataques provenientes de Switchs con VLANs inseguras.
Aplicación de Host	Podría decirse que este era el sistema original de NAC, donde la evaluación y la ejecución del host a través de un firewall del host permitían o denegaba el acceso a tráfico de red.	Es posible controlar el acceso no sólo del tráfico de la red al host, sino también controla las aplicaciones en el host que puede tener acceso a los puertos de la red. A menos que el host sea un servidor de correo, no hay razón para que una aplicación pueda	El software del host tiene que ser administrado, y la solución de problemas a un usuario remoto que está teniendo problemas de conexión puede ser difícil.

		tomar el puerto de correo. Además, la aplicación vigila al host, aunque este fuera de la red, por lo que un host puede ser protegido de acuerdo a la política de la empresa mientras se esté conectado a redes remotas.	
Administración DHCP	DHCP maneja las asignaciones de direcciones IP a los hosts. Un administrador de configuración DHCP intercepta las peticiones DHCP y asigna las direcciones IP en su sitio. Por lo tanto, la aplicación de NAC se produce en la capa IP basadas en la subred y la asignación de IP.	Fácil de instalar y configurar. Debido a que el DHCP está bien soportado, este funciona en cualquier equipo que utilice DHCP para solicitar una dirección IP.	La administración DHCP es fácilmente derrotada por un computador que se asigna estáticamente su propia dirección IP.
Administración ARP	También se llama "spoofing ARP" o "man-in-the-middle". El protocolo de resolución de direcciones se utiliza para decir otras máquinas que las direcciones IP se asignan a una dirección MAC. Estas tareas se llevan a cabo en una tabla ARP en cada host y es actualizado periódicamente. Este método administra una tabla ARP de hosts de forma dinámica enviando las tablas ARP con diferentes asignaciones IP-MAC.	ARP se utiliza en cualquier host IP y siempre funcionará sin cambios en la configuración de los hosts.	Al igual que en la administración de DHCP, asignando estáticamente una entrada a la tabla ARP cae este método. Además, las nuevas funciones de seguridad en los Switchs diseñados para prevenir maliciosos ARP Spoofing pueden hacer que este método no sea utilizable.
Wildcard DNS	Similarmente DNS asigna nombres de host a direcciones IP. Del mismo modo, los mapas DNS del host a direcciones IP.	Como administra DHCP y ARP, este método funciona con cualquier host que utilice DNS.	Como administra DHCP y ARP, si un host no utiliza DNS, este método falla. Además, los

	Wildcard DNS responderá a cualquier consulta DNS con una dirección IP, efectivamente reorientando de los hosts a un servidor específico.	A menudo, el usuario termina en una página Web, donde se tiene que autenticar o aceptar un contrato. Se basa en el hecho de que los usuarios eventualmente utilizarán un navegador web y por lo tanto se les redirige a una página Web.	computadores pueden tener entradas estáticas de hosts.
Walled Garden	Un “walled garden” fuerza a un usuario a una red privada, donde pueden acceder a los recursos limitados, como una página web para aceptar un acuerdo, a sistemas de actualización, y realizar otras funciones. Una vez que el host ha pasado, se puede permitir el paso a otra red.	Si a un host se le niega el acceso a la red, ¿cómo pueden actualizarse? Un walled garden se utiliza a menudo en combinación con otro método de ejecución.	Se tiene que mantener actualizados los servidores y otros equipos en el walled garden.
Línea de Bloqueo	La línea de bloqueo es similar a un firewall de red, excepto que el control de acceso está en función de cada host y asignados de forma dinámica. Además, los sistemas en línea pueden monitorear el tráfico de la red y tomar una decisión sobre la actividad maliciosa.	La línea de bloqueo es generalmente bastante fina porque los puertos y, en algunos casos, incluso el tráfico de carga se puede controlar. Otros métodos están primariamente sólo basados en el host.	La línea de bloqueo esta menudo entre las capas de conmutación, y esto significa que un host malicioso puede atacar a otros equipos que son accesibles sin tener que pasar por el dispositivo en línea. Dispositivos en línea tienen que ser desplegados en cada punto.
Restablecimiento de mensajes TCP/ICMP	El sistema NAC mata las conexiones TCP enviando restablecimientos TCP para el cliente y el servidor. Una vez que el host recibe un restablecimiento TCP, la conexión TCP es cerrada. Los protocolos que son TCP se gestionan mediante	Al igual que otros métodos pasivos, el restablecimiento TCP trabaja con cualquier computadora con conexión TCP y pasará a través de cualquier firewall o gateway de seguridad.	Los protocolos no TCP son difíciles de soportar. Ataques de un paquete simple utilizan UDP, como SQL Slammer, que pasan a través de la red.

	mensajes ICMP	Los protocolos no TCP utilizan mensajes ICMP, pero no hay garantía de que cada host respetara los mensajes ICMP.	
Parches, Actualizaciones y cambio de configuraciones	También usados en conjunción con otros métodos de control, cada host parchado de forma automática o manual puede ajustarse de conformidad y prepararse para una nueva evaluación.	Para los equipos propiedad de la compañía, esta es una buena medida para garantizar que los hosts sean actualizados y configurados correctamente.	No siempre se puede obligar a los usuarios externos, como los contratistas, para actualizar sus computadoras o instalar software. Además, obligando a una actualización antes de acceder a la red puede afectar a la productividad.

La parte más espinosa de la ejecución se trata de las excepciones. Los host que no se pueden evaluar utilizando cualquiera de los métodos definidos todavía necesita la aplicación de algún tipo. Piense en todos los dispositivos de la red que no se puede instalar un software, desde impresoras hasta cámaras Web a teléfonos de VoIP para dispositivos de aplicación. Normalmente, el método de ejecución sólo es para la lista blanca de las direcciones de estos dispositivos MAC. Sin embargo, las direcciones MAC son fácilmente falsificadas, se puede evitar implementando las medidas de seguridad basadas en MAC para prevenir el acceso a los Switchs, o al menos reducir la probabilidad de estos ataques.

2.2.7.4 Implementación De Estilos

Hay cuatro formas básicas en que los sistemas NAC pueden integrarse en la red, cada uno con ventajas y desventajas. Muchos de los productos NAC prevén más de un modelo de implementación.

NAC on line pone un dispositivo en una piedra en el alambre, por lo general entre el Switch de acceso y el Switch de distribución. Al decidir dónde colocar el dispositivo, recuerde que cuanto más lejos este de los hosts, los objetivos de mayor potencial están disponibles para un atacante.

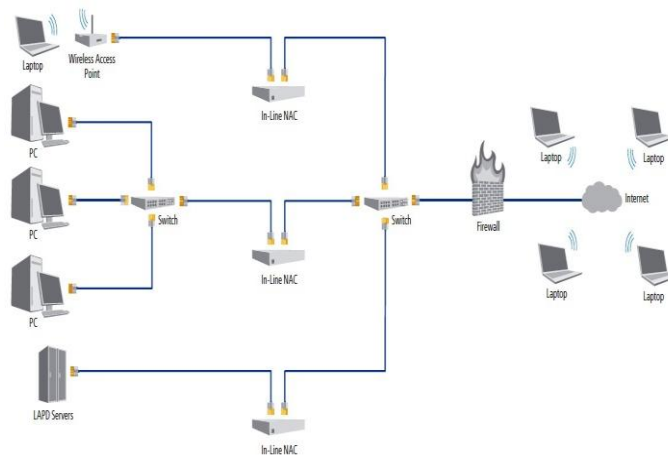


Figura II.03: NAC en línea.

Un producto NAC online puede bloquear el tráfico, como un firewall de red, pero su ACL se adapta a las máquinas individuales. Otros métodos de aplicación, como direccionamiento por VLANs, están también disponibles. El beneficio de la NAC online es que si no hay método de ejecución se dispone de otra, el bloqueo en línea sigue siendo una opción. Las desventajas son que va a añadir otro punto de falla potencial (determinar si el dispositivo falla al abrir o cerrar), y necesitara un dispositivo por cada punto de aplicación.

NAC out-band se usa más comúnmente que en banda cubre los productos que son PDP pero usan otros métodos, como 802.1X, DHCP y administración de ARP, o el manejo de VLANs, para hacer cumplir las políticas. Como los hosts están en línea, el producto NAC interviene y realiza algún tipo de evaluación, entonces concede el acceso a algún lado. El beneficio de NAC fuera de banda es que hay poco impacto en el rendimiento de la red, y menos dispositivos son necesarios. La eficacia de NAC out-band depende de los mecanismos de descubrimiento y de aplicación. El control de DHCP, por ejemplo, es fácil desviarse si un host tiene una dirección IP estática.

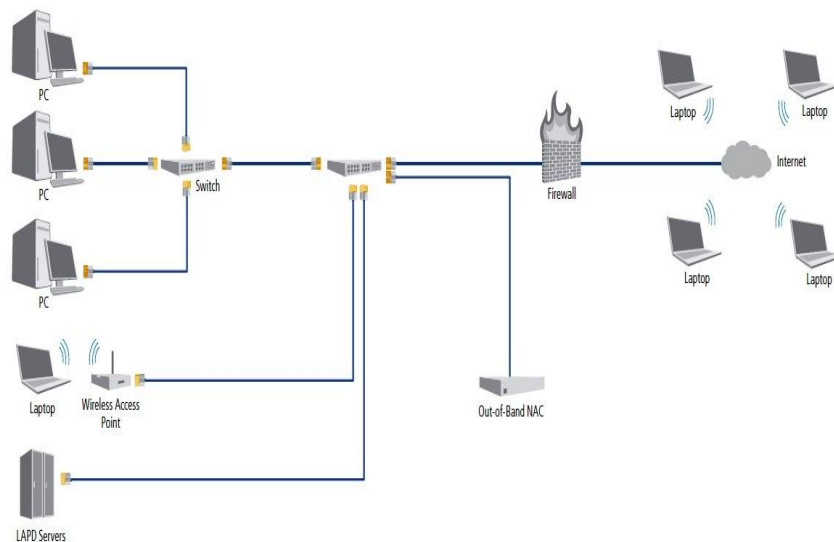


Figura II.04: NAC fuera de banda.

NAC basado en un Switch es similar a NAC en banda, pero en lugar de tener la aplicación y distribución entre el switch, la aplicación se produce en el propio switch. Lo que diferencia a NAC basada en switch es que simplemente usa 802.1X para controlar un puerto. Ofertas de NAC basado en switches no requieren 802.1X para comunicarse con el solicitante de acceso.

Una vez que el host hace peticiones de acceso, este es evaluado mediante un agente o sin agentes de exploración y, a continuación el PDP establece la política en el puerto del switch. Los productos NAC basados en switches ofrecen detección de intrusos internos y la detección de anomalías en función de cada puerto, así que no hay necesidad de integrar un sistema externo. Al igual que NAC en banda, NAC basada en switches pueden también aplicar los controles de acceso a los puertos de uso de la red y por tipo de tráfico. Idealmente, NAC debería aplicarse a un nivel de puerto para el mejor control, así que si se piensa actualizar los switches, debe investigar las características avanzadas de los switches.

NAC basado en host se basa en un agente de host instalado para evaluar y hacer cumplir políticas de acceso. Agentes instalados con una gestión centralizada, y la política de acceso al siguiente host, incluso cuando este fuera de la red. A diferencia de los mecanismos de aplicación basados en la red, NAC basado en host puede controlar no sólo el tráfico que pasa hacia y desde la red, sino también las aplicaciones que se pueden utilizar en la red. Por ejemplo, no hay razón para que una estación de trabajo deba tener un programa conectado al puerto de correo. El control de grano fino del agente, y la interacción limitada con el usuario son razones de peso para NAC basado en host. Por supuesto, hay otro agente software que tiene que ser administrado, y el invitado y el acceso del contratista a menudo no son bien soportados. Además, los hosts que no son Windows pueden no ser compatibles.

2.3 HERRAMIENTAS OPENSOURCE NETWORK ADMISSION CONTROL

Existen algunas herramientas OpenSource gracias sobre todo a la liberación de código por parte de CISCO. Las herramientas que se pueden encontrar son las siguientes.

2.3.1 FREENAC

2.3.1.1 Descripción

FreeNAC provee una solución transparente para la administración dinámica de redes virtuales, a la vez que restringe la conectividad a la red. Desde el punto de vista de la seguridad, detecta dispositivos 'desconocidos' que están tratando de obtener acceso a través de un conector de red Ethernet abierto, negando el acceso (y registrando el evento). Los dispositivos conocidos y registrados son colocados a la red virtual que es atribuida a ellos.

Los visitantes (dispositivos desconocidos), pueden opcionalmente tener acceso a una zona de redes virtuales por defecto o para invitados. Esto puede ser útil, por ejemplo, para organizaciones que desean permitir a sus visitantes acceso Web/VPN a Internet, pero restringir el acceso a las redes internas.

Con FreeNAC, tan pronto como un nuevo dispositivo es conectado al puerto del Switch, su dirección MAC se pasa al servidor, donde será almacenada y comprobada para determinar si este dispositivo tiene acceso a la red. Si el dispositivo está autorizado a tener acceso, el servidor le regresará al Switch la red virtual a la que este dispositivo pertenece. Si este dispositivo todavía no está registrado, su acceso es bloqueado o se coloca en una red virtual limitada, dependiendo en la política.

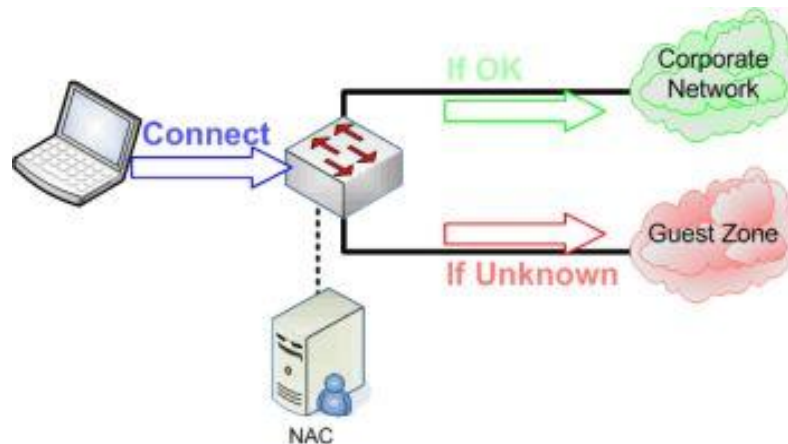


Figura II.05: Arquitectura de FREENAC.

2.3.1.2 Modos de Operación

FreeNAC tiene dos modos de operación:

- VMPS
- 802.1X

VMPS (VLAN Management Policy Server) es un método para asignar puertos de un switch a redes virtuales específicas de acuerdo a la dirección MAC del dispositivo que busca acceso a la red. En modo VMPS, un switch compatible con VMPS detecta una nueva PC y crea una petición VMPS pidiendo autorización de FreeNAC, el cual revisa en su base de datos y permite o niega el acceso a la red basándose en la dirección MAC. El Switch se encarga de respaldar la decisión tomada por FreeNAC y niega acceso o en caso contrario, coloca el dispositivo de manera dinámica en su red virtual por defecto.

802.1X es un estándar creado por la IEEE para el control de acceso a redes basándose en el puerto del Switch. Proporciona autenticación a dispositivos conectados a un puerto de la red, estableciendo una conexión punto a punto o restringiendo el acceso en caso de que la autenticación falle. 802.1x está disponible en algunos modelos recientes de Switches y puede ser configurado para autenticar equipos los cuales

cuenten con un software suplicante, no permitiendo accesos no autorizados a la red en la capa de enlace.

En modo 802.1x, FreeNAC verifica las credenciales de los usuarios ((a través del uso de un servidor de autenticación externo) y usa la dirección MAC del dispositivo que se conecta para asignarlo a una red virtual. Esto crea un par nombre de usuario/dispositivo que es único para cada cliente que se conecta.

Para un usuario malicioso no basta con saber únicamente la dirección MAC, sino que también debe de obtener credenciales válidas, lo cual hace más difícil el obtener acceso a la red.

Para dispositivos que no son compatibles con 802.1x y que usan Switches Cisco compatibles con 802.1x, usamos un modo especial de autenticación llamado "MAC-Authentication bypass" para autorizar el dispositivo y asignar una red virtual. Autenticar al usuario y al dispositivo es más seguro que autenticar solamente el dispositivo; este es un compromiso riesgo/beneficio.

2.3.1.3 Características

FreeNAC contiene numerosas funciones para ayudar al administrador con el manejo y puesta en marcha de redes virtuales, al mismo tiempo que proporciona control de acceso a redes.

Las características principales son:

- Asignación dinámica de redes virtuales
- Control de acceso a redes
- Flexibilidad en mecanismos de autenticación para redes: 802.1x, VMPS, Cisco Mac-Auth-Bypass
- Altamente automatizado
- Redundancia y repartición de carga de red para una mejor disponibilidad
- Inventario en tiempo real de los aparatos conectados a la red
- Documentación del cableado de la red
- Reportes flexibles

La **edición comunitaria** se puede descargar gratuitamente; la **versión Empresarial** provee características adicionales, como se detalla a continuación:

Tabla II. IV: Tabla comparativa de FreeNac

Comparación de características	Comunitaria	Empresarial
Autenticación basada en dirección MAC (VMPS mac-auth-bypass)	✓	✓
Autenticación 802.1x	✓	✓
Interfaz de usuario Windows	✓	✓
Interfaz de usuario basada en Web	✓	✓
Integración con Active Directory	✓	✓
Integración inteligente de hubs	✓	✓
Comprobación de puertos abiertos e identificación del sistema operativo en los dispositivos	✓	✓
Documentación de cableado	✓	✓
Inventario automatizado de nombres de	✓	✓

computadoras		
Establecer una fecha de validez para cada dirección MAC (para permitir el acceso a los visitantes por un día por ejemplo)	✓	✓
Soporte para el manejo de máquinas virtuales	✓	✓
Asignación de redes virtuales dependiendo de la localización del switch	✓	✓
Scripts para ayudar en la importación inicial de sistemas desde un archivo CSV	✓	✓
Alertas de eventos claves del sistema	✓	✓
Detección automática de dispositivos no manejados activamente por NAC, para proporcionar un inventario completo de los dispositivos en la red		✓
Integración con servidores de antivirus McAfee EPO		✓
Integración con servidores SMS de Microsoft (Software package/gestión del sistema)		✓
Herramienta web para ayudar en documentar la localización de cables/puertos de switches		✓
Herramienta de "paro" de emergencia la cual puede desactivar NAC y rápidamente configurar redes virtuales estáticas en los puertos del switch (recuperación en un desastre o en una situación extrema)		✓
Módulos personalizados para entornos de clientes específicos (por ejemplo, interfaces a sistemas corporativos "estáticos" de inventario)		✓
Soporte prioritario de parte del equipo FreeNAC		✓

2.3.1.4 Beneficios

2.3.1.4.1 Principales beneficios

- Una red dinámica le permite un mejor uso de los puertos de switches disponibles, lo cual reduce costos y aumenta la eficiencia, facilita la configuración de los switches y hace posible tener menos cambios en el cableado durante reorganizaciones.
- FreeNAC no requiere software instalado en los dispositivos en modo VMPS. En modo '802.1x', un software 'suplicante' necesita ser instalado. Clientes que ya usan "acceso manual basado en puerto" ahorrarán tiempo y ganarán efectividad.
- FreeNAC también funciona con antiguos switches Cisco, no es necesario adquirir nuevo hardware Cisco.
- Inventario automatizado de la red.

2.3.1.4.2 Beneficios adicionales

- Permite que el cableado de red sea más dinámico y eficiente.
- Altamente automatizado y fácil de usar, lo que reduce costos por soporte.
- Extensible: agregue sus propios módulos o interfaces a sus sistemas para integrar NAC mejor en sus procesos y "workflows". Estándares abiertos, OpenSource, usted lo puede modificar a sus deseos.

- NAC corre sobre hardware y sistemas operativos estándar (Linux/Unix).
- Tecnología comprobada: en producción desde 2004.
- La interfaz gráfica puede ser utilizada por soporte técnico. No es necesario tener experiencia en Cisco.
- Más eficiente que "acceso manual basado en puerto" o VMPS clásico.

2.3.1.5 Servicios ofrecidos

- Manejo dinámico y asignación de redes virtuales para cada dispositivo.
- Control de acceso a su red (autenticación, autorización, asignación de redes virtuales por dispositivo).
- Inventario eficiente de los diversos elementos en su red.
- Permite la movilidad de sus equipos a través de varias habitaciones o edificios.

Dónde se puede utilizar FreeNAC?

Básicamente en cualquier lugar dentro de su organización, pero está especialmente adaptado para:

- Unidades de investigación y desarrollo, donde hay generalmente muchas subredes y es necesario crear rápidamente nuevas redes dinámicas, por ejemplo, para grupos de proyectos.
- Redes de estaciones de trabajo.
- Salas de reuniones.
- Salas o habitaciones expuestas al público, o para empleados ajenos a la compañía.
- Oficinas en espacios abiertos.
- Durante reorganizaciones, para rastrear y controlar el acceso a la red.

2.3.1.4.3 Administración de Switches

Configurar switches para usar VMPS es fácil con FreeNAC, permitiendo, por medio de una interfaz gráfica, configurar simplemente los puertos de los switches. Incluso cuando no tiene experiencia para manejar los switches, FreeNAC permite economizar tiempo al configurar una red.

Para los usuarios experimentados, configurar un Switch no es una tarea ardua, pero puede consumir mucho tiempo. Esta característica de NAC permite economizar tiempo, mejorando la productividad de los administradores de red, los cuales requieren de menos tiempo para configurar una serie de switches.

2.3.2 PACKETFENCE

PacketFence es totalmente compatible, confiable, Libre y un Sistema OpenSource para el control de acceso a la red (NAC). Con un impresionante conjunto de funciones que incluye un portal cautivo, para el registro y la rehabilitación, gestión centralizada de cable e inalámbricas, soporte 802.1X, aislamiento de dispositivos problemáticos de capa 2, la integración con el IDS (Sistema de Detección de Intrusos) Snort y el escáner de vulnerabilidades Nessus, PacketFence se puede utilizar de manera efectiva en redes de seguridad de redes heterogéneas pequeñas a muy grandes.

Principalmente desarrollado en Perl con un poco de PHP, Web (HTML / CSS / JavaScript) y SQL, PacketFence aprovecha los componentes de los famosos proyectos de código abierto como Snort, Apache HTTPD, el Net-SNMP FreeRADIUS, mod_perl, MySQL, dhcpd, Bind (nombre), OpenVAS y mucho más.

PacketFence es totalmente compatible, confiable, Libre y un Sistema OpenSource para el control de acceso a la red (NAC). La integración con el IDS (Sistema de Detección de Intrusos) Snort y el escáner de vulnerabilidades Nessus, PacketFence se puede utilizar de manera efectiva en redes de seguridad de redes heterogéneas pequeñas a muy grandes.

PacketFence es una solución discreta que trabaja con equipos de muchos vendedores (por cable o inalámbrica), tales como 3Com, Aerohive, Allied Telesis, Aruba, Cisco, Dell, Enterasys, ExtremeNetworks, Extricom, Fundición / Brocade, Hewlett-Packard, Intel, Juniper Networks, LG-Ericsson EE.UU., Meru Networks, Motorola, Nortel / Avaya, Ruckus y Xirrus.

Packetfence puede utilizarse en redes de:

- Bancos
- Colegios y universidades
- Empresas de ingeniería
- Centros de convenciones y exposiciones
- Hospitales y centros médicos
- Hoteles
- Fabrica

2.3.2.1 Características

PacketFence ofrece una impresionante lista de características compatibles. Entre ellos se encuentran:

Fuera de banda

La operación de PacketFence es completamente fuera de banda la cual permite la solución a escala geográfica y por lo tanto resistente a las fallas. Al utilizar la tecnología adecuada, un solo servidor PacketFence puede ser usado para asegurar cientos de Switchs y a los muchos miles nodos conectados a estos.

Soporte Voz sobre IP (VoIP)

También llamada telefonía IP (IPT), VoIP es totalmente compatible (incluso en entornos heterogéneos) para los múltiples fabricantes de conmutadores (Cisco, Edge-Core, HP, Linksys, Nortel Networks y muchos más).

802.1X

802.1X inalámbrico y por cable es soportado a través del módulo externo de FreeRADIUS.

Integración Inalámbrica

PacketFence se integra perfectamente con las redes inalámbricas a través del módulo externo de FreeRADIUS.

Esto le permite asegurar sus redes cableadas e inalámbricas de la misma forma con la base de datos de usuario y la utilización del mismo portal cautivo, proporcionando una experiencia de usuario consistente.

Una mezcla de proveedores de Puntos de Acceso (AP) y controladores inalámbricos están soportados.

Registro

PacketFence cuenta con un mecanismo de registro opcional similares a las soluciones de portales captivos.

Contrariamente a la mayoría de soluciones de portal cautivo, PacketFence recuerda que los usuarios previamente registrados y automáticamente se les dará acceso sin otra autenticación. Por supuesto, esto es configurable. Una Política de Uso Aceptable se puede especificar de forma que los usuarios no pueden permitir el acceso a la red sin haberlo aceptado.

Detección de actividades de red anormales.

Actividades anormales de la red (virus, gusanos, software espía, el tráfico denegado por el establecimiento de políticas, etc.) pueden ser detectados utilizando sensores Snort locales y remotos. Más allá de una simple detección, las capas de PacketFence tienen sus propios mecanismos de alerta y supresión en cada tipo de alerta.

Un conjunto configurable de acciones por cada violación está disponible para los administradores.

Analiza vulnerabilidad proactiva

El escaneo de vulnerabilidades de Nessus se puede realizar en el registro, programarlo sobre una base ad-hoc. PacketFence correlaciona el ID de la vulnerabilidad de Nessus de cada configuración de escaneo de violación, retornando las páginas web con el contenido específico sobre que vulnerabilidad el nodo puede tener.

El aislamiento de dispositivos problemáticos

PacketFence soporta varias técnicas de aislamiento, incluyendo el aislamiento de VLAN's con soporte VoIP (incluso en entornos heterogéneos) para múltiples fabricantes de Switchs.

Remediación a través de un portal cautivo

Una vez atrapado, todo el tráfico de red se determina con el sistema PacketFence. Con base en el estado de los nodos actuales (violación abierta, no registrado, etc), se redirige al usuario a la URL correspondiente. En el caso de una violación, al usuario se le presenta instrucciones para la situación particular en el/la que se encuentre, reduce la intervención costosa mesa de ayuda.

De línea de comandos y gestión basada en Web

Tiene las interfaces basadas en web y línea de comandos para todas las tareas de gestión. Administración basada en web es compatible con diferentes niveles de permisos para usuarios y autenticación de usuarios con Active Directory (AD).

Administración de VLANS

La solución se basa en el concepto de aislamiento de la red a través de la asignación de VLAN. Debido a su larga experiencia, la gestión de VLAN de PacketFence llegó a ser muy flexible con los años. La configuración de VLAN se mantiene, sin embargo en Packetfence se debe añadir dos VLAN más en toda la red, esta son: el registro de VLAN y VLAN aislada. Por otra parte, PacketFence también pueden hacer uso de las funciones de apoyo de muchos proveedores de equipos.

Las VLAN se pueden crear por los siguientes roles:

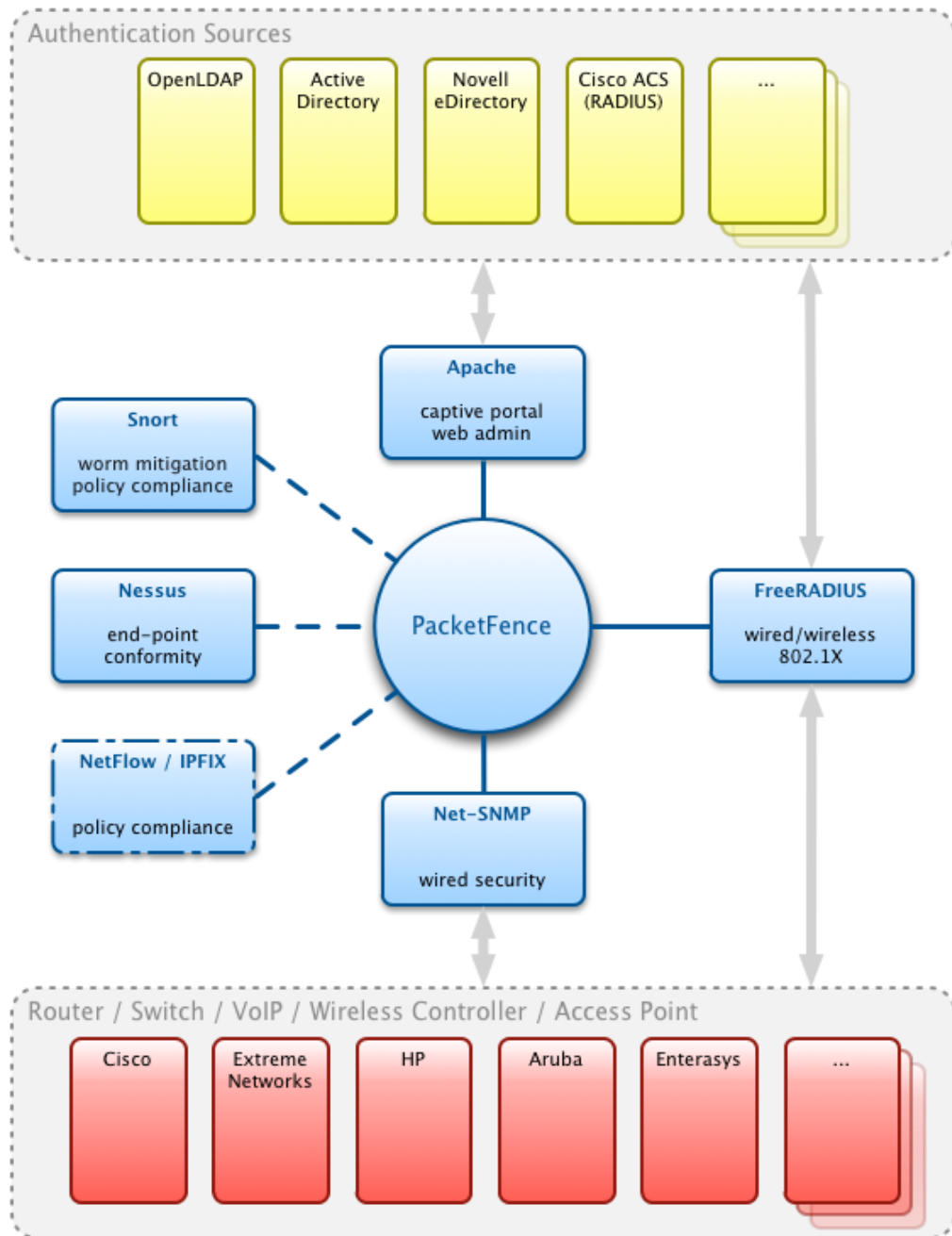
- Por switch (como VLAN por defecto)
- Por categoría del cliente, según las funciones realizadas por los clientes.

Además, de la VLAN de configuración del switch, se puede combinar con otras VLANS. Por ejemplo, con una configuración por defecto de PacketFence, es una VLAN que puede ser asignada a las impresoras y los computadores (si se clasifican correctamente) que están conectados a la red. Esto implica que usted puede fácilmente tener por cada dispositivo una Vlan para este tipo de dispositivo.

2.3.2.2 Componentes

Los componentes de Packetfence se ven representados en la siguiente imagen.

Figura II.06: Arquitectura de Packetfence.



2.3.23. Administración de Packetfence.

La administración está basada en Web y las interfaces de línea de comandos para todas las tareas de gestión. La Administración basada en Web es compatible con diferentes niveles de permisos para los usuarios y la autenticación de usuarios contra LDAP o Microsoft Active Directory.

Administración del acceso a invitados.

Hoy en día, la mayoría de las organizaciones deben hacer frente a una gran cantidad de consultores de diversas empresas que requieren acceso a Internet para su trabajo desde la red interna. En la mayoría de los casos, un acceso a la red corporativa se da con poca o ninguna auditoría de la persona o dispositivo.

PacketFence es compatible con una VLAN de invitados, esta VLAN de invitados se configura en su red solamente para tener acceso desde su red hacia internet; el registro de VLAN y el portal cautivo son los componentes que se utilizan para explicar al cliente cómo registrarse para tener acceso y cómo funciona su acceso. Esto generalmente se marca por la organización que ofrece el acceso. Existen varios medios de registro para los huéspedes estos pueden ser:

- El registro manual de los invitados (por adelantado o por)
- Contraseña del día
- Auto-registro (con o sin credenciales)
- El acceso de invitados patrocinados (empleado que dé fe de un invitado)
- El acceso de invitado activado por un correo electrónico de confirmación.
- El acceso de invitado activado por la confirmación en un mensaje de teléfono móvil mediante SMS.

PacketFence también soporta los huéspedes creaciones de acceso y las importaciones. Se integra con la solución de facturación en línea, como Authorize.net. Utilizando esta

integración, se puede manejar los pagos en línea, necesarios para obtener acceso a la red correcta.

Administración de los tipos de violación

PacketFence bloquea automáticamente los equipos de particulares en la red, además de usar Snort, OpenVAS Nessus como fuente de información, PacketFence puede combinar los siguientes mecanismos de detección para bloquear efectivamente acceso a la red de estos dispositivos no deseados:

DHCP de huellas dactilares

PacketFence puede bloquear los dispositivos en función de su huella digital DHCP. Casi todos los sistemas que operan allí tienen una huella digital única DHCP. PacketFence puede hacer uso de esta información y bloquear el acceso de la red de estos dispositivos. Sobre la base de las huellas dactilares de DHCP, automáticamente podría bloquear, por ejemplo:

- Sony PlayStation o cualquier otro dispositivos de consolas de juegos de otros
- Puntos de acceso inalámbrico (WAP)
- teléfonos VoIP

User-Agent

PacketFence puede bloquear los dispositivos basados en el User-Agent que se activa cuando esos dispositivos particulares realizan actividad de la red utilizando su navegador web incorporado. El uso de este, automáticamente podría bloquear, por ejemplo:

- Apple iPod o dispositivos iPhone
- Cualquier equipo que utilice una versión antigua de Microsoft Internet Explorer

Las direcciones MAC

PacketFence puede bloquear el acceso a la red a los dispositivos que tienen un patrón específico de direcciones MAC. El uso de este, automáticamente podría bloquear, por ejemplo, todos los dispositivos de red de un proveedor específico.

Registro automático

Debido a que la mayoría de las redes de producción son muy grandes y complejas, PacketFence ofrece varios medios para registrar de forma automática a un cliente o dispositivo, estos pueden ser:

1.- Al dispositivo de red

Un dispositivo de red (Switch, AP, Wireless Controller) se puede configurar para registrar automáticamente todas las direcciones MAC que solicite acceso a la red. Es muy útil para una transición a la producción.

2.- Por las huellas dactilares de DHCP

Toma de huellas dactilares de DHCP se puede utilizar para registrar automáticamente los tipos específicos de dispositivos (ej. teléfonos VoIP, impresoras).

3.- Al proveedor de direcciones MAC

La parte vendedora de una dirección MAC se puede utilizar para registrar automáticamente los dispositivos de un proveedor. Por ejemplo, todos los productos de Apple podría ser automáticamente registrados con dicha regla.

Administración de la duración de acceso.

La duración de acceso a la red se puede controlar con los parámetros de configuración. Se puede configurar por fecha (por ejemplo, "Jue Ene 20 20:00:00 EST 2011"), o por un periodo determinado de tiempo (por ejemplo, "cuatro semanas a partir de primer acceso de red") o tan pronto como el dispositivo se vuelve inactivo. La expiración de

dispositivos registrados quedado registrada. Con un poco de personalización también es posible hacer esto sobre una categoría de dispositivos. El vencimiento también puede ser editado manualmente en función de cada nodo.

Ancho de banda de Contabilidad

PacketFence puede detectar automáticamente la cantidad de ancho de banda consumido por los dispositivos de la red. Gracias a su compatibilidad integrada con intrusiones, puede poner en nivel de acceso de cuarentena o el cambio de dispositivos que están consumiendo ancho de banda en exceso durante un periodo de tiempo en particular. PacketFence también tiene informes sobre el consumo de ancho de banda

Administración de Los dispositivos flotantes de red

Un dispositivo de red flotante es un punto de acceso (AP) que se puede mover alrededor de su red y que está conectado a los puertos de acceso. Una vez configurado correctamente, PacketFence reconocerá los dispositivos de red flotante y configurará los puertos de acceso se suele permitir varias VLAN y más direcciones MAC. En este punto, el dispositivo de red flotante también puede acceder a la red a través de PacketFence. Una vez que el dispositivo está desconectado PacketFence retorna a configuración original.

Autenticación flexible

PacketFence puede autenticar a los usuarios que utilizan varios protocolos y normas. Esto le permite integrar PacketFence en su entorno sin necesidad de que los usuarios tengan otro nombre de usuario y contraseña. Las fuentes de autenticación son los siguientes:

- Microsoft Active Directory
- Novell eDirectory
- OpenLDAP
- Cisco ACS

- RADIUS (FreeRADIUS, radiador, etc)
- Archivo de usuario local

Redes enrutadas

La arquitectura de PacketFence le permite trabajar en redes enrutadas. El servidor puede estar ubicado en el centro de datos y todavía las sucursales pueden acceder satisfactoriamente al servidor.

Implementación gradual

Debido a la naturaleza intrusiva de control de acceso a la red, PacketFence viene con controles de grano fino a la hora de la implementación, automáticamente se puede pre-registrarse nodos, pero también se puede controlar el nivel de un acceso de un switch y por puerto-o.

Pass-Through

PacketFence puede ser configurado para permitir el acceso a los recursos especificados incluso cuando el nodo está en el aislamiento. Esto le permite dar acceso a herramientas específicas o parches a través del portal cautivo.

De alta disponibilidad

PacketFence se desarrolla con una alta disponibilidad en mente. Todos los despliegues se realizan utilizando activo-pasivo de alta disponibilidad así que la solución se ha demostrado en ese sentido.

Hardware soportado

PacketFence es compatible con hardware de red de varios proveedores y trabaja con estas tecnologías en una forma integrada.

Basado en estándares.

PacketFence está construido utilizando estándares abiertos para evitar la dependencia de un proveedor. Entre las normas que Packetfence permite se encuentran:

- 802.1X
- Simple Network Management Protocol (SNMP)
- La gestión estándar de SNMP base de información Netflow / IPFIX
- Wireless ISP Roaming (WISPr)

Extensible / fácilmente personalizable

PacketFence tiene un par de puntos de extensión donde se puede anular el comportamiento predeterminado de PacketFence con un poco de código Perl. La API se ha diseñado para ser fácil de entender con sólo un par de puntos de entrada de alto nivel. Además, al actualizar, PacketFence no reemplaza los archivos en los puntos de extensiones, de esta manera se mantiene su comportamiento en las actualizaciones.

Las plantillas de portal cautivo, también son fácilmente personalizables con HTML y CSS, se construyen utilizando la plantilla de Perl Toolkit.

2.4 POLÍTICAS DE SEGURIDAD

Las políticas de seguridad son normas que marcan el comportamiento de una red con relación a su seguridad. Definir políticas de seguridad de una red significa desarrollar procedimientos y planes que protejan a los recursos de la red contra pérdidas y daños. Es importante tener políticas de seguridades bien concebidas y efectivas, ya que de ellas depende que una organización pueda protegerse. Las políticas de seguridad son óptimas cuando los recursos de la organización están bien protegidos.

Lo primero y más importante para que un administrador de red pueda elaborar las políticas de seguridad de su organización, es identificar qué tipo de servicios y recursos se permiten a los usuarios acceder y cuales tendrán restricción debido a riesgos de seguridad.

2.4.1 Políticas De Seguridad Local

Una organización puede tener múltiples lugares y en cada lugar sus propias redes. Si la organización es grande lo más probable es que cada lugar tenga diferentes administraciones con diferentes objetivos. Si los lugares no están interconectados entre sí a través de una red interna, estos pueden tener sus propias políticas locales, pero si estos lugares están interconectados entre si las políticas de seguridad deben tener metas comunes.

Las políticas de seguridad local deberán tomar en consideración la protección de sus recursos.

Debido a que los lugares están conectados a otras redes, las políticas deben considerar las necesidades de seguridad y requerimientos de las otras redes interconectadas.

2.4.2 Objetivos De Las Políticas De Seguridad

Los objetivos del uso de una política de seguridad son:

- Informar a los consumidores de la red las obligaciones que tienen para proteger los recursos.
- Especificar los mecanismos a través de los cuales los requerimientos establecidos pueden ser cumplidos.
- Proveer una guía que permitirá implementar, configurar y controlar los sistemas de la red para determinar su conformidad con la política.

2.4.3 Componentes De Las Políticas De Seguridad

Los principales componentes de una política de seguridad son:

- **Política de Privacidad:** Define expectativas de privacidad con respecto a monitoreo, actividades y acceso a recursos de la red.
- **Política de acceso:** Permite definir los derechos de acceso y privilegios para protección ante una pérdida.
- **Política de autenticación:** Se establece un servicio confiable a través del establecimiento de contraseñas o firmas digitales.
- **Política de Administración de la red:** Describe como pueden manipular las tecnologías los encargados de la administración interna y externa.

Al diseñar una política de seguridad, debemos dar respuestas a las siguientes preguntas:

- ¿Qué recursos se tratan de proteger?
- ¿De quién se tratan de proteger los recursos?
- ¿Cuáles y cómo son las amenazas que afectan tales recursos?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas pueden ser implementadas para proteger el recurso?
- ¿Cuál es el costo de tal medida y en qué tiempo puede ser implementada?
- ¿Quién es el administrador?

2.4.4 Elementos De Una Política De Seguridad Informática

Los elementos que se deben tomar en cuenta son:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

2.4.5 Parámetros Para Establecer Políticas De Seguridad

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.

- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.
- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

2.5 ACERCAMIENTO A LAS POLÍTICAS DE SEGURIDAD

Para desarrollar las políticas de seguridad en una organización es necesario considerar los siguientes pasos:

- **Determinar la importancia y el riesgo de los recursos con que dispone la organización:** Para esto se realiza un análisis de riesgo de cada recurso en el cual se reconoce, la importancia en el normal funcionamiento de la organización y el riesgo o peligro al que está expuesto. Con este paso se logra descubrir los puntos más sensibles de la red.
- **Determinar la relación entre los usuarios y los recursos:** Para esto es necesario distinguir qué tipos de usuarios van a tener acceso a los recursos, y cuál es el comportamiento adecuado de los usuarios frente a los recursos.
- **Diseñar un modelo de seguridad:** Con los dos pasos anteriores desarrollados, ya es posible diseñar una estrategia de seguridad para brindar protección a los

puntos más sensibles de la red. Para esto es necesario aplicar los conocimientos de arquitecturas y tecnologías de firewalls. La información que se recopile en los pasos relatados anteriormente puede ser almacenada en la siguiente tabla:

Tabla II.I: Formato para establecer Políticas de Seguridad.

Recursos de la Red			Probabilidades de Riesgo	Tipo de Usuario de quienes protegerse	Medidas de Protección
Código	Nombre	Importancia			

Las columnas de la tabla describen la siguiente información:

- **Código del recurso:** es una identificación interna del recurso asignada por el administrador (información del 1er. paso).
- **Nombre:** es el nombre con que se reconoce al recurso (Información del 1er. paso).
- **Importancia:** En este campo se anota el grado de importancia del recurso en el normal funcionamiento de la organización. Puede ser evaluada en una escala numérica de 0 a 10, o usando expresiones difusas en lenguaje natural como: alta, moderada, baja, etc. [SIYA95].
- **Probabilidades de Riesgo:** Esta columna contiene la probabilidad de riesgo de que se den sobre cada recurso. Puede ser evaluada con valores numéricos o con expresiones difusas en lenguaje natural como en el caso anterior de la columna de importancia (información del 1er. Paso).
- **Tipos de usuarios de quienes protegerse:** Es una columna que describe que tipos de usuarios pueden ocasionar daños a los recursos de la red interna dependiendo de la accesibilidad tanto física como remota a dichos recursos (Información del 2do. paso).

- **Medidas de protección:** Contiene valores como: permisos del sistema operativo para archivos y directorios, alertar para servicios de red, firewalls para hosts y dispositivos de red, o cualquier otro tipo de descripción del tipo de control de seguridad (Información del 3er. paso).

En este acercamiento a las políticas de seguridad se desarrollara el primer paso (análisis de riesgo) y los dos siguientes, en las secciones 2.5. Uso y responsabilidades de la red y 2.6. Modelo de seguridad respectivamente, debido a la extensión de estos temas.

2.5.1 Análisis De Riesgo

Cuando se diseñan políticas de seguridad es importante entender que la razón para crearlas es asegurar que los mayores esfuerzos de protección se enfoquen a los puntos más importantes de la red. Esto significa que hay que entender que recursos de la red requieren ser protegidos y cuales son más importantes que otros. Además, hay que identificar la fuente de peligro de la cual se están protegiendo los recursos para brindar el tipo de protección que necesitan los recursos.

Para iniciar este análisis es necesario que el administrador tome en consideración las respuestas a las siguientes preguntas:

- ¿Qué es lo que necesita proteger?
- ¿De qué o quienes necesita proteger a los recursos?

En las siguientes sub-secciones se despejara estas incógnitas y se detallara como se efectúa el análisis de riesgo.

2.5.2 Identificación De Los Recursos

A continuación se provee una lista de los recursos que deberían ser considerados en la estimación de amenazas:

- Hardware: Procesadores, tarjetas, teclados, terminales, computadoras personales, impresoras, disqueteras, líneas de comunicación, servidores de terminal, ruteadores, etc.
- Software: programas fuentes, programas objetos, utilitarios, programas de diagnóstico, sistemas operativos, programas de comunicación, etc.
- Datos: durante ejecución, almacenados en línea, archivados, respaldos, archivos de auditoría, base de datos, etc.
- Personas: usuarios, operadores, etc.
- Documentación: en programas, hardware, sistemas, procedimientos locales administrativos, etc.
- Suministros: medios magnéticos, formas, etc.

2.5.3 Identificación De Amenazas

Para cada recurso es necesario establecer que tipos de peligro puede correr en su normal funcionamiento, para esto se hace una revisión de todos los posibles riesgos que puede sufrir cada recurso de acuerdo a la clasificación de tipos de ataques.

2.5.4 Cálculo Del Riesgo

El riesgo debe ser graduado en base a dos factores:

- Estimación de riesgo ante la pérdida del recurso → **(R)**
- Estimación de la importancia del recurso en el normal funcionamiento de la red → **(W)**

Estas variables pueden tomar valores numéricos o difusos mediante términos lingüísticos. Por ejemplo, al riesgo de pérdida de un recurso (R) se le puede asignar un valor de 0 hasta 10; donde 0 representa ningún riesgo, y 10 representa alto riesgo. Similarmente, a la importancia de un recurso (W) se le puede asignar un valor entre 0 y 10; donde 0 representa ninguna importancia y 10 significa alta importancia. El peso total

de riesgo de un recurso entonces es el producto del valor del riesgo y su importancia. Se podría expresar de la siguiente manera:

$$W_{R_i} = R_i \cdot W_i$$

Dónde:

W_{R_i} = Peso total de riesgo del recurso i.

R_i = Riesgo del recurso i.

W_i = Importancia del recurso i.

En donde "0" es el producto aritmético de los valores de R_i y W_i [SIYA95].

Tabla II.II: Recursos de la Red

Recursos de la Red		Riesgo del Recurso (R)	Importancia del Recurso (W)	Peso Total del Riesgo (R O W)
Número	Nombre			

Representada la Tabla II.II aun no se puede completar, ya que hasta ahora solo se ha podido listar la importancia y el riesgo de los recursos. Falta por determinar las columnas: tipos de usuarios de quienes proteger y las medidas de protección. En las siguientes secciones se detallan los métodos para obtener la información faltante.

2.6 USO Y RESPONSABILIDADES EN LA RED

Otro aspecto que debe considerarse en la definición de las políticas de seguridad es el uso y responsabilidades en la red. A continuación se da una serie de preguntas que ayudarían a determinar el, uso y responsabilidades en una red:

- ¿A quién es permitido el uso de recursos?
- ¿Cuál es el uso apropiado de los recursos?
- ¿Quién está autorizado a otorgar accesos y aprobar usos?

- ¿Cuáles son las responsabilidades de los usuarios?
- ¿Cuáles son las responsabilidades del administrador?
- ¿Qué hacer con la información susceptible?

2.6.1 Identificando A Quien Es Permitido El Uso De Recursos De La Red.

Es necesario llevar un registro de todos los usuarios con sus alcances y características por cada recurso para luego, identificar a quienes es permitido el uso de los mismos. Por ejemplo:

- Usuarios internos: Son las cuentas asignadas a personas de la red interna. Estas personas pueden tener acceso físico y remoto a los recursos. Pueden constituirse en enemigos potenciales de la seguridad.
- Usuarios externos: Son usuarios de Internet. Estos usuarios pueden tener acceso remoto a la red y perpetrar un ataque.
- Nombres de grupos: Son un conjunto de usuarios clasificados de acuerdo al carácter de la organización. Por ejemplo: gerentes, asistentes, etc., para una organización comercial. Estos grupos pueden contar con usuarios internos o externos, por lo que pueden ganar acceso físico o remoto a la red interna.

2.6.2 Identificando El Uso Apropiado De Un Recurso.

Después de determinar cuáles son los usuarios que pueden acceder a los recursos de la red, se debe proveer de guías para el uso adecuado de estos recursos. Estas guías dependerán de la clase de usuario (interno, externo, grupos) y del recurso (servidores: Telnet, FTP, de impresión, etc.). Las guías de usuarios deben definir que se considera como uso aceptable, inaceptable y restringido por cada recurso. Estas guías se colocaran dentro de un documento llamado “Uso aceptable de políticas” (UAP).

El UAP debe indicar claramente a los usuarios que estos son responsables por sus acciones. No tiene sentido que se construyan mecanismos de seguridad si el usuario libera información haciendo la disponible para posibles atacantes.

A continuación se presentan algunas preguntas que servirán de guía para que el administrador pueda un UAP:

- ¿Está permitido forzar contraseñas? : Si a los usuarios se les ha permitido forzar las contraseñas pueden infiltrarse en cualquier sistema y provocar un ataque.
- ¿Está permitido el interrumpir servicios? : No todos los usuarios deben tener privilegios (mayor acceso a recursos) sobre los sistemas, ya que por ignorancia o malicia, pueden provocar daños (interrupción de servicios, eliminación de datos, etc.).
- ¿Está permitido al usuario modificar archivos que no son de su propiedad?: Se debe controlar el ambiente sobre el cual interaccionan los usuarios, caso contrario, estos pueden modificar archivos que no son de su propiedad y provocar daños.
- ¿Podrían los usuarios compartir sus cuentas?: Es aconsejable establecer que las cuentas de usuarios son personales y no se deben compartir. De esta manera si un usuario interno causa un daño se sabrá de que persona se trata.

2.6.3 Determinando Quien Está Autorizado Para Otorgar Acceso Y Aprobar El Uso.

Las políticas de seguridad en una red deben establecer quien está autorizado para otorgar acceso a los servicios de la red. Si el administrador no tiene control de quien está otorgando acceso al sistema, es difícil controlar quien está usando la red. Si el administrador puede identificar a las personas que están encargadas de dar acceso a la red, se puede establecer qué tipo de acceso o control ha sido otorgado. Esto ayuda a identificar la causa de posibles agujeros en la seguridad, como por ejemplo el otorgamiento de privilegios a usuarios que no lo ameritan.

Hay que considerar los siguientes factores para determinar quién o quienes darán acceso a los servicios en las redes:

- ¿Se otorgara el acceso a servicios desde un punto central?
- ¿Qué métodos se usaran para crear cuentas?

Si la organización es grande y descentralizada, se pueden tener diversos puntos, por ejemplo uno para cada departamento, con propia responsabilidad sobre su red. En este caso, se debe tener una guía global de que tipos de servicios son permitidos para cada clase de usuario. Por otro lado, la administración centralizada puede crear problemas cuando los departamentos quieran tener más control sobre sus propios recursos.

El administrador necesitara acceso especial a la red, pero otros usuarios también pueden necesitar ciertos privilegios. Es cierto que al restringir el acceso y no otorgar privilegios a los usuarios, hacemos más segura a la red, pero podríamos hacer que los usuarios no cumplan eficientemente con sus tareas. Por lo tanto, es necesario un balance entre denegar privilegios para hacer más segura la red y otorgar privilegios a las personas que realmente los necesiten.

Si existe un gran número de redes y administradores es difícil mantener un seguimiento de que permisos han sido otorgados. Después que el usuario hace el requerimiento de privilegios y este es autorizado por el usuario supervisor, el administrador debe documentar los cambios producidos. A continuación se presenta una tabla cuyo formato sirve para este propósito:

Tabla II.III: Recursos de la Red

Recursos de la Red		Tipo de Usuario	Tipo de Acceso
Código	Nombre		

Tipos de usuarios: Los diversos tipos de usuarios que posee una organización. Por ejemplo, usuario externo, interno, etc.

Tipo de acceso: puede ser usado para una descripción del acceso, por ejemplo “solo lectura” o “solo ejecución”, etc.

2.6.4 Determinando Las Responsabilidades De Los Usuarios.

Las políticas de seguridad deben definir los derechos y responsabilidades para usar los recursos y servicios de la red. A continuación se citan una serie de aspectos a considerar:

- ¿Que se considera abuso en términos de uso de recursos en la red?
- ¿Está permitido a los usuarios compartir cuentas o dejar que otros las usen?
- ¿Deberían los usuarios revelar sus contraseñas en bases temporales para permitir que otros trabajen con sus cuentas?
- En las políticas de contraseñas: ¿Cuan frecuente deben los usuarios cambiar sus contraseñas?
- ¿Son los usuarios responsables de sacar respaldos de sus datos o es responsabilidad del administrador?
- ¿Qué acciones legales se tomarían en caso de revelación de información?
- Una política concerniente a correos controversiales, listas de correo o discusión. Establecer que tipos de foros serán permitidos, contenido de correo, etc.

2.6.5 Determinando Las Responsabilidades Del Administrador Del Sistema.

Cuando se corre riesgo en la seguridad de un sistema, el administrador puede tener la necesidad de recoger información de los archivos del sistema, incluyendo los del directorio “home” de cada usuario. Por otro lado el usuario también requiere de cierta privacidad.

Entonces surge una controversia de la privacidad y derechos del usuario con la necesidad de los administradores.

Las políticas de seguridad deben especificar si el o los administradores pueden examinar los directorios privados para el diagnóstico de problemas e investigaciones de

violaciones a la seguridad. También se adjuntarían las respuestas a las siguientes preguntas:

- ¿Puede el administrador monitorear o leer archivos de un usuario por cualquier razón?
- ¿Pueden los administradores tener el derecho de examinar la red y su tráfico?

2.7 PLAN DE ACCIÓN CUANDO LAS POLÍTICAS DE SEGURIDAD SON VIOLADAS

Un aspecto aparte del método para desarrollar políticas de seguridad anteriormente detallado es el establecimiento de acciones de contingencia. Si las políticas de seguridad son violadas, el sistema está abierto a cualquier tipo de ataque. Algunas veces es fácil detectar cuando una política ha sido violada, pero otras veces puede ser indetectable. Los procedimientos de seguridad que el administrador implemente minimizan la posibilidad de que la infracción no sea detectada. Cuando se encuentre una violación a las políticas, se la debe clasificar si fue por negligencia, por accidente o error, ignorancia de las reglas, o deliberadamente. Para cada una de estas circunstancias, las políticas de seguridad deben proveer la guía necesaria de las acciones a tomar.

2.7.1 Respuesta A Violaciones Por Parte De Usuarios Internos

Ante violaciones por parte de los usuarios internos se pueden tener las siguientes situaciones:

- Un usuario local viola las políticas del sistema local.
- Un usuario local viola las políticas de un sistema externo.

Si se trata del primer caso, el administrador puede tener más control sobre qué tipo de respuesta se debe tomar por la falta cometida. En el segundo caso, si un usuario local ha irrumpido en la seguridad de un sistema externo, la situación es muy complicada debido a que involucra a otra organización, y la respuesta que se tome sería discutida con la

organización cuya política ha sido violada. Además, tendría que consultarse con organizaciones internacionales especializadas en leyes de seguridad de computadores.

2.7.2 Respuesta A Violaciones Por Parte De Usuarios Externos

En el caso de que usuarios externos (usuarios de Internet, ajenos a la organización), al igual que en el segundo caso de violaciones de usuarios internos a un sistema externo, la situación es complicada. Dependiendo de la gravedad de la falta, lo recomendable es que la organización interna se ponga en contacto con la organización a la que pertenece el usuario externo a fin de discutir la acción a tomar. Como medida adicional se debe tomar en consideración los criterios de agencias de leyes internacionales que definen protocolos para estos casos.

2.7.3 Estrategias De Respuesta

Ante las posibilidades de respuesta anteriormente descritas, existen dos tipos de estrategias de respuestas opuestas:

- Proteger y Proceder
- Perseguir y Acusar

2.7.3.1 Proteger Y Proceder

Si los administradores sienten que la organización es muy vulnerable, deben elegir esta estrategia. La meta de esta estrategia es proteger inmediatamente la red y restaurarla a su normal funcionamiento para que los usuarios continúen con su trabajo. Para hacer esto el administrador debe interferir con las acciones de los intrusos y prevenir futuros problemas. Al final, se requiere hacer un análisis de la cantidad del daño hecho.

A veces no es posible restaurar inmediatamente la red y ponerla en su normal funcionamiento resulta un proceso lento. También puede ser necesario aislar segmentos de red y apagar los sistemas con el objetivo de prevenir accesos no

autorizados. Una desventaja de este método es que los intrusos conocen si han sido detectados y evitan ser perseguidos. Además en un futuro ya conocen los puntos débiles del sistema de seguridad.

La estrategia “proteger y proceder” debe ser usado bajo las siguientes condiciones:

Si los recursos de la red no están bien protegidos: Si los recursos están desprotegidos, es muy probable que se originen ataques que ocasionen daños potenciales y urgentes de restaurar.

Si una actividad intrusa continuamente resulta un gran daño y riesgo financiero:

Si los intrusos ocasionan graves daños financieros, es necesario restaurar antes de que se haga más grande.

Si existe un considerable riesgo para los usuarios de la red: Los usuarios internos pueden ser objeto de robos de contraseñas, robo de información personal, números de cuentas de banco, tarjetas de crédito, etc.), etc. Esto puede constituirse en una puerta abierta para los intrusos.

Si el costo de una persecución a un intruso es muy alto: Para perseguir a un posible intruso es necesario tener mecanismos de monitoreo, programas especiales o trampas, los cuales pueden tener un costo muy elevado para una organización.

2.7.3.2 Perseguir Y Acusar

Este método tiene como meta permitir intrusos para perseguir sus acciones mientras se monitorea sus actividades. Este método no establece restricciones a los potenciales intrusos, de tal manera que estos no se dan cuenta que están siendo monitoreados. Es recomendado por agencias de leyes, debido a que se llevan pruebas a estas agencias para que puedan iniciar una acusación legal contra los intrusos.

Una posible manera de monitorear a los intrusos sin que puedan causar daños al sistema es construir una cárcel, la cual define un ambiente simulado con datos falsos en el que los intrusos puedan ser monitoreados y registrados sin sospechar que los están vigilando.

Es recomendable instalar una cárcel en una máquina de sacrificio que se encuentre en un segmento aislado de una red para minimizar el riesgo de las actividades del intruso. Se puede construir una cárcel usando dos métodos: modificando el sistema operativo o utilizando un programa especial o trampa. El primer método depende del grado de manejo del sistema operativo. La persona que modifique el sistema operativo tiene que tener gran dominio sobre las variables de ambiente, procesos, y comandos del sistema operativo. El segundo método consiste en utilizar programas especiales (comerciales o públicos) sobre el sistema operativo, los cuales pueden ser complejos de instalar.

El método “Perseguir y acusar” puede ser usado bajo las siguientes condiciones:

- Si los recursos y sistemas están bien protegidos: Si los recursos son seguros, el administrador no se preocupa por restaurar y se dedica a perseguir a los autores del daño.
- Si la red ha sido centro de ataques de intrusos y estos no dejan de hacerlo: El administrador puede cansarse de restaurar los daños frecuentemente y dedicarse a perseguir a los causantes.
- Si la red es apropiada: Si la red de la organización es segura como para incurrir el riesgo de permitir intrusos, es decir que existan mecanismos de seguridad, monitoreo, registro de acciones se puede obtener pruebas para acusar sin sufrir un ataque.

- Si las herramientas de monitoreo y registro pueden archivar bastante información: Si la capacidad de registro es completa se pueden recoger evidencias y posteriormente acusar al intruso.
- Si existe disponibilidad para acusar: En el caso de que un usuario interno sea el causante de un daño, la organización deberá sancionarlo; si se trata de un usuario externo, este tendría que ser denunciado a la organización a la que pertenece y establecer una demanda si ambas organizaciones están afiliadas a agencias de leyes de seguridad de computadores.

2.7.4 Contactos Y Responsabilidades Con Organizaciones Externas.

Las políticas de seguridad de red incluyen también la definición de procedimientos para interactuar con organizaciones externas que puedan tener contactos con agencias de leyes o expertos legales. En el Ecuador no existe aún ley o entidad alguna que delimite el comportamiento adecuado entre organizaciones nacionales que se conectan a Internet.

Por lo tanto lo recomendable es afiliarse a las organizaciones extranjeras que ofrecen ayuda (soporte) ante problemas de seguridad, como CERT (Computer Emergency Response Team), CIAC (Computer Incident Advisory Capability).

CAPITULO III

ANÁLISIS COMPARATIVO DE HERRAMIENTAS NAC OPENSOURCE

3.1 ANÁLISIS DE LA INFRAESTRUCTURA DE RED DE LA INSTITUCIÓN.

La Unidad Informática de la Dirección Provincial del Consejo de la Judicatura de Chimborazo cuenta con varios servicios que proporcionan a los funcionarios judiciales para el trabajo diario dentro de la institución. Por este motivo se necesita un control adecuado de los recursos de la red interna para asegurar el correcto funcionamiento de la misma.

Actualmente se carece de una forma eficaz de detectar o prevenir fallas de seguridad que puedan ocurrir dentro de la red interna, el fallo se detecta cuando se recibe la notificación de un usuario o por algún control realizado por los administradores de la Unidad Informática; ante esta situación y por la necesidad de detectar y prevenir fallas de seguridad en la red interna, de forma más rápida y segura surge la necesidad de implementar una solución que prevenga y detecte automáticamente las fallas de seguridad dentro de la LAN y notifique a los administradores de la red las ocurrencias. Esta solución puede consistir en la instalación de una herramienta que monitoree, identifique problemas y los notifique a las personas indicadas para su resolución.

Diagrama de Red del Consejo Nacional de la Judicatura de Chimborazo.

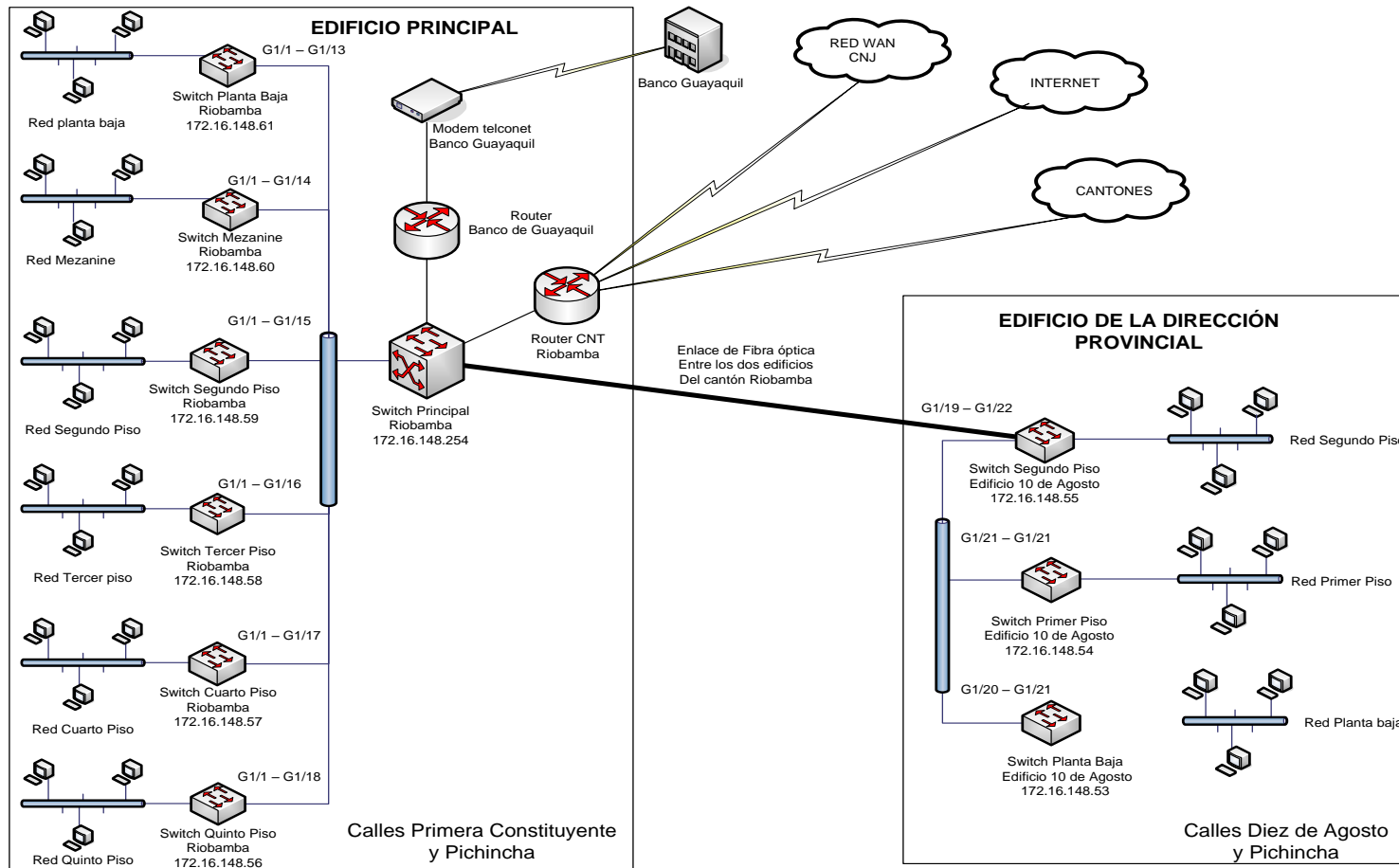


Figura III.01: Infraestructura de Red Actual para la Institución.

3.1.1 Subredes

La red de LAN de la institución está conformada por varias subredes, distribuidas entre las diferentes dependencias de la institución. Los rangos de las subredes mencionadas son:

Tabla III.I: Subredes de la Red de la Institución

NUMERO VLAN	NOMBRE VLAN	DESCRIPCIÓN
2	PENALES	Todos los equipos de los usuarios de la Sala de lo penal, Tribunales y Juzgados Penales y Presidencia del cantón Riobamba.
3	NIÑEZ	Juzgados de la Niñez y Oficina Técnica.
4	APOYO	Oficina de Sorteos, Citaciones, Auditorio, Aula de capacitación.
5	CIVILES	Sala Civil y Juzgados Civiles del cantón Riobamba.
6	SISTEMAS	En esta VLAN solo se encuentra los usuarios de sistemas, equipos de red como switch capa dos y capa tres y todos los servidores de la Función Judicial de Chimborazo.
7	ADMINISTRATIVOS	Dirección Provincial, Unidad Financiera y Defensoría pública.
8	OTROS JUZGADOS	Juzgados de Transito, Inquilinato y Trabajo.
9	COLTA	Todas las judicaturas localizadas en el cantón Colta.
10	GUAMOTE	Todas las judicaturas localizadas en el cantón Guamote.
11	PALLATANGA	Todas las judicaturas localizadas en el cantón Pallatanga
12	ALASI	Todas las judicaturas localizadas en el cantón Alasi.
13	GUANO	Todas las judicaturas localizadas en el cantón Guano.
14	CHUNCHI	Todas las judicaturas localizadas en el cantón Chunchi.

Del rango de direcciones asignado a la red de Chimborazo, están en varias subredes con la finalidad de asignar una subred a cada una de las Vlans, cada subred cuenta con 253 direcciones de host hábiles, la siguiente tabla muestra el direccionamiento asignado a las Vlans existentes.

Tabla III.II: Rangos de Direccionamiento de la Institución

VLAN	DIRECCIÓN SUBRED	RANGO DE DIRECCIONES DISPONIBLES	MASCARA SUBRED
Penales	172.16.144.0	172.16.144.1 – 172.16.144.253	255.255.255.0
Niñez	172.16.145.0	172.16.145.1 – 172.16.145.253	255.255.255.0
Apoyo	172.16.146.0	172.16.146.1 – 172.16.146.253	255.255.255.0
Civiles	172.16.147.0	172.16.147.1 – 172.16.147.253	255.255.255.0
Sistemas	172.16.148.0	172.16.148.1 – 172.16.148.253	255.255.255.0
Administrativos	172.16.149.0	172.16.149.1 – 172.16.149.253	255.255.255.0
Otros Juzgados	172.16.150.0	172.16.150.1 – 172.16.151.253	255.255.255.0
Guamote	172.16.151.0	172.16.151.1 – 172.16.151.62	255.255.255.192
Alausi	172.16.152.0	172.16.152.1 – 172.16.152.62	255.255.255.192
Colta	172.16.154.0	172.16.154.128 – 172.16.154.192	255.255.255.192
Chunchi	172.16.155.0	172.16.155.1 – 172.16.155.62	255.255.255.192
Pallatanga	172.16.156.0	172.16.156.1 – 172.16.156.62	255.255.255.192
Guano	172.16.157.0	172.16.157.1 – 172.16.157.62	255.255.255.192

3.1.2 Equipos de la Institución

3.1.2.1 Servidores

A continuación se detalla la información de los servidores existentes de la Dirección Provincial de Chimborazo, los mismos que se encuentran ubicados en la Unidad Informática.

Tabla III.III: Servidores de NAC.

SERVIDOR	DIRECCIÓN	MASCARA DE RED
Servidor Proxy, Correo, DHCP	172.16.148.1	255.255.255.0
Servidor Web	172.16.148.2	255.255.255.0
Servidor de Trámite Judicial	172.16.148.4	255.255.255.0
Servidor de Antivirus y Dominios	172.16.148.8	255.255.255.0
Servidor de Pensiones alimenticias	172.16.148.10	255.255.255.0
Servidor de Información	172.16.148.14	255.255.255.0
Servidor de Reloj	172.16.148.20	255.255.255.0
Servidor de Información al público	172.16.148.101	255.255.255.0
Servidor de Trámite Judicial Cantones	172.16.148.114	255.255.255.0

3.1.2.2 Equipos de Red

EDIFICIO PRINCIPAL (PRIMERA CONSTITUYENTE Y PICHINCHA).

A continuación se detalla el direccionamiento de los equipos que pertenecen a la Dirección Provincial de Chimborazo.

Tabla III.IV: Dispositivos de Conectividad de la Institución Ed. Principal.

EQUIPO DE RED	DIRECCIÓN IP DE ADMINISTRACIÓN	MASCARA DE RED
Switch Catalyst 4503 (Principal)	172.16.148.254	255.255.255.0
Switch Catalyst 2960 (Quinto piso)	172.16.148.56	255.255.255.0
Switch Catalyst 2960 (Cuarto piso)	172.16.148.57	255.255.255.0
Switch Catalyst 2960 (Tercer piso)	172.16.148.58	255.255.255.0
Switch Catalyst 2960 (Segundo piso)	172.16.148.59	255.255.255.0
Switch Catalyst 2960 (Mezanine)	172.16.148.60	255.255.255.0
Switch Catalyst 2960 (Planta baja)	172.16.148.61	255.255.255.0

EDIFICIO NUEVO (DIEZ DE AGOSTO Y PICHINCHA).

A continuación se detalla todos los switch existentes en el edificio ubicado en las calles Diez de Agosto y Primera constituyente.

Tabla III.V: Dispositivos de Conectividad de la Institución Ed. Nuevo.

EQUIPO DE RED	DIRECCIÓN IP DE ADMINISTRACIÓN	MASCARA DE RED
Switch Catalyst 2960 (Planta baja)	172.16.148.53	255.255.255.0
Switch Catalyst 2960 (Segundo piso)	172.16.148.54	255.255.255.0
Switch Catalyst 2960 (Tercer piso)	172.16.148.55	255.255.255.0

3.2 IMPLEMENTACIÓN DE HERRAMIENTAS NAC OPENSOURCE EN UN AMBIENTE DE PRUEBAS

Para implementar las herramientas NAC OpenSource se habilito un escenario de pruebas para instalar estas y no interferir en el funcionamiento diario de la institución.

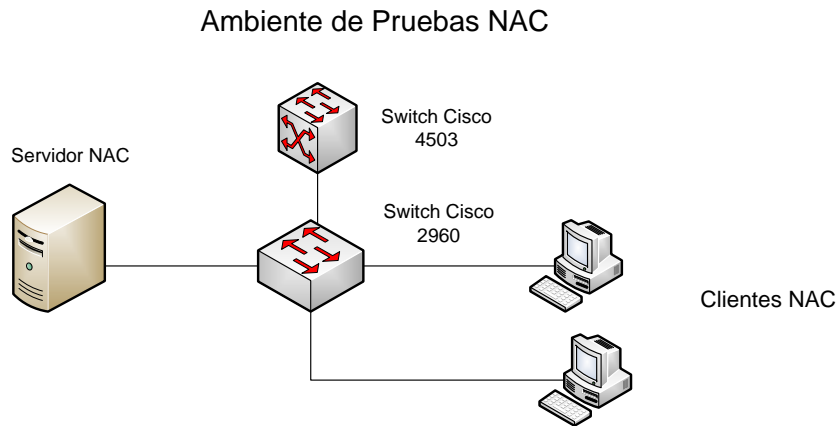


Figura III.02: Ambiente de Pruebas de NAC.

3.2.1 Pruebas Con La Herramienta FreeNAC

3.2.1.1 Interfaz de Escritorio

FreeNAC ofrece dos formas de administración remota la primera por medio de una aplicación de escritorio que se ejecuta sobre Windows que se la pueda descargar libremente de la página oficial. Y la segunda mediante una interfaz web que se instala con la herramienta.

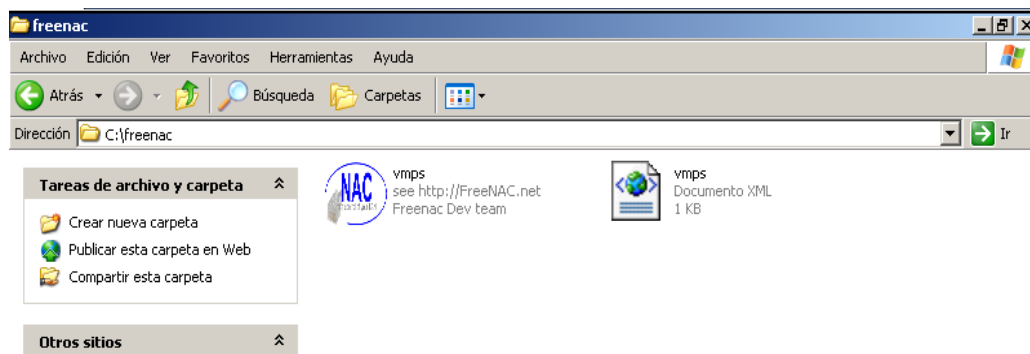
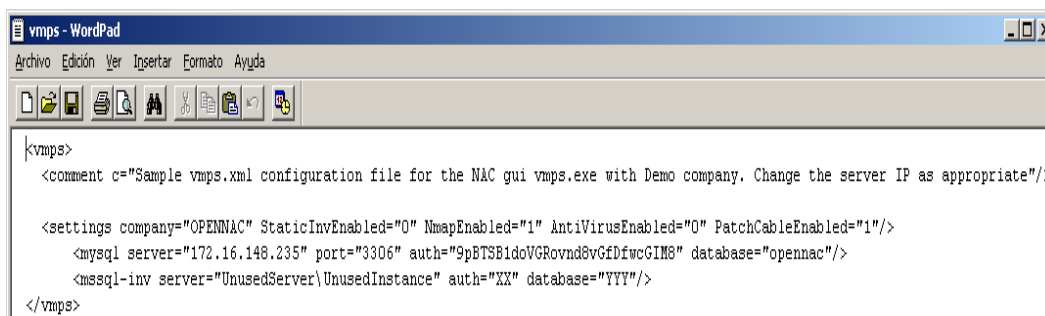


Figura III.03: Ejecución de interfaz de Escritorio

Para acceder a la herramienta de administración de escritorio se debe configurar un archivo de texto en formato xml que viene con la aplicación.



```
<vmps>
  <comment c="Sample vmps.xml configuration file for the NAC gui vmps.exe with Demo company. Change the server IP as appropriate"/>

  <settings company="OPENNAC" StaticInvEnabled="0" NmapEnabled="1" AntiVirusEnabled="0" PatchCableEnabled="1"/>
  <mysql server="172.16.148.235" port="3306" auth="9pBT5B1doVGRovnd8vGfdfwcGIN8" database="opennac"/>
  <mssql-inv server="UnusedServer\UnusedInstance" auth="XX" database="YYY"/>
</vmps>
```

Figura III.04: Configuración de Ingreso a FreeNac.

Luego solo se procede a ingresar a la aplicación. Para eso se presiona en el botón Connect.

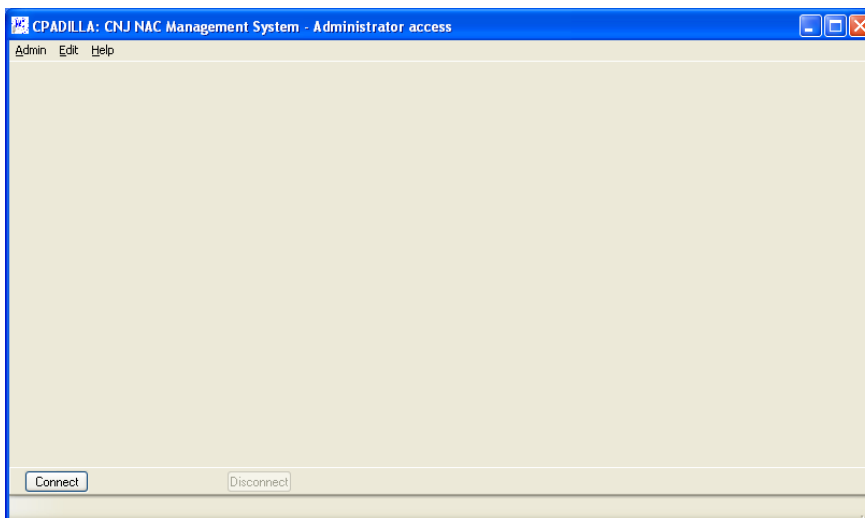


Figura III.05: Interfaz para la administración de FreeNac.

Al conectar muestra todos los últimos cambios que sucedieron en la LAN.

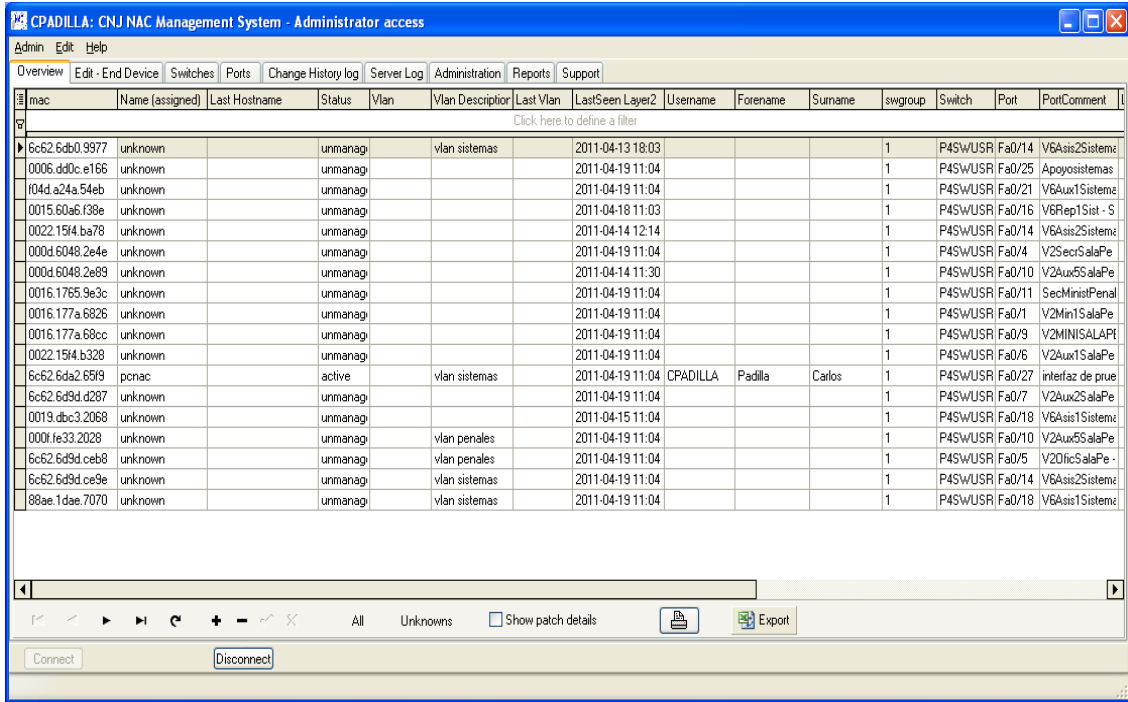


Figura III.06: Pantalla inicial de FreeNac.

Al ubicarnos sobre un dispositivo de la lista de la ventana anterior en la opción de Editar podemos modificar los dispositivos finales; como son el nombre, tipo, estado, entre otros.

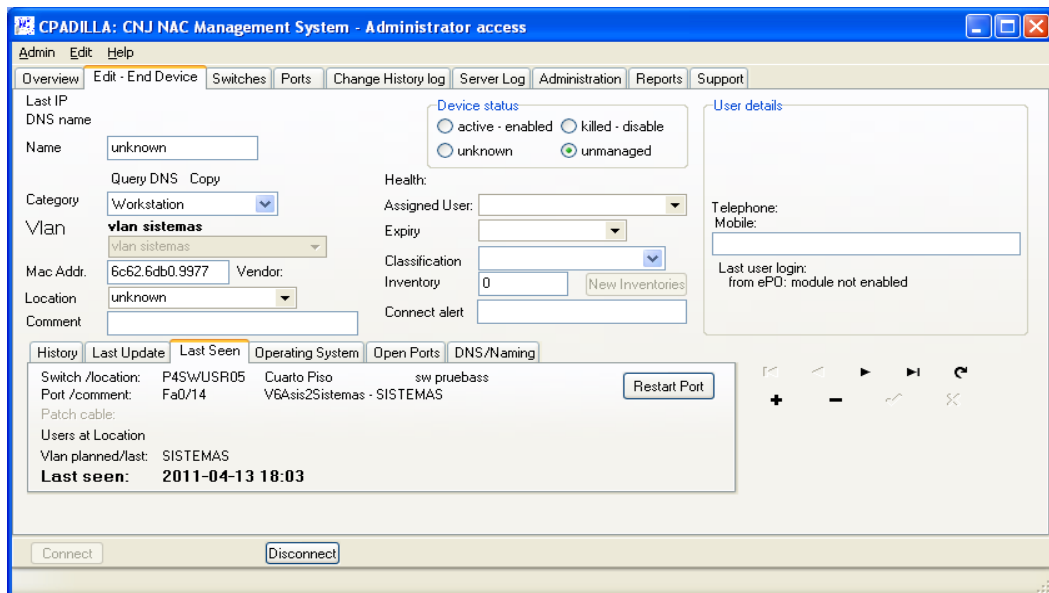


Figura III.07: Edición de Dispositivos Finales.

En la opción de Switchs podemos administrar cada uno de los Switchs de la red y configurar las diferentes opciones.

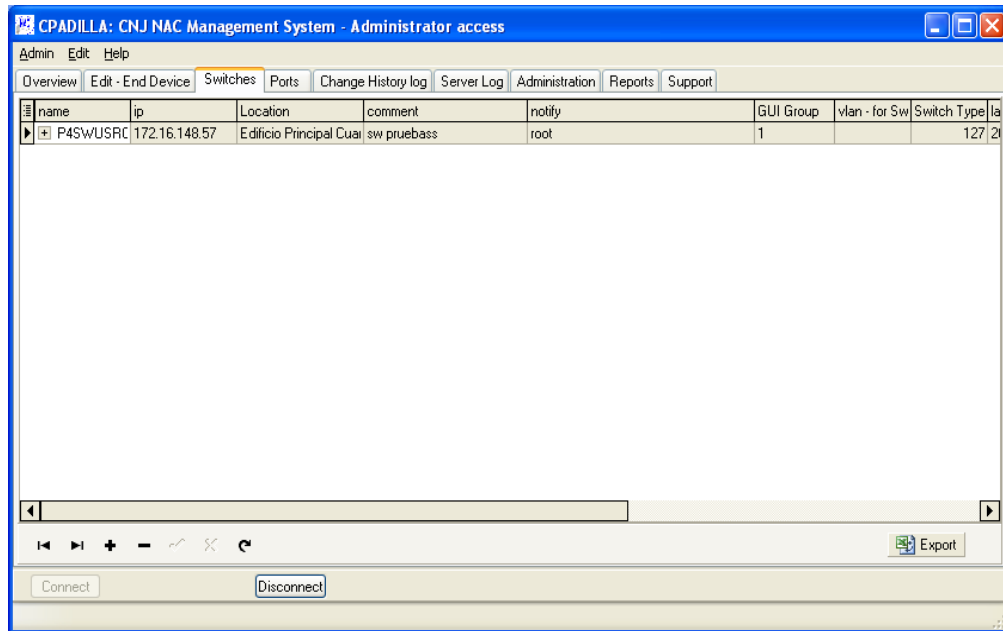


Figura III.08: Administración de Switchs.

También podemos administrar los puertos de cada Switch y permite detectar que equipo se conecta y a que VLAN pertenece.

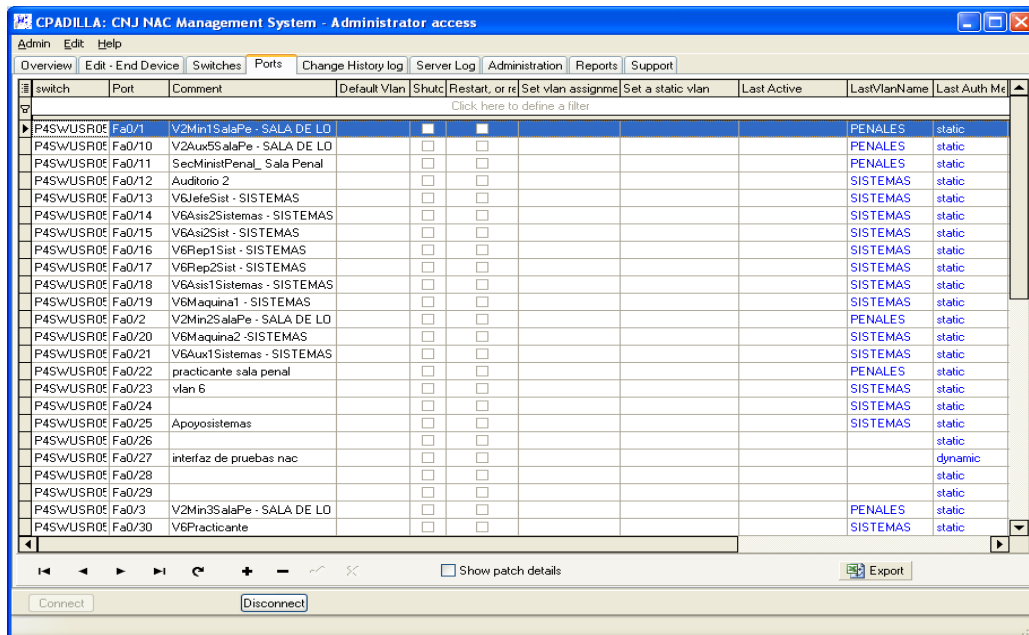


Figura III.09: Administración de Puertos de los Switchs.

En esta ventana podemos visualizar los mensajes de acceso al sistema.

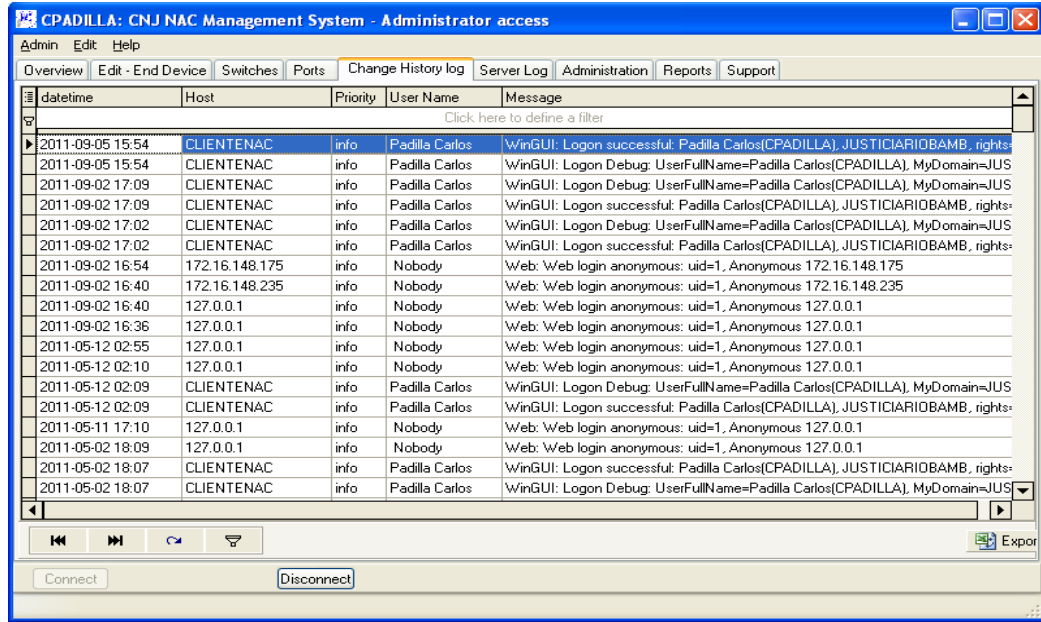


Figura III.10: Registro de Acceso a la interfaz de Administración.

Esta ventana nos muestra las operaciones que realiza el servidor.

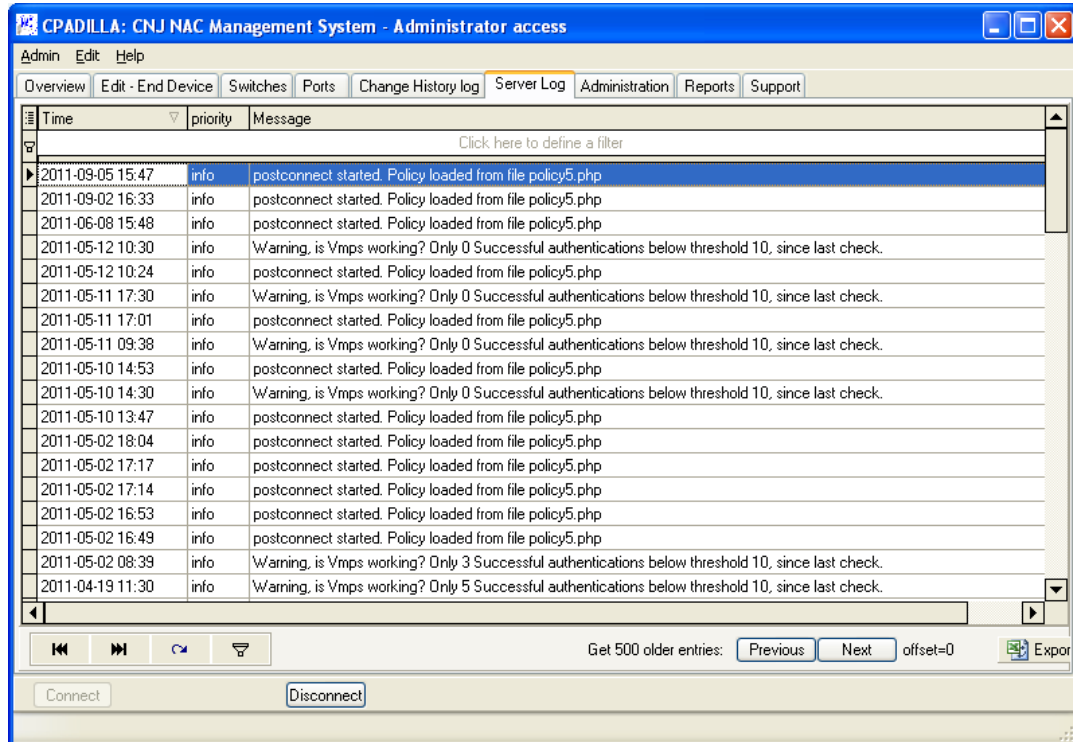


Figura III.11: Registro de Sucesos del Servidor.

En el menú de administración hay algunas opciones que podemos encontrar para configurar los parámetros de funcionamiento de la herramienta. La opción por defecto es Vlans.

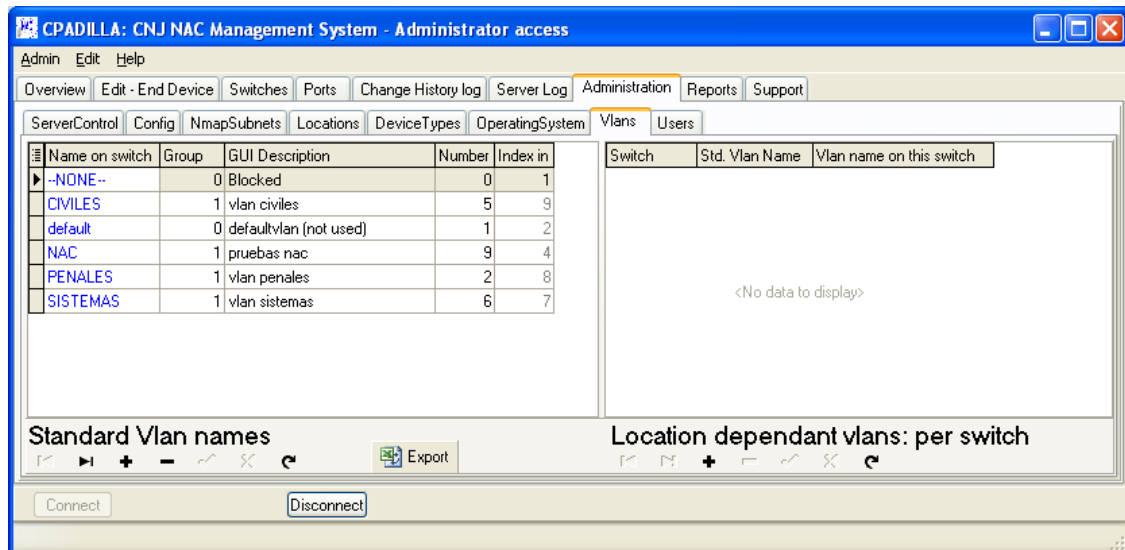


Figura III.12: Administración dinámicas de Vlans.

En la opción de ServerControl nos permite reiniciar los servicios de PACKETFENCE.

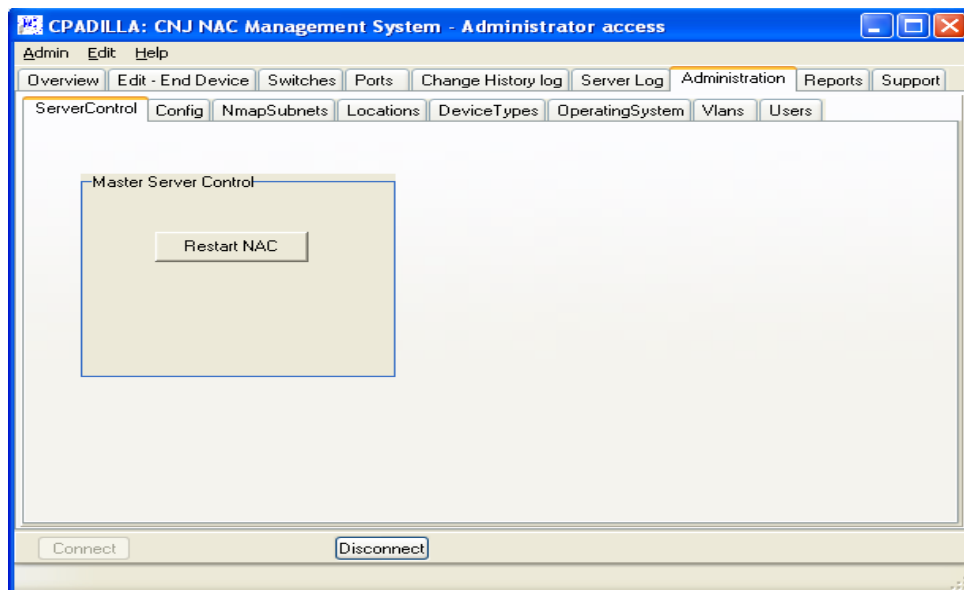


Figura III.13: Reinicio de la Herramienta.

En la opción de Config podemos encontrar las configuraciones generales de la herramienta.

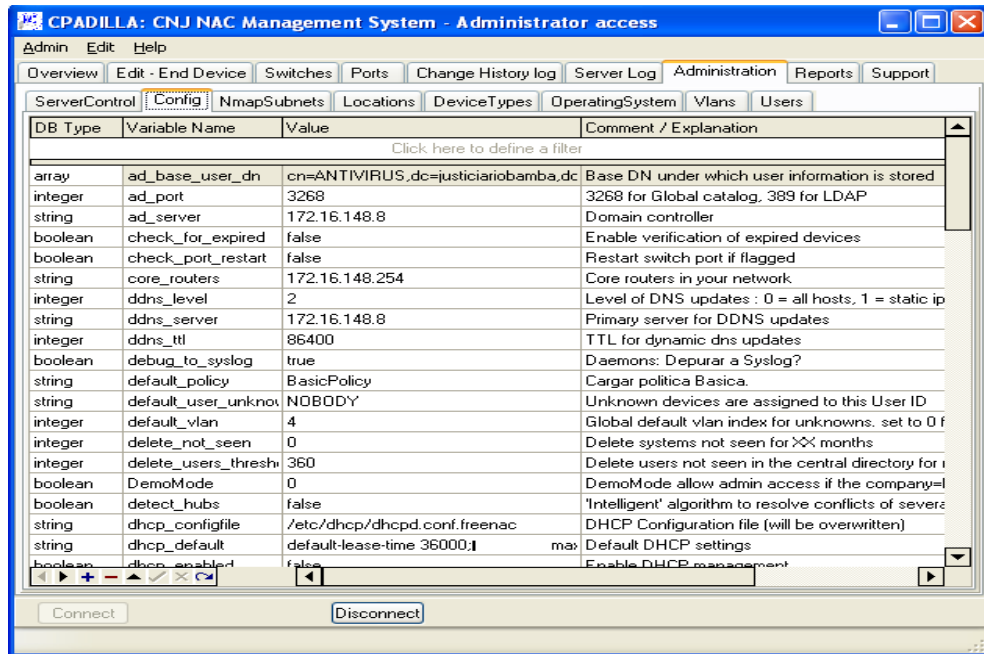


Figura III.14: Configuración de la Herramienta.

En esta opción establecemos las Vlan's que queremos supervisar con nmap.

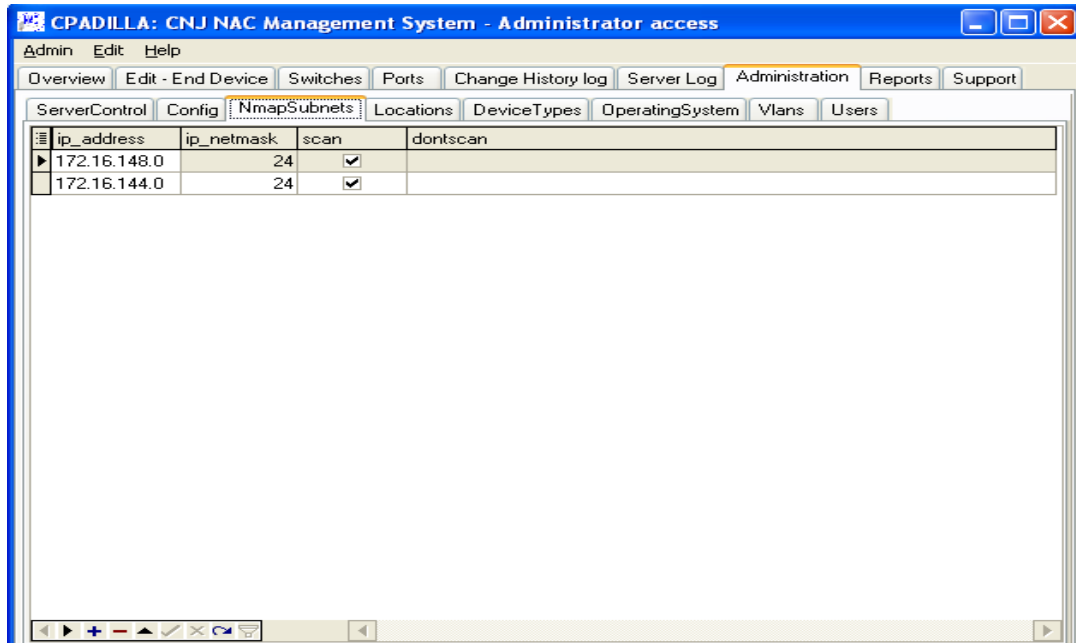


Figura III.15: Escaneo de Subredes.

Debemos ingresar manualmente las ubicaciones de los diferentes dispositivos.

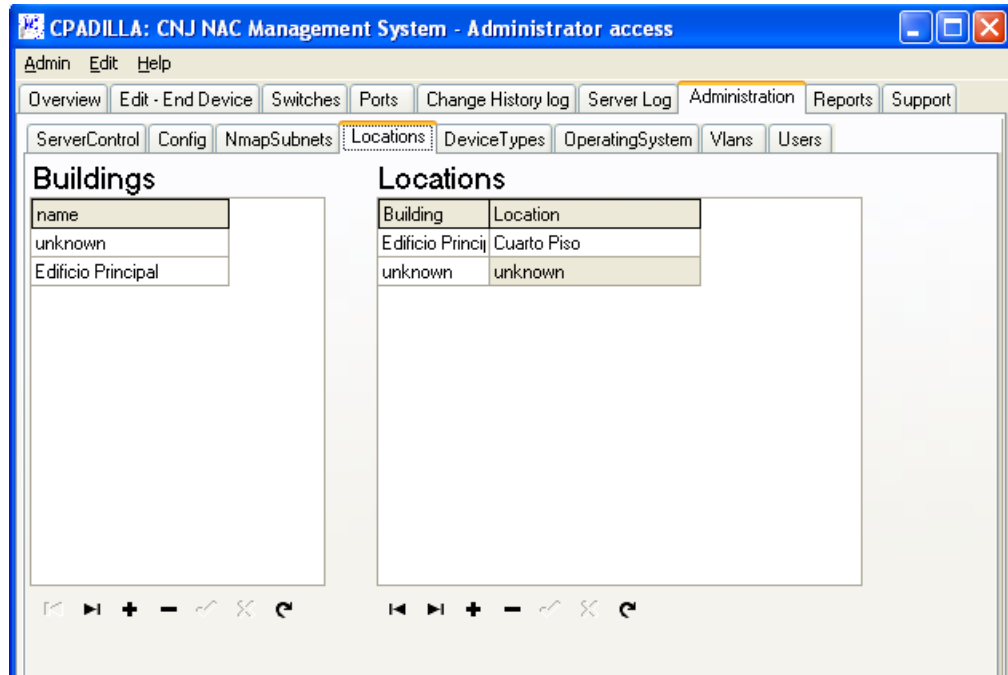


Figura III.16: Configuración de Ubicaciones Físicas.

Los Tipos de Dispositivos también son ingresados manualmente según las necesidades de quien utilice la herramienta.

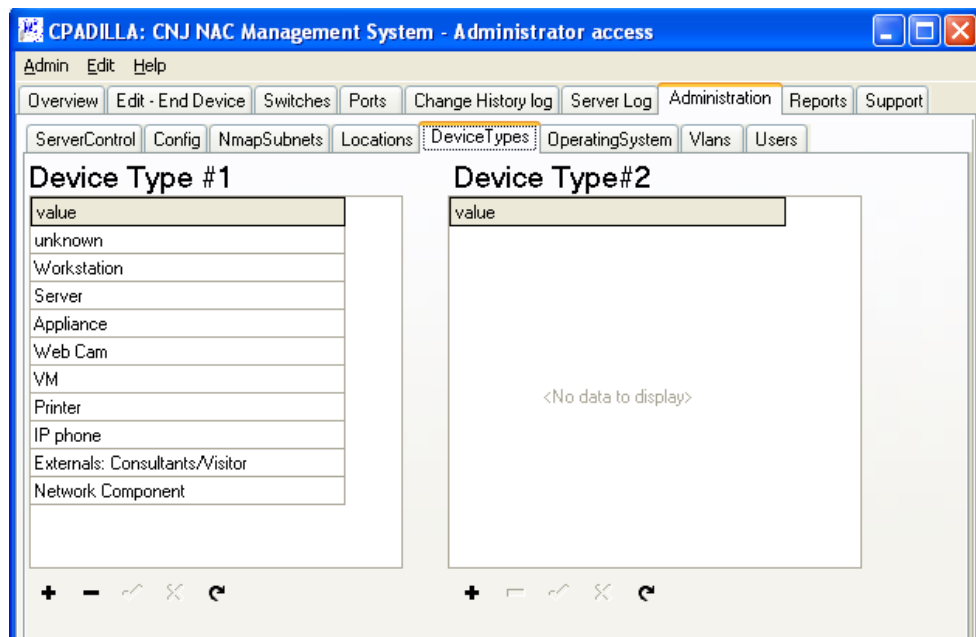


Figura III.17: Configuración de tipos de Dispositivos.

Lo sistemas operativos que se tiene también se deben ingresar para llevar el inventario de la herramienta de una forma correcta.

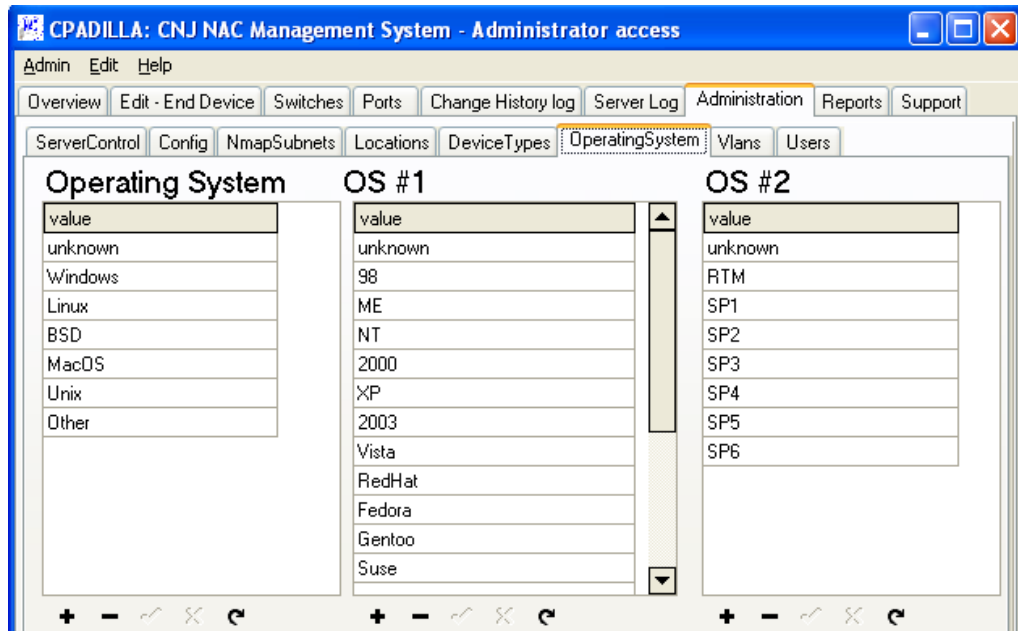


Figura III.18: Configuración de la Herramienta.

Los usuarios son administrados por la herramienta sobre todo para la administración de la misma la cual deben coincidir con los usuarios del dominio.

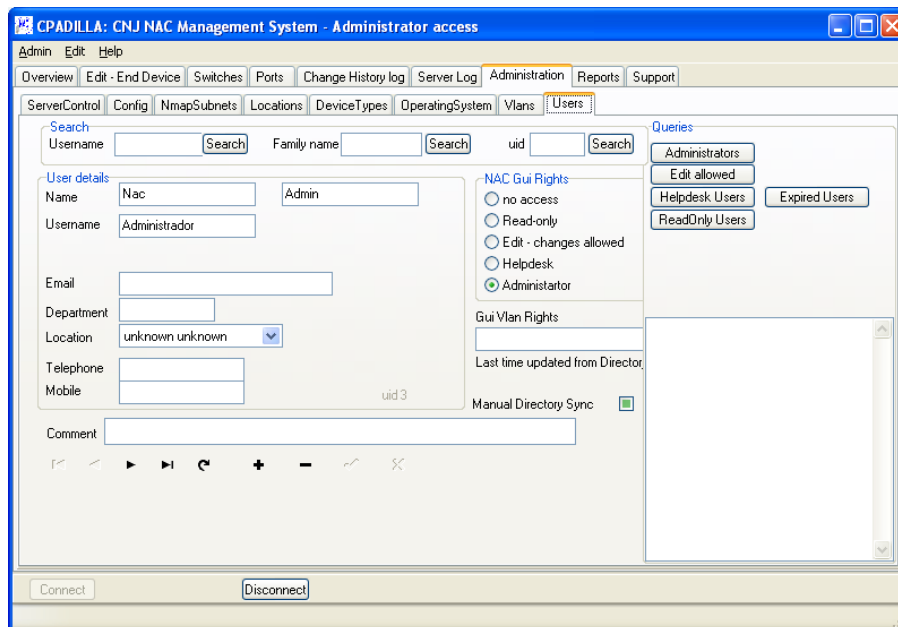


Figura III.19: Configuración de Usuarios

En la administración con una aplicación de escritorio los reportes no se generan con gráficos por lo cual puede parecer algo rudimentario algo que no sucede con la administración web.

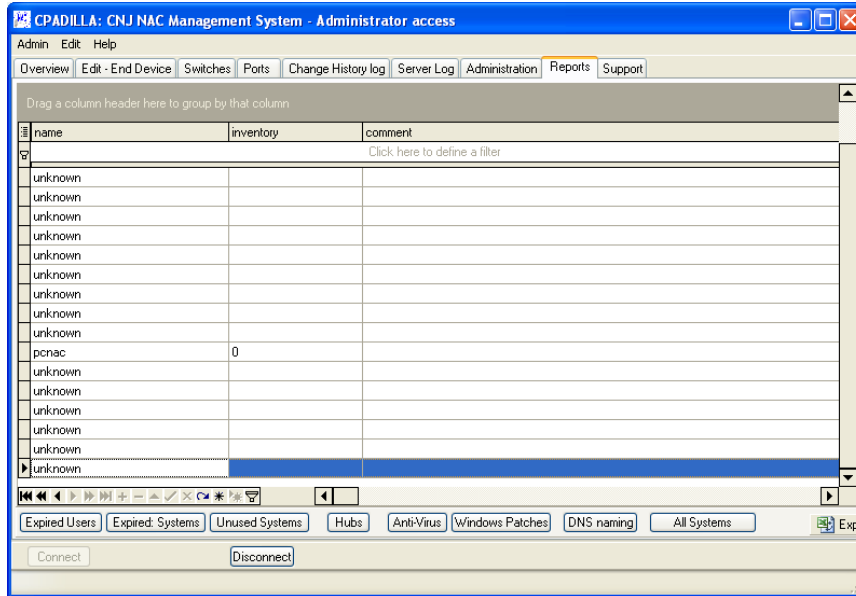


Figura III.20: Reportes de la Herramienta.

En la opción de soporte solo son opciones para dirigir a las páginas web oficiales.

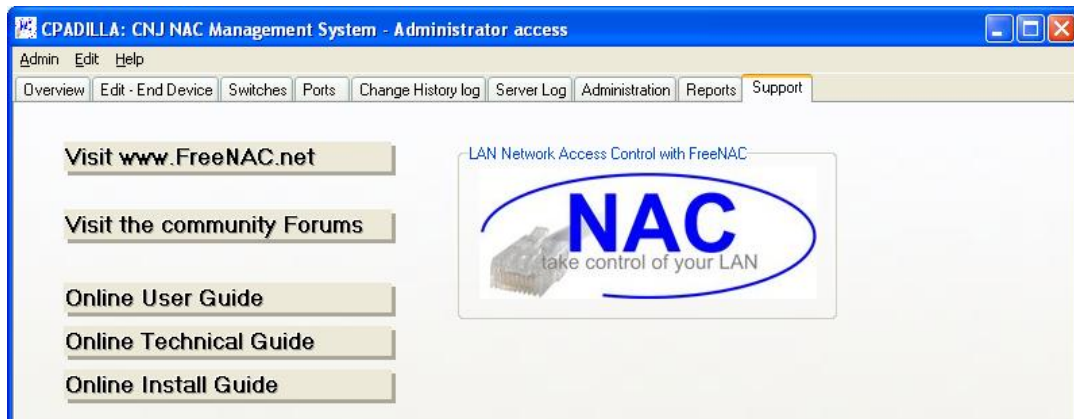


Figura III.21: Enlaces para Soporte Web.

3.2.1.2 Interfaz Web

FreeNAC también se puede administrar por medio de una interfaz web. Para esto solo tenemos que ingresar en la dirección del navegador <http://172.16.148.235/nac>. Por defecto muestra la siguiente página.

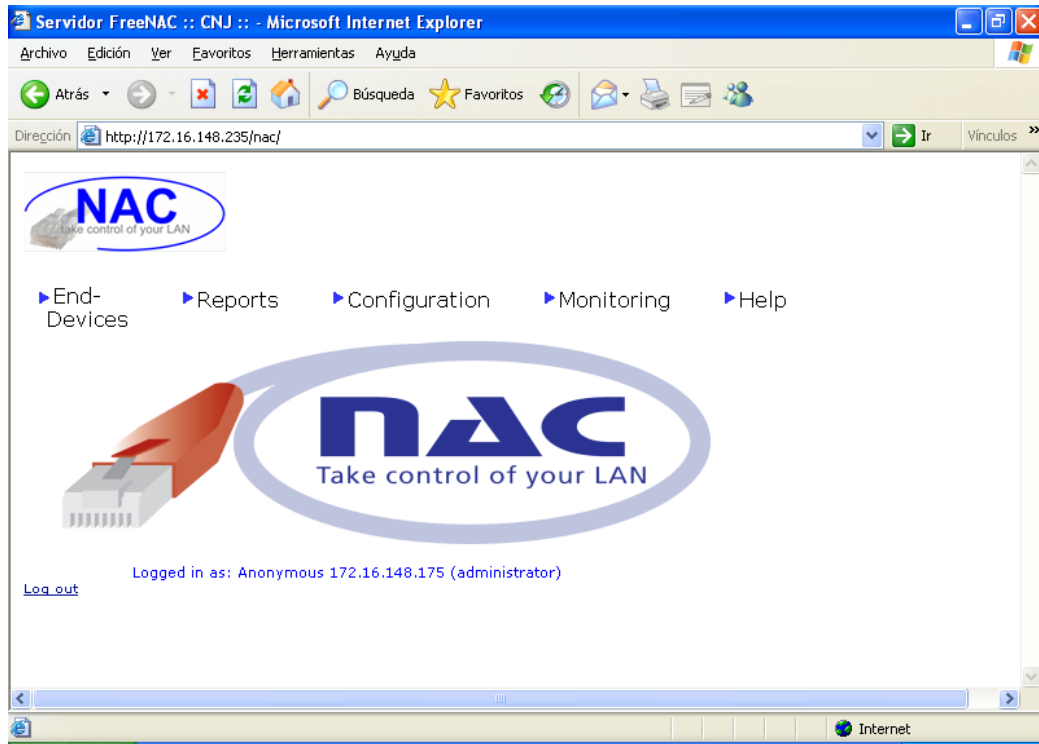


Figura III.22: Página de Inicio de FreeNac.

En la opción End-Devices existen las opciones que nos permite realizar sobre la herramienta referente a los dispositivos finales en esta vista podemos observar todos los dispositivos de red detectados.

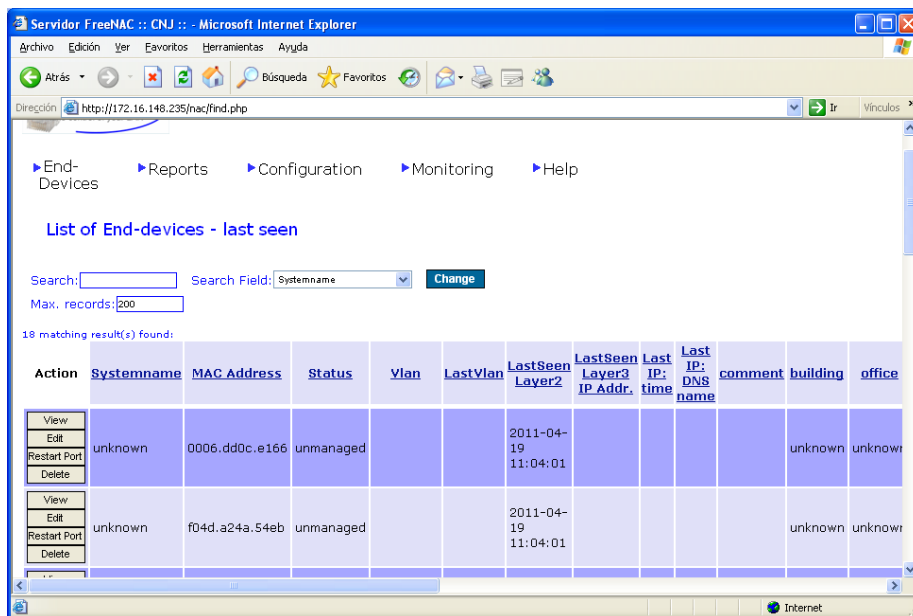


Figura III.23: Reporte Inicial de Dispositivos Detectados.

En esta ventana podemos visualizar la opción de administrar dispositivos.

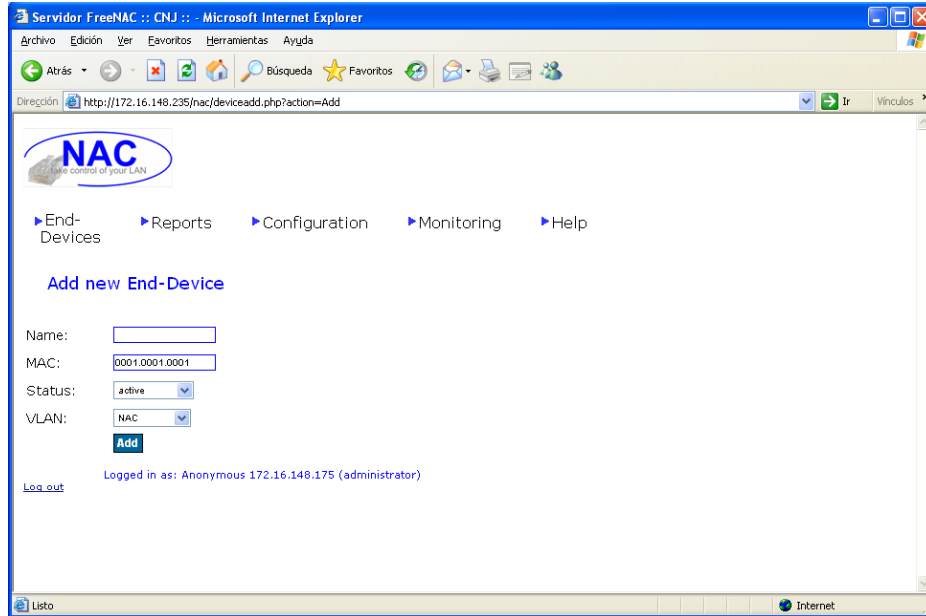


Figura III.24: Agregación de Dispositivos.

Si hay demasiados dispositivos podemos realizar una búsqueda sobre la Base de Datos de la herramienta por medio de la dirección MAC del dispositivo.

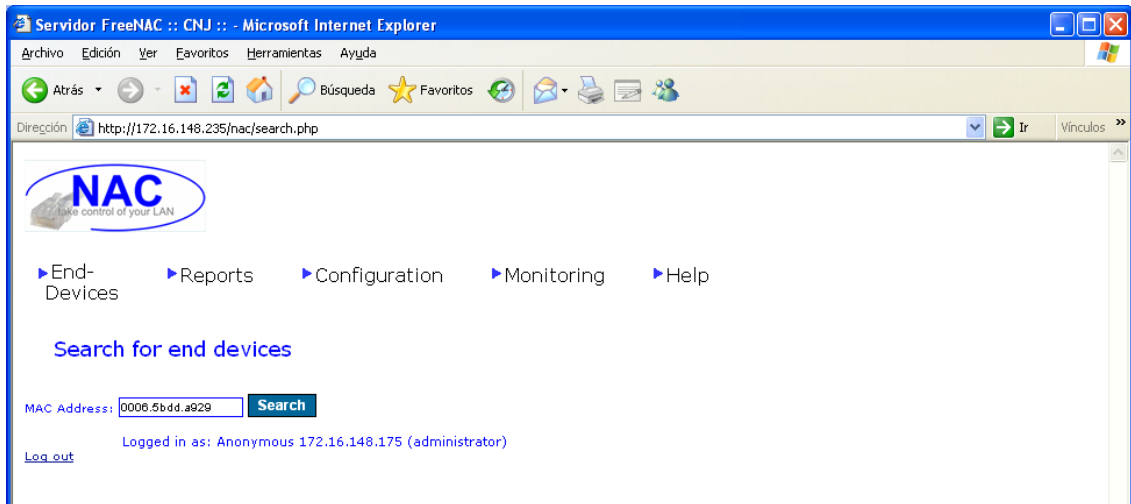


Figura III.25: Búsqueda de Dispositivos Finales.

También permite visualizar gráficos estadísticos para comodidad del usuario. En esta ventana observamos el número de dispositivos filtrado por tipo.

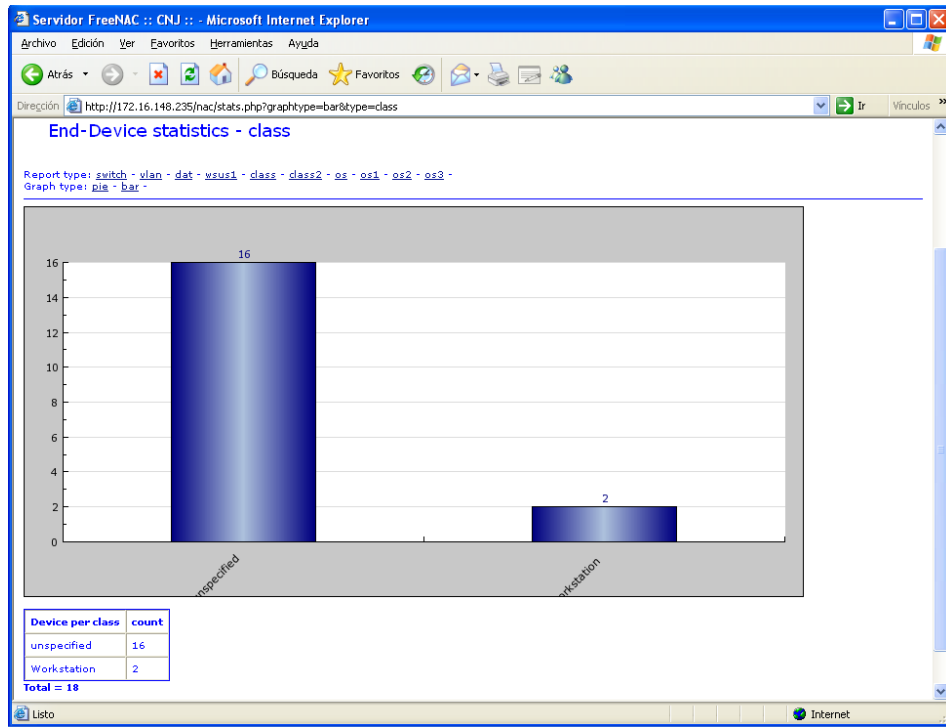


Figura III.26: Grafica de Dispositivos Detectados.

Aquí están filtrados por el tipo de sistema operativo que tienen.

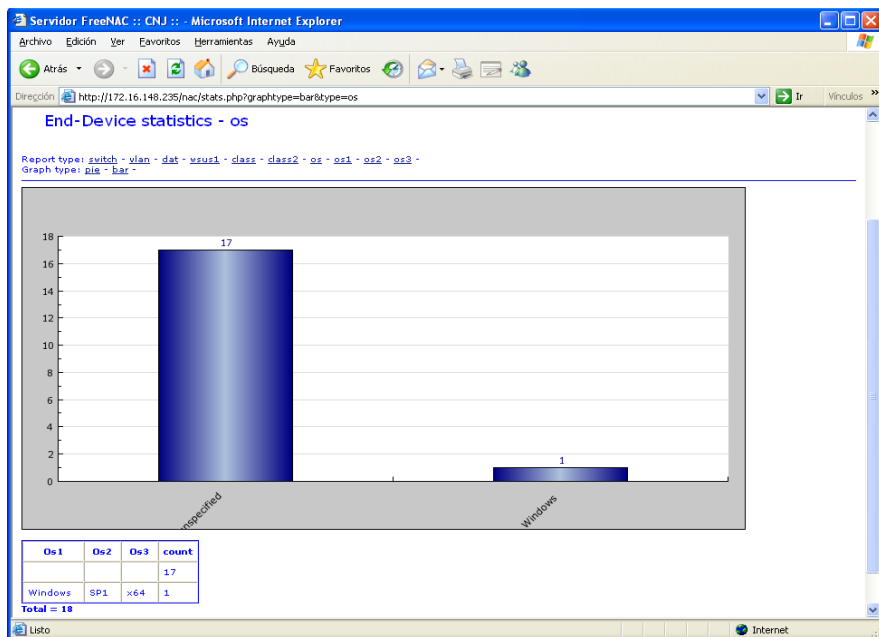


Figura III.27: Grafica de Sistemas Operativos Detectados.

En esta ventana se muestran por el tipo de arquitectura del dispositivo final.

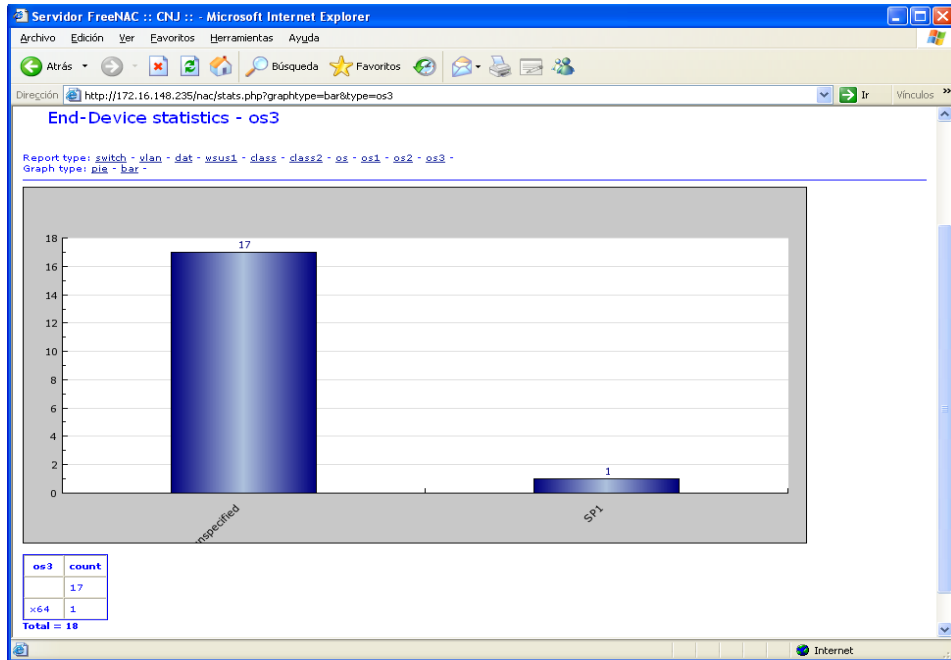


Figura III.28: Grafica de Hardware Detectado.

En la interfaz también contamos con la opción de configurar la herramienta de acuerdo a las necesidades requeridas. En esta ventana podemos ver la configuración de los diferentes puertos del Switch en que se realizó las pruebas.

Switch-Port configuration

Search: Search Field: SwitchName

Max. records: 200

50 matching result(s) found:

Action	SwitchName	Port	LastVlan	Last used	Comment	VlanAuth	Static Vlan	Default Vlan	Last Monitored	Port is up	Switch IP Addr.	switchport
View Restart Delete	P4SWUSR05	Fa0/1	PENALES		V2Min1SalaPe - SALA DE LO PENAL	static			2011-04-19 11:10:03	1	172.16.148.57	P4SWUSR05 Fa0/1
View Restart Delete	P4SWUSR05	Fa0/2	PENALES		V2Min2SalaPe - SALA DE LO PENAL	static			2011-04-19 11:10:03	1	172.16.148.57	P4SWUSR05 Fa0/2
View Restart Delete	P4SWUSR05	Fa0/3	PENALES		V2Min3SalaPe - SALA DE LO PENAL	static			2011-04-19 11:10:03	1	172.16.148.57	P4SWUSR05 Fa0/3

Figura III.29: Configuración de los Puertos del Switch.

En esta ventana observamos la configuración que se puede realizar sobre el Switch que se desea administrar.

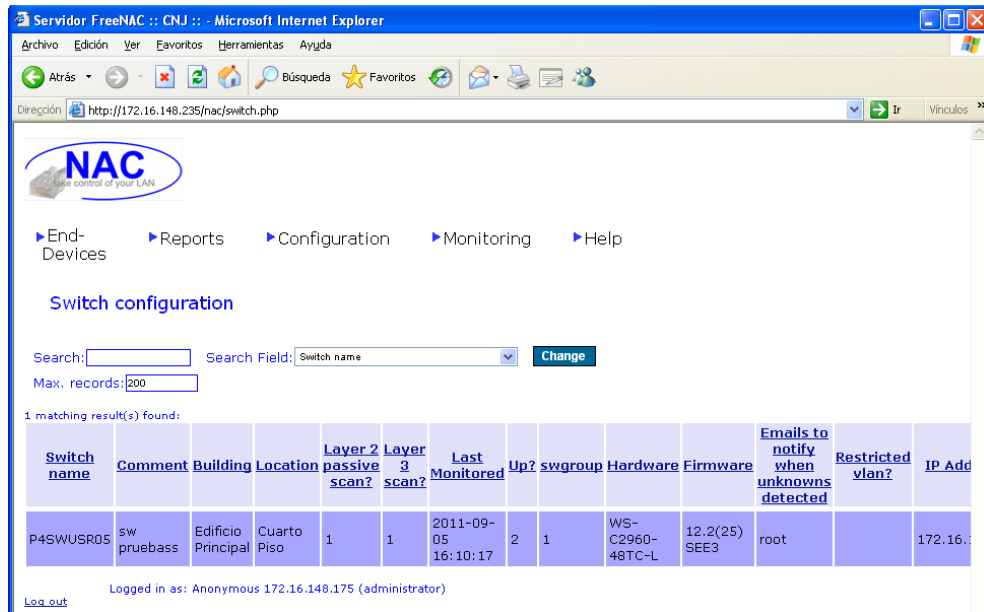


Figura III.30: Configuración del Switch.

Aquí podemos configurar las diferentes Vlans para la administración dinámica.

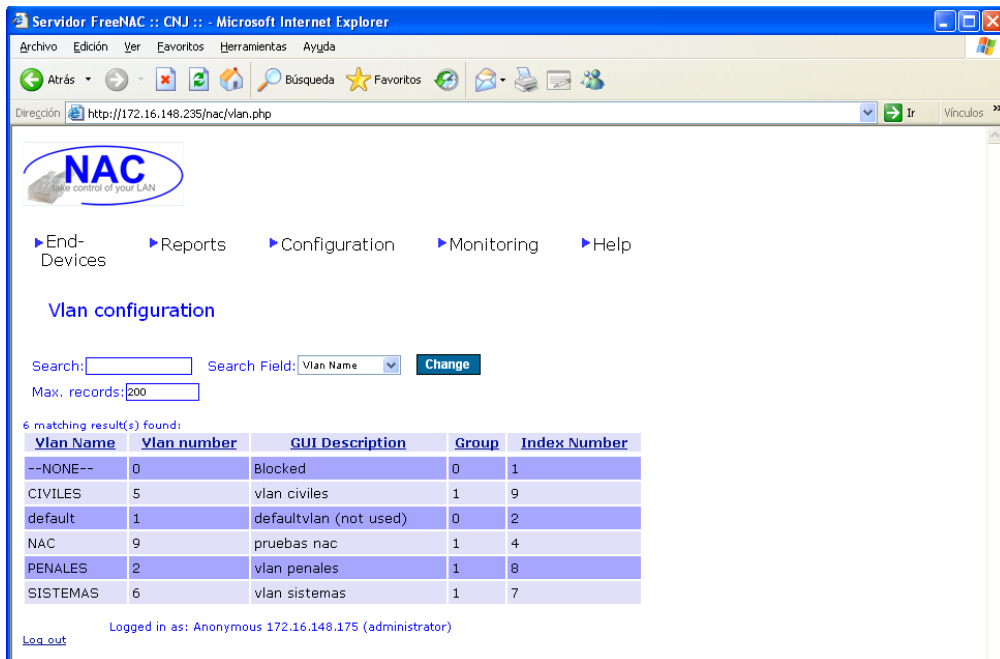


Figura III.31: Configuración de Vlans para Administración Dinámica.

En esta ventana configuramos la lista de usuarios de la herramienta.

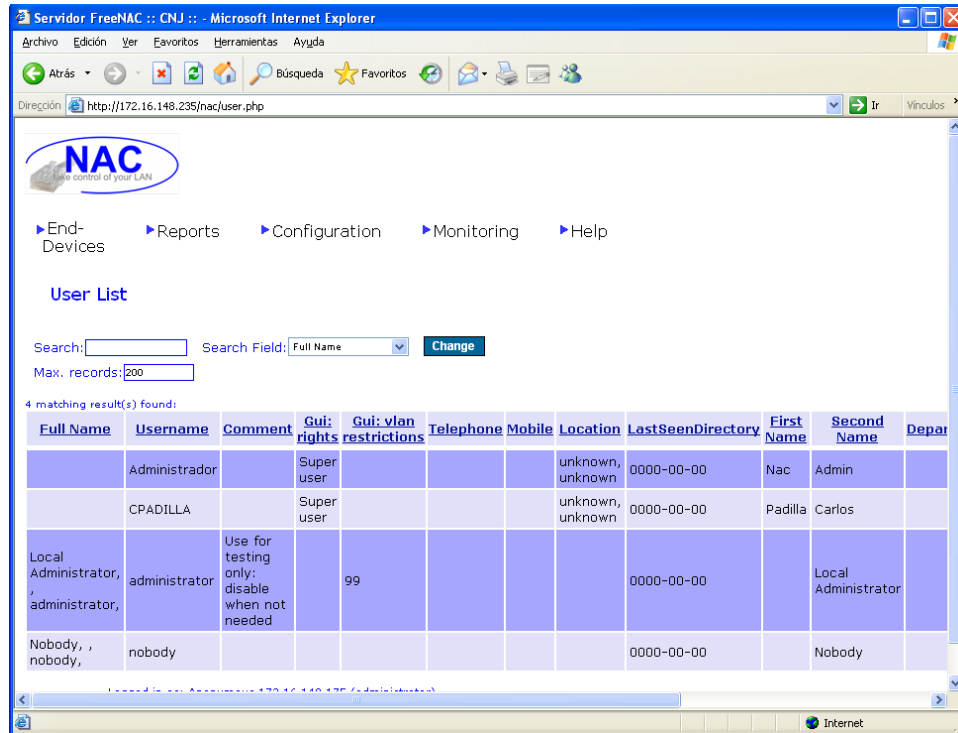


Figura III.32: Listado de Usuarios.

En esta ventana ingresamos las ubicaciones de los dispositivos finales.

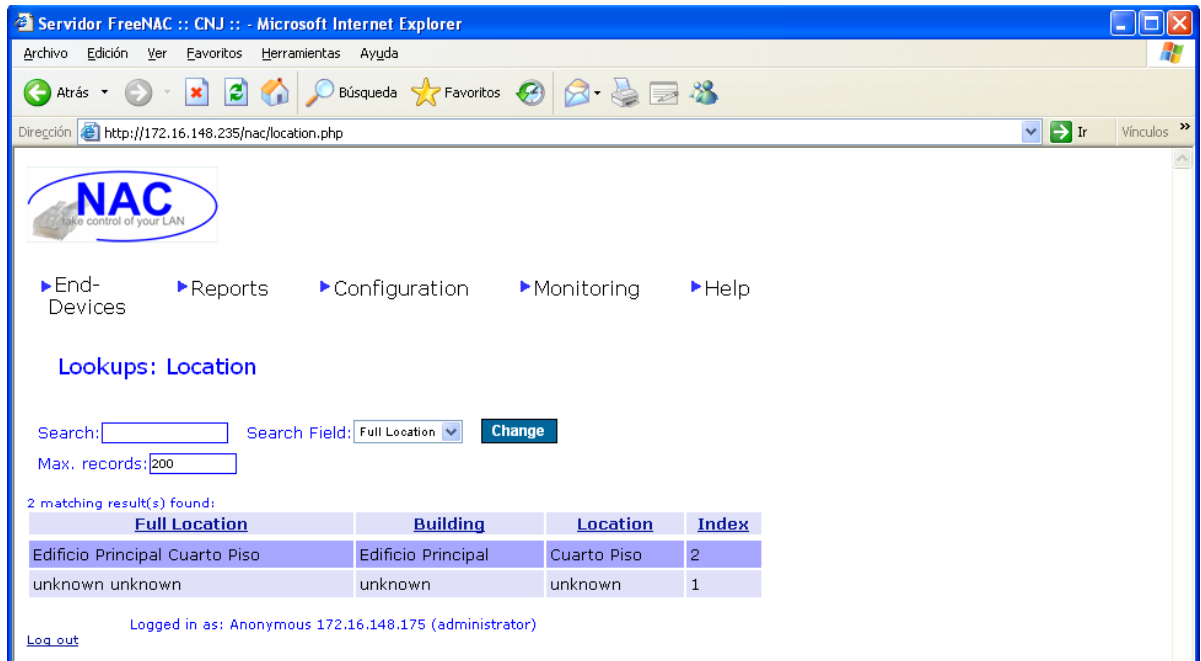


Figura III.33: Búsqueda de Ubicaciones.

Aquí podemos configurar las opciones de supervisión de Vlans con Nmap.

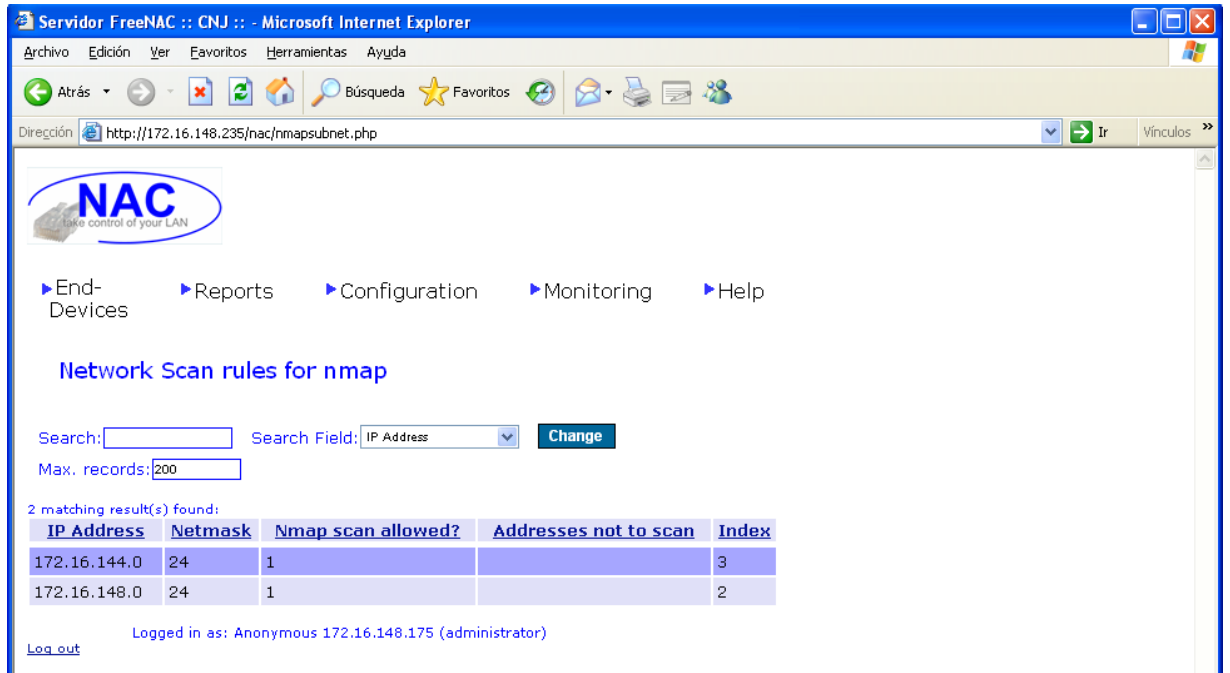


Figura III.34: Configuración de Nmap.

Las configuraciones de tipos de dispositivos.

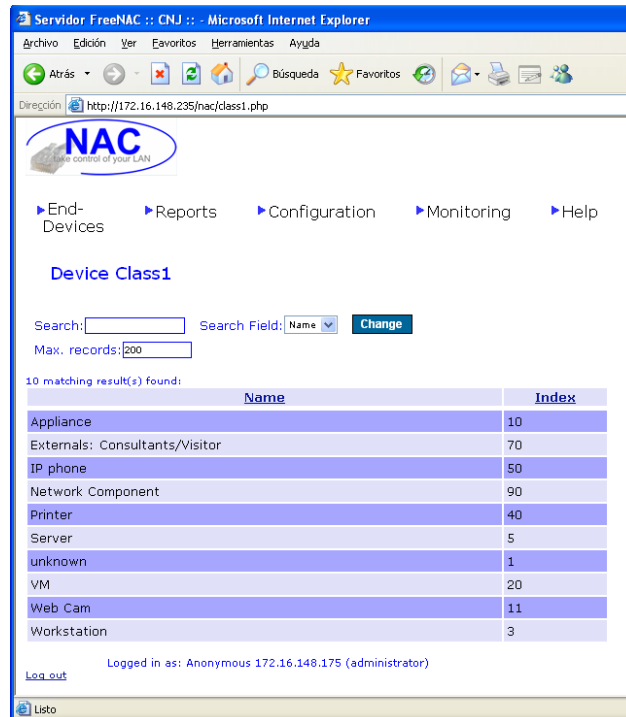


Figura III.35: Configuración de los Tipos de Dispositivos.

En esta captura observamos los registros de sucesos de la herramienta.

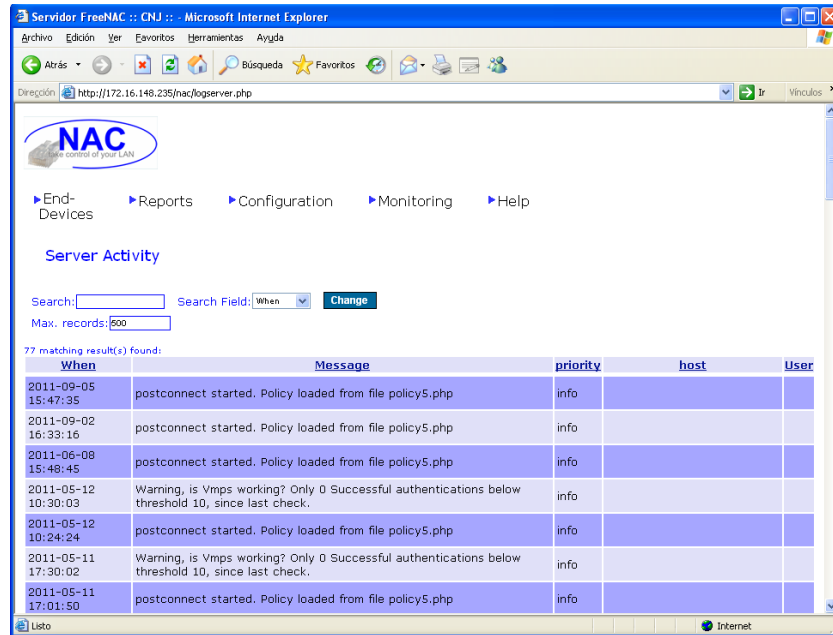


Figura III.36: Reporte de Sucesos de la herramienta.

En esta pantalla en cambio visualizamos los sucesos de ingreso a la administración de la herramienta.

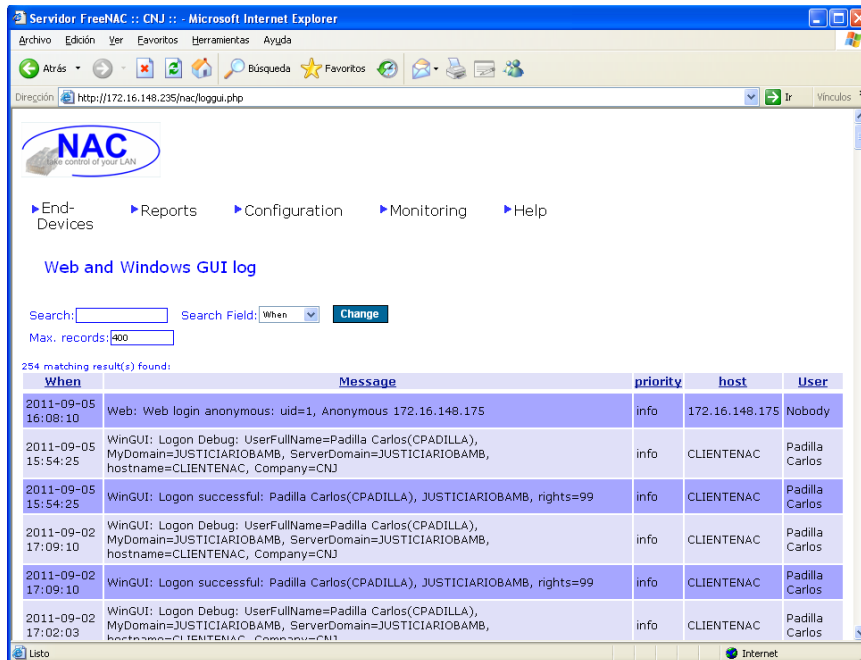


Figura III.37: Reporte de Sucesos de Ingreso al Sistema.

En esta ventana en cambio visualizamos los sucesos del sistema.

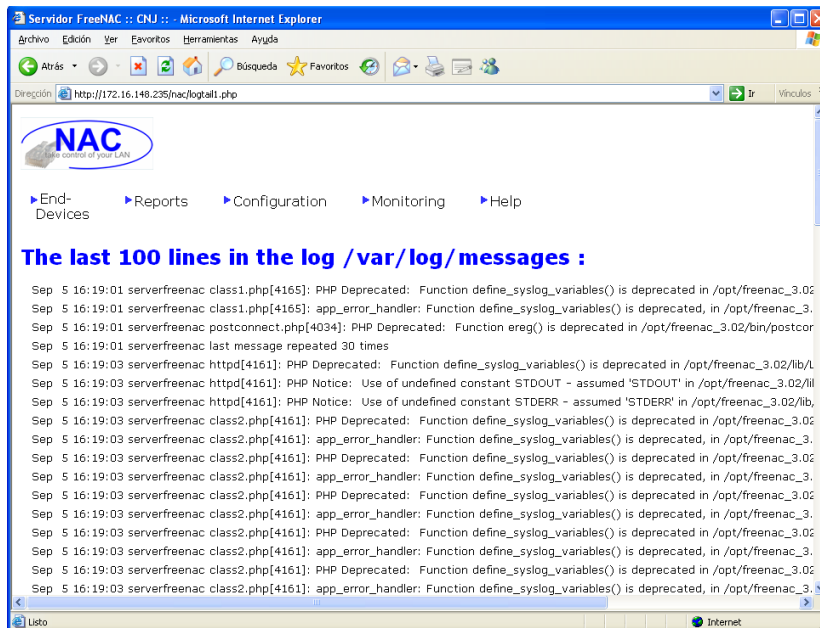


Figura III.38: Reporte de Sucesos Generales.

Y la última opción de la administración web es la de la información del sistema operativo.

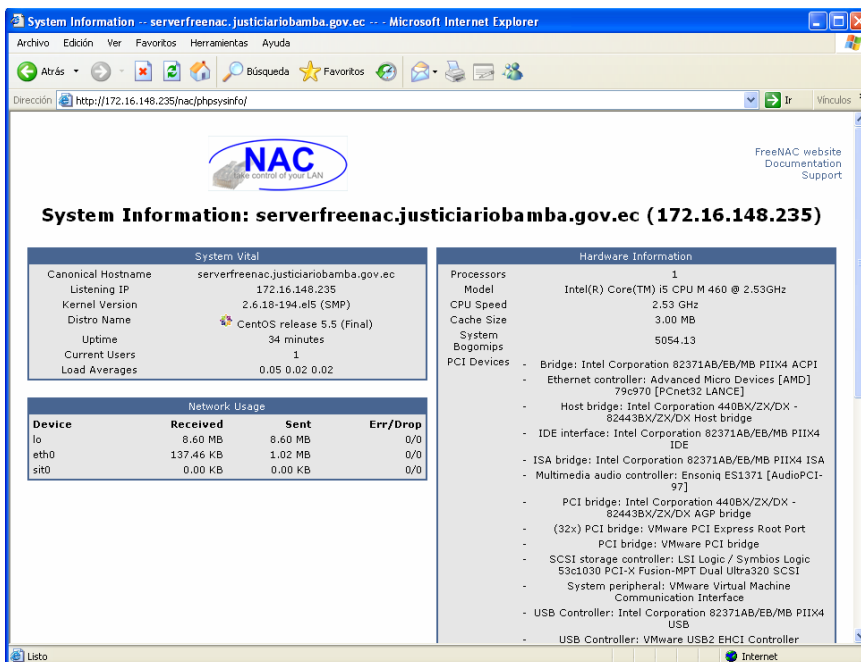


Figura III.39: Reporte de Información del Sistema.

3.2.2 Pruebas Con La Herramienta Packetfence

La herramienta Packetfence se puede administrar mediante una interfaz web. En nuestro ambiente de pruebas la dirección web del servidor es la siguiente <http://172.16.148.30:1443>. Para ingresar al sitio de administración de la herramienta lo hacemos con el usuario admin y contraseña 123456.

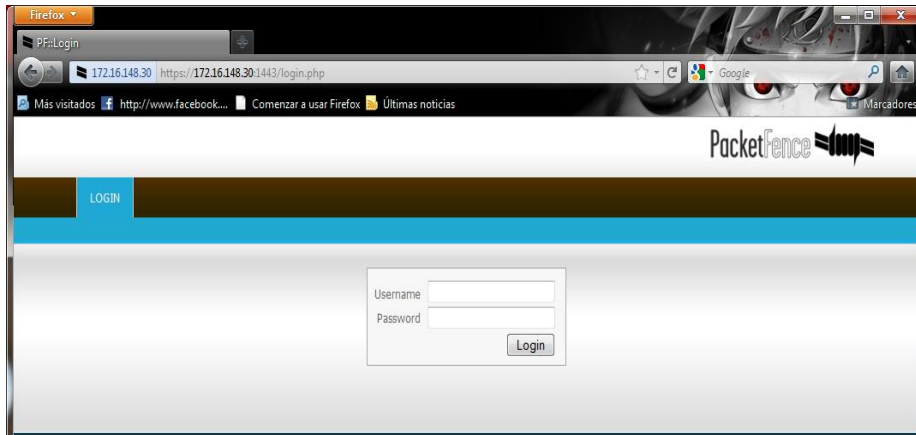


Figura III.40: Página de Ingreso a PacketFence.

Una vez ingresado al sitio de administración se presenta la pantalla inicial que trata sobre el estado actual del servidor.

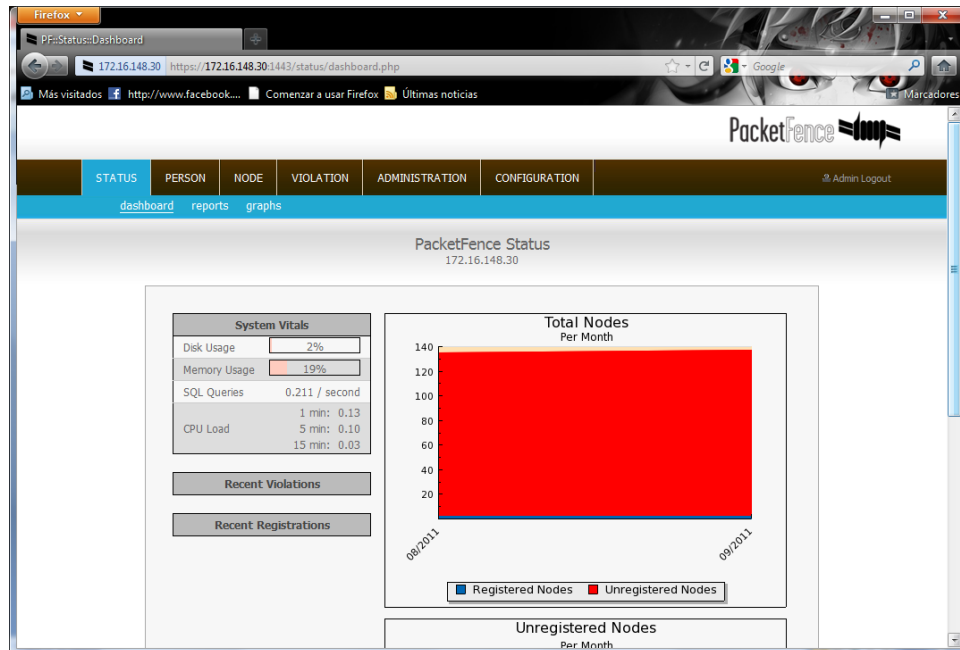
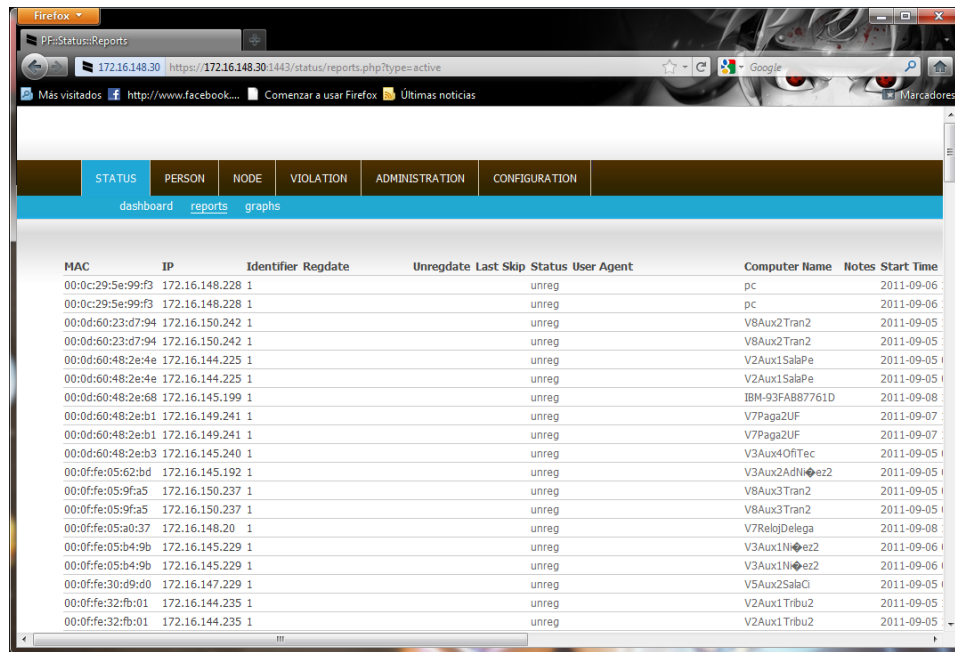


Figura III.41: Página de Inicio de PacketFence.

En la opción de status o estado podemos ver también los reportes de nodos que encontramos dentro de la red LAN (registrados y no registrados).



The screenshot shows the 'Status: Reports' page in a Firefox browser. The page has a navigation menu with 'STATUS', 'PERSON', 'NODE', 'VIOLATION', 'ADMINISTRATION', and 'CONFIGURATION'. Below the menu, there are tabs for 'dashboard', 'reports', and 'graphs'. The main content is a table with the following columns: MAC, IP, Identifier, Regdate, Unregdate, Last Skip, Status, User Agent, Computer Name, Notes, and Start Time. The table contains 20 rows of data, all with a status of 'unreg'.

MAC	IP	Identifier	Regdate	Unregdate	Last Skip	Status	User Agent	Computer Name	Notes	Start Time
00:0c:29:5e:99:f3	172.16.148.228	1				unreg		pc		2011-09-06
00:0c:29:5e:99:f3	172.16.148.228	1				unreg		pc		2011-09-06
00:0d:60:23:d7:94	172.16.150.242	1				unreg		V8Aux2Tran2		2011-09-05
00:0d:60:23:d7:94	172.16.150.242	1				unreg		V8Aux2Tran2		2011-09-05
00:0d:60:48:2e:4e	172.16.144.225	1				unreg		V2Aux1SalaPe		2011-09-05
00:0d:60:48:2e:4e	172.16.144.225	1				unreg		V2Aux1SalaPe		2011-09-05
00:0d:60:48:2e:68	172.16.145.199	1				unreg		IBM-93FAB87761D		2011-09-08
00:0d:60:48:2e:b1	172.16.149.241	1				unreg		V7Paga2UF		2011-09-07
00:0d:60:48:2e:b1	172.16.149.241	1				unreg		V7Paga2UF		2011-09-07
00:0d:60:48:2e:b3	172.16.145.240	1				unreg		V3Aux4OfTec		2011-09-05
00:0ffe:05:62:bd	172.16.145.192	1				unreg		V3Aux2Adm		2011-09-05
00:0ffe:05:9fa5	172.16.150.237	1				unreg		V8Aux3Tran2		2011-09-05
00:0ffe:05:9fa5	172.16.150.237	1				unreg		V8Aux3Tran2		2011-09-05
00:0ffe:05:a0:37	172.16.148.20	1				unreg		V7RelojDelega		2011-09-08
00:0ffe:05:b4:9b	172.16.145.229	1				unreg		V3Aux1N		2011-09-06
00:0ffe:05:b4:9b	172.16.145.229	1				unreg		V3Aux1N		2011-09-06
00:0ffe:30:d9:d0	172.16.147.229	1				unreg		V5Aux2SalaC		2011-09-05
00:0ffe:32:fb:01	172.16.144.235	1				unreg		V2Aux1Trbu2		2011-09-05
00:0ffe:32:fb:01	172.16.144.235	1				unreg		V2Aux1Trbu2		2011-09-05

Figura III.42: Estado de Nodos de la Red LAN.

Los reportes dependiendo de las opciones pueden ser texto o gráficos.

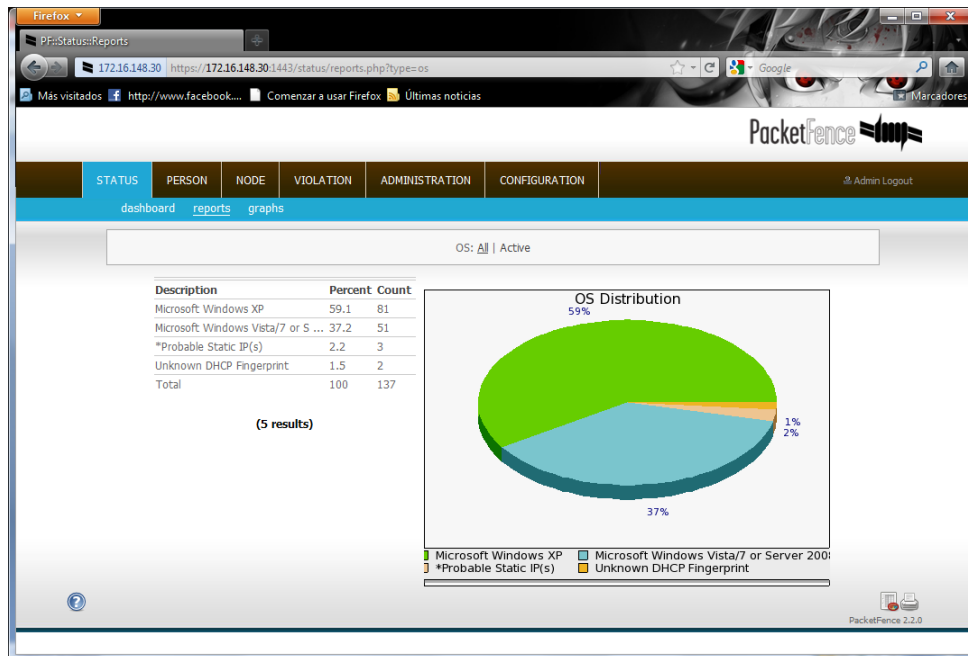


Figura III.43: Grafico del Estado de los Nodos en la Red LAN.

Los reportes también se pueden generar solo gráficamente; por defecto se muestra el grafico del número de nodos conocidos o desconocidos.

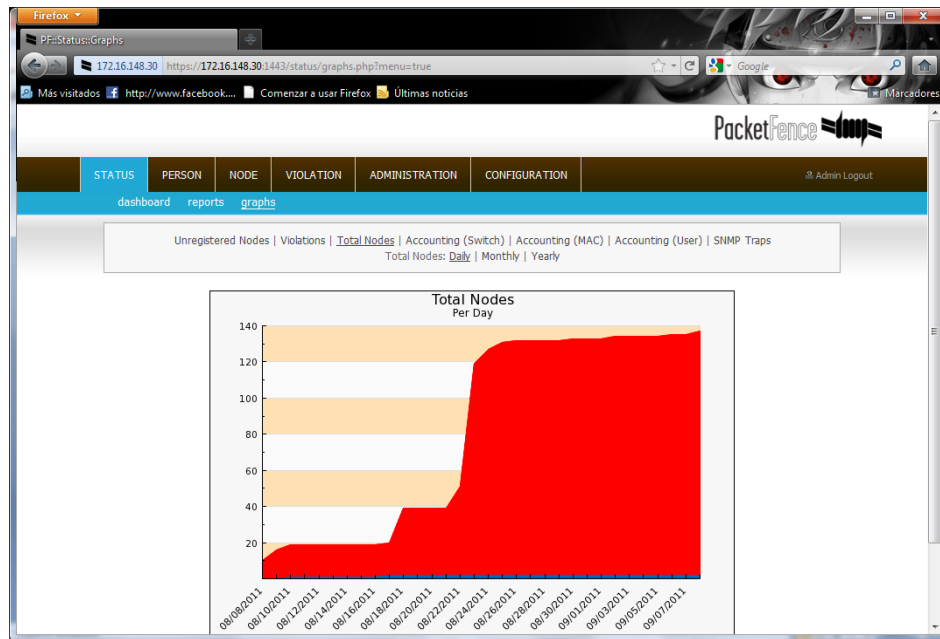


Figura III.44: Grafica del Total de Nodos.

Se puede clasificar el número de nodos por desconocidos como se muestra en esta imagen.

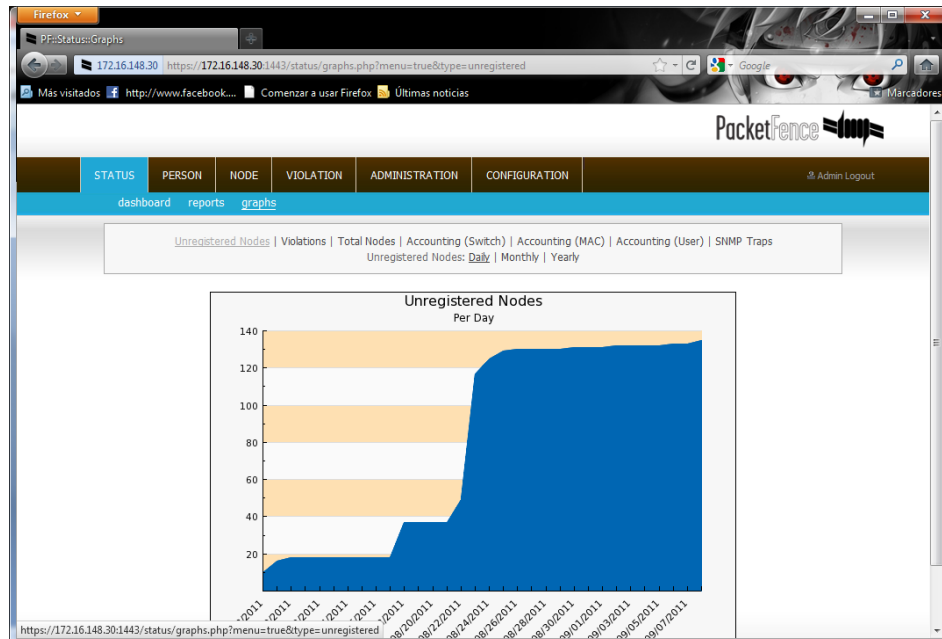


Figura III.45: Grafica del Total de Nodos No Registrados.

El número de violaciones dentro de la red entre otros.

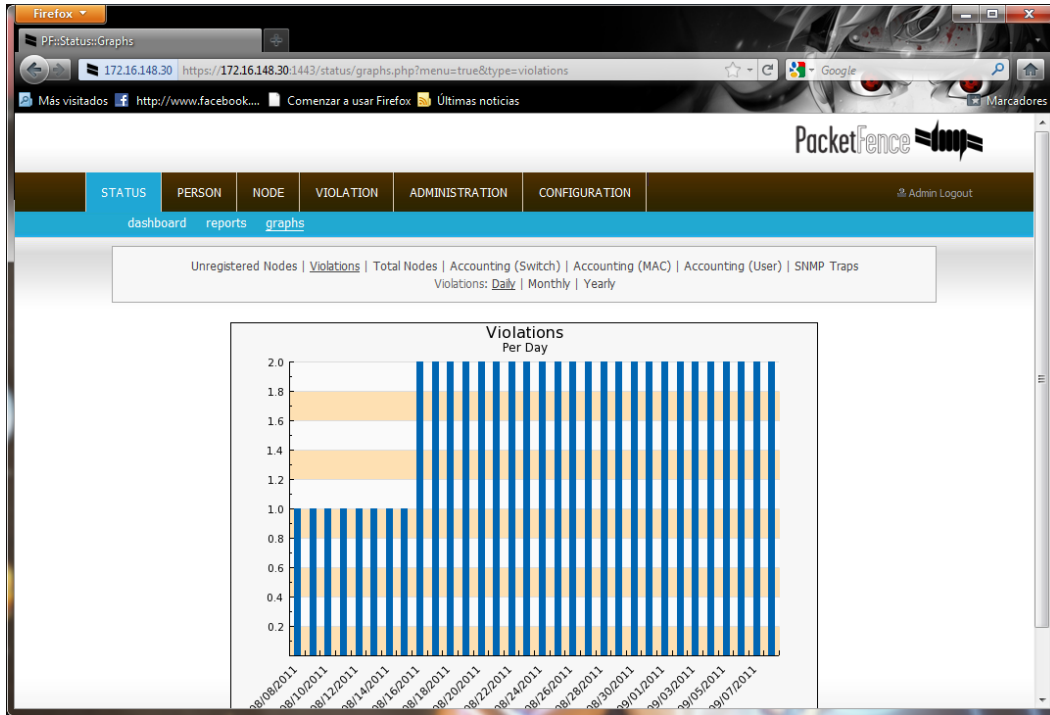


Figura III.46: Grafica de Violaciones Detectadas por Día.

En la opción de PERSON se administra los usuarios finales de los nodos que tienen acceso a la LAN. Se pueden Agregar u observar la historia del usuario y los nodos registrados a través del sistema.

The screenshot shows the PacketFence web interface for the PERSON section. The browser address bar indicates the URL: https://172.16.148.30/person/view.php. The page has a navigation menu with tabs for STATUS, PERSON, NODE, VIOLATION, ADMINISTRATION, and CONFIGURATION. Below the menu, there are sub-tabs for view, add, and lookup. The main content area displays a table of registered users. The table has columns for Identifier, Firstname, Lastname, Email, Phone, Company, Address, and Notes. There are three rows of data: 1, carlos, and user1. The Notes column for the first row contains "Default User - do not delete". Below the table, it says "(3 results)".

Identifier	Firstname	Lastname	Email	Phone	Company	Address	Notes
1							Default User - do not delete
carlos							
user1							

Figura III.47: Página de Usuarios Registrados.

Agregación de Usuarios que usaran los dispositivos finales.

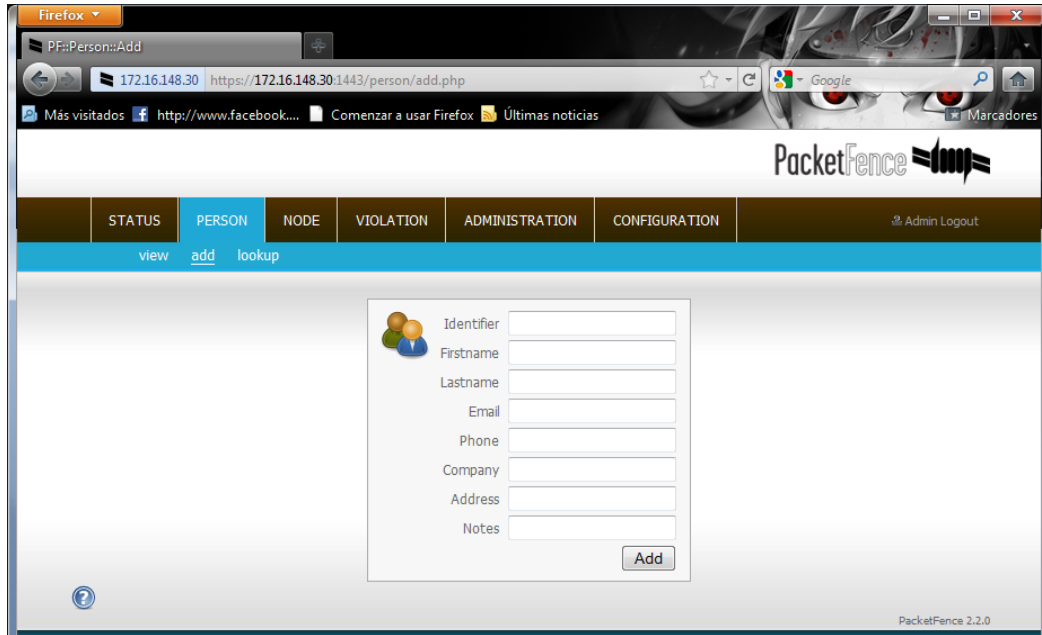


Figura III.48: Agregar Usuarios.

La opción de NODE presenta varias opciones para administrar los dispositivos finales en esta pantalla se muestra los nodos detectados en la red.

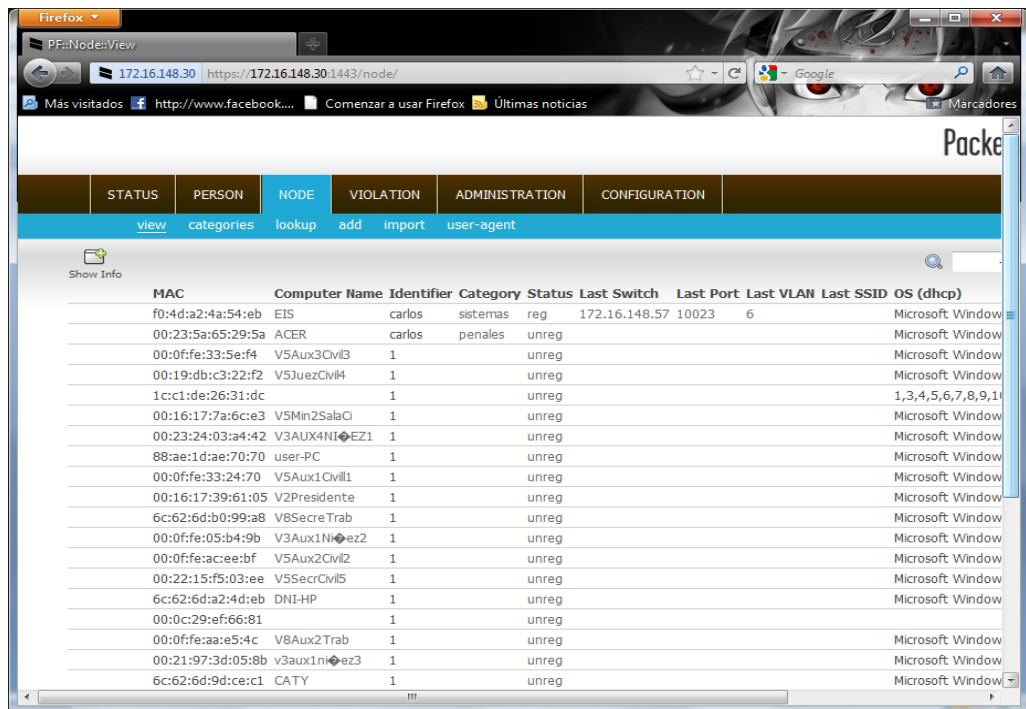


Figura III.49: Información de los Equipo Finales.

Importación de nodos de un archivo.

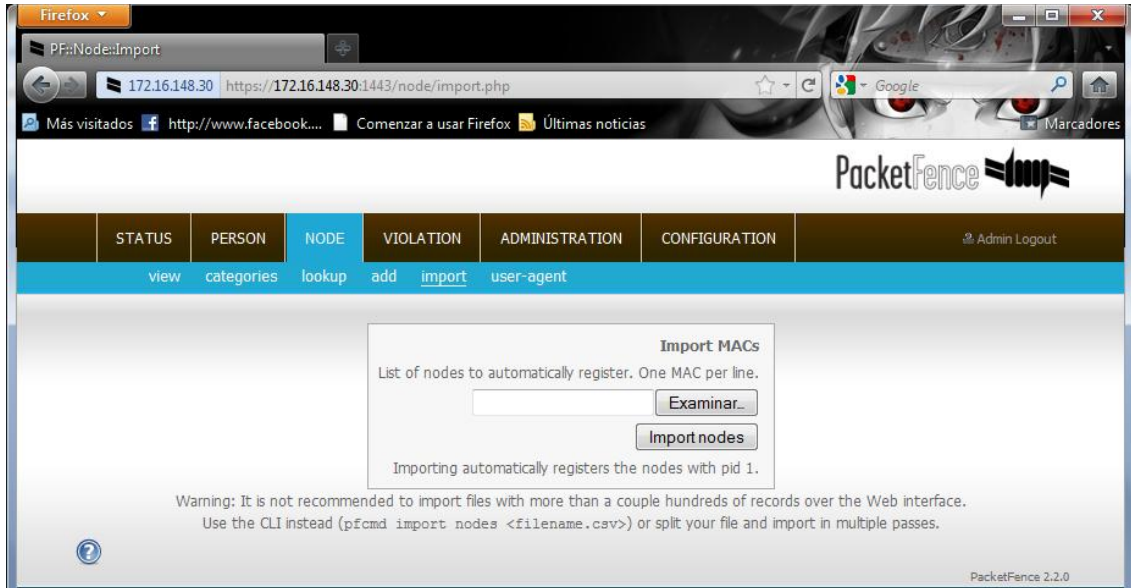


Figura III.50: Importación de Nodos.

En esta pantalla se muestra las violaciones que han tenido los equipos y si siguen abiertos o cerrados.

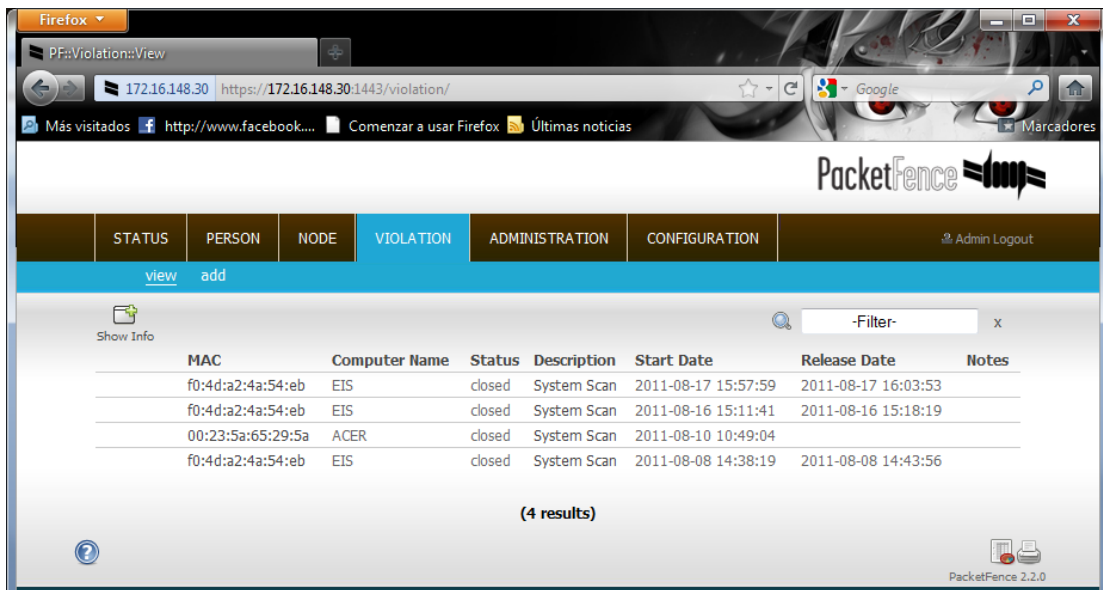
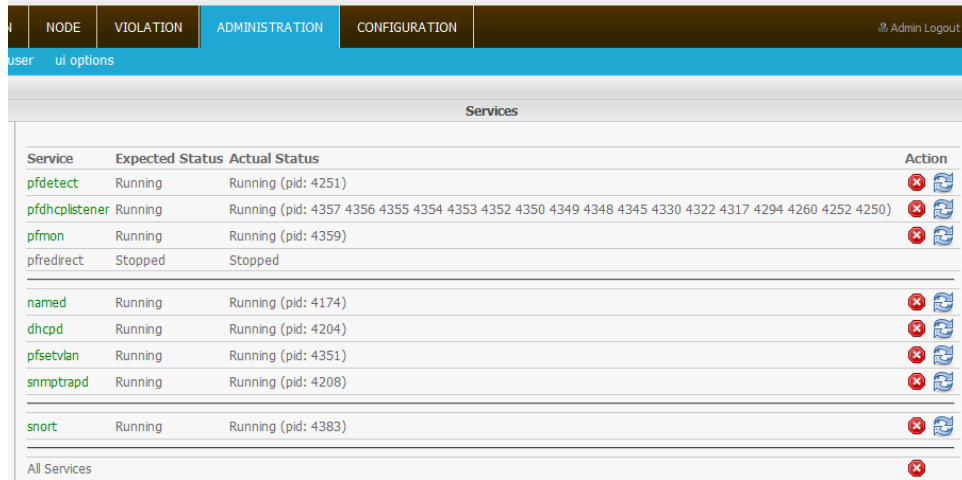


Figura III.51: Reporte de Violaciones (abiertas o cerradas).

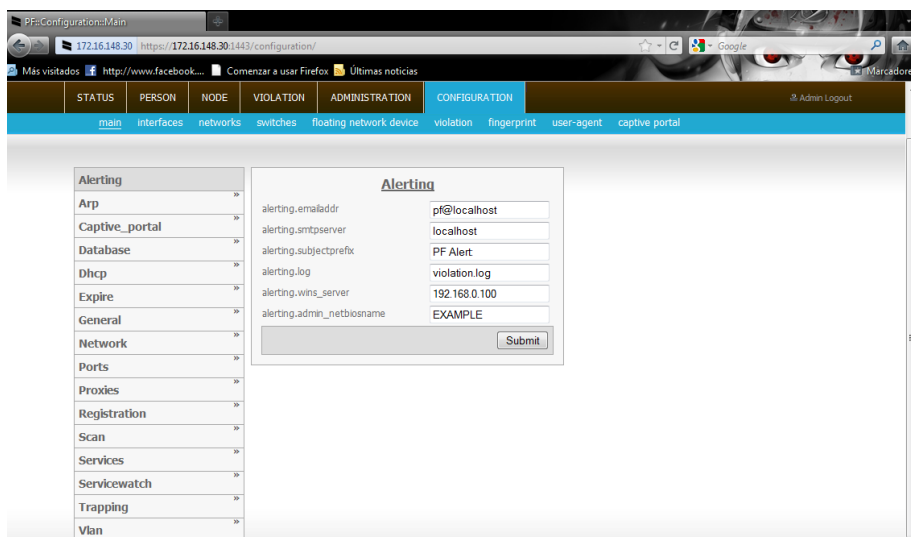
En la opción de ADMINISTRATION podemos observar que existen varios servicios que se necesitan para que la herramienta funcione correctamente.



Service	Expected Status	Actual Status	Action
pfdetect	Running	Running (pid: 4251)	
pfdhcpd	Running	Running (pid: 4357 4356 4355 4354 4353 4352 4350 4349 4348 4345 4330 4322 4317 4294 4260 4252 4250)	
pfmon	Running	Running (pid: 4359)	
pfredirect	Stopped	Stopped	
named	Running	Running (pid: 4174)	
dhcpd	Running	Running (pid: 4204)	
pfsetvlan	Running	Running (pid: 4351)	
snmptrapd	Running	Running (pid: 4208)	
snort	Running	Running (pid: 4383)	
All Services			

Figura III.52: Administración de Servicios que utiliza PacketFence.

En la opción de CONFIGURATION podemos configurar las diferentes características de la herramienta. Por defecto se muestra en la opción de configuración main; Como su nombre lo indica son las características principales. En esta pantalla muestra la configuración de alerta al usuario que administra la red. La herramienta tiene muchas opciones de configuración y tienen muchas opciones de configuración.



Alerting

Arp	
Captive_portal	
Database	
Dhcp	
Expire	
General	
Network	
Ports	
Proxies	
Registration	
Scan	
Services	
Servicewatch	
Trapping	
Vlan	

Alerting

alerting_emailaddr	pf@localhost
alerting_smtpserver	localhost
alerting_subjectprefix	PF Alert
alerting_log	violation.log
alerting_wins_server	192.168.0.100
alerting_admin_netbiosname	EXAMPLE

Submit

Figura III.53: Configuración de Todas las Opciones PacketFence.

3.3 DEFINICIÓN DE LOS PARÁMETROS DE COMPARACIÓN

Los parámetros que a continuación se definirán para la realización del estudio comparativo entre las herramientas de FreeNac y Packetfence, están basados en los requerimientos planteados para la Dirección Provincial del Consejo de la Judicatura de Chimborazo, y según los criterios del autor de la tesis. Los criterios de comparación que se tomaron en cuenta son los siguientes:

Tabla III.VI: Parámetros de Comparación.

PARÁMETRO	DEFINICIÓN
Usabilidad	Facilidad de instalación, configuración, implementación y uso.
Gestión y Administración de Usuarios	Se refiere al tipo de seguridad ofrecida por la herramienta para gestionar y administrar usuarios que administran las herramientas.
Administración de Switchs	Habilidad para administrar y manipular los Switchs de la red LAN.
Autodescubrimiento de Dispositivos y Recolección de Información en Tiempo Real	Habilidad descubrir y recolectar continuamente información acerca de los dispositivos finales y reportarla en tiempo real.
Políticas de Red	Facilidad de aplicación selección y refuerzo de las políticas de red de la institución.
Análisis y Detección de Vulnerabilidades	Facilidad de analizar la red y detectar vulnerabilidades y tomar las decisiones respectivas.
Soporte	Soporte en línea a través de wikis, foros, comunidades.
Reportes	Facilidad de generar reportes e inventarios de los equipos pertenecientes a la Red LAN.

3.4 DEFINICIÓN DE ESCALAS

La forma para evaluar las herramientas de Administración y Monitoreo de Redes en base a los parámetros mencionados anteriormente, se calificarán utilizando una escala que va desde 1 hasta 5, a continuación su descripción.

Tabla III.VII: Definición de Escalas.

Cualitativa	Bajo	Medio Bajo	Medio	Medio Alto	Alto
Cuantitativa	1	2	3	4	5

3.5 Análisis Comparativo de Herramientas NAC

▪ Usabilidad

Tabla III.VIII: Valoración del Parámetro Usabilidad.

	FreeNac	PacketFence
Administración de Servicios	Medio Alto	Alto
Interfaz Web	Medio	Alto
Opciones de Personalización	Alto	Alto
Total	12	15

Observando los parámetros de Usabilidad en cada una de las herramientas NAC OpenSource se pudo observar y comprobar lo siguiente:

En la administración de Servicios se pudo observar que FreeNac permitía una administración de Servicios aceptable ya que permitía configurar sus propios servicios de una manera óptima. En la herramienta Packetfence se puede administrar sus propios servicios pero también se puede configurar los servicios de los dispositivos de red (Switch) por esta razón tiene una puntuación alta en ese parámetro y FreeNac una puntuación media alta.

En el parámetro de Interfaz Web se observó que la herramienta FreeNac tiene una interfaz sencilla y poco amigable al usuario, al contrario de la herramienta Packetfence que posee una interfaz elaborada, útil e intuitiva para la administración de esta; por estos motivos FreeNac obtiene una calificación media y PacketFence obtiene una calificación Alta.

En Opciones de Personalización FreeNac puede ser configurado tanto mediante interfaz web como de escritorio. La herramienta Packetfence permite una configuración dinámica de su página de inicio en la cual se puede modificar las graficas e información que se desea observar para un adecuado uso y administración de la herramienta. Por estas razones FreeNac y PacketFence obtiene una puntuación alta en este parámetro.

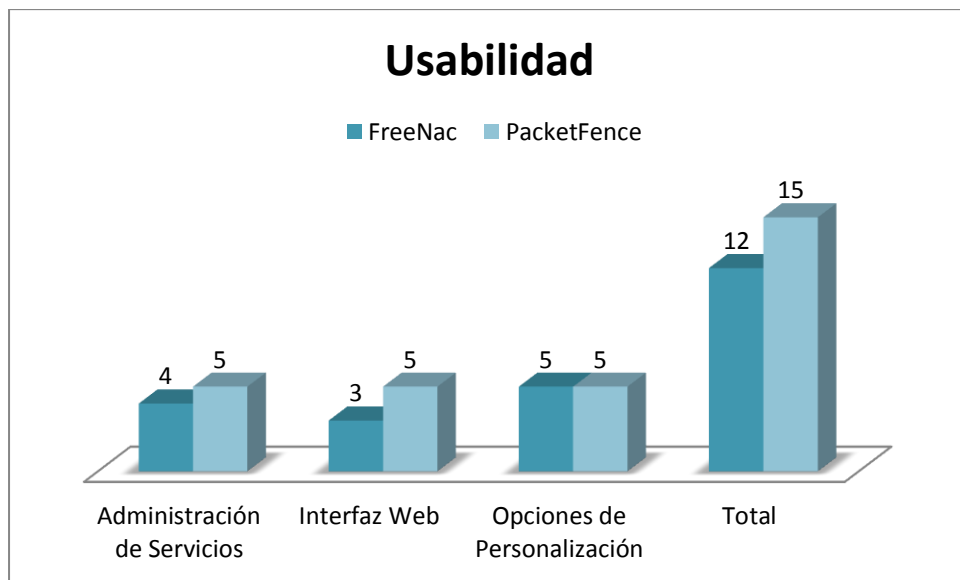


Fig.III.54 Grafica de Resultados de Usabilidad

▪ **Gestión y Administración de Usuarios**

Tabla III.IX: Valoración del Parámetro Gestión y Administración de Usuarios.

	FreeNac	PacketFence
Diferentes Metodos de Autenticación	Medio	Alto
Tipos de Usuarios	Medio	Medio
Auditoria de Acceso al Sistema	Alto	Medio Alto
Total	11	12

En el parámetro de Gestión y Administración de Usuarios se verifico en base a lo siguiente:

En el sub parámetro de Diferentes Metodos de Autenticación se pudo determinar que FreeNac posee dos métodos de autenticación Local y Active Directory; En cambio la Herramienta PacketFence posee varios métodos de autenticación como son Local, LDAP, Kerberos, Active Directory. Por este motivo la herramienta que tiene mejor calificación es Packetefence.

En tipos de usuarios tanto FreeNac como PacketFence tienen la misma calificación ya que los dos permiten varios tipos de usuarios como son: Administradores, Usuarios y Clientes.

En auditoria de acceso al sistema la herramienta FreeNac posee un mejor control del acceso a la administración de la herramienta ya que permite analizar desde la herramienta los accesos a esta. Mientras que Packetfence posee solo se puede revisar los accesos solo desde los archivos logs.

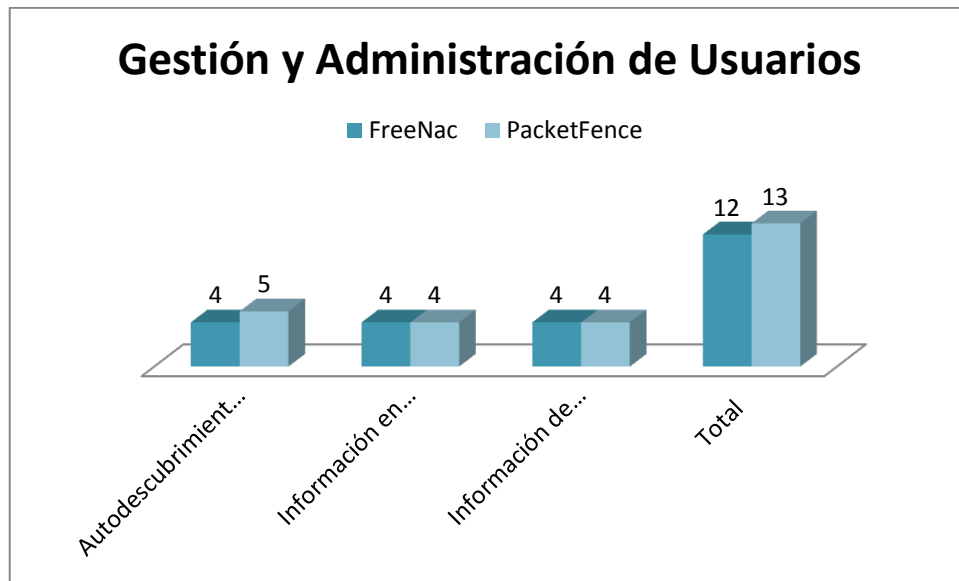


Fig.III.55 Grafica de Resultados de Gestión y Administración de Usuarios

▪ **Administración de Switchs**

Tabla III.X: Valoración del Parámetro Administración de Switchs.

	FreeNac	PacketFence
Compatibilidad con varias marcas	Nulo	Alto
Registro de Eventos	Medio	Medio
Asignamiento dinámico de Vlans	Alto	Alto
Total	8	13

Para el parámetro de Administración de Switchs se analizo de la siguiente forma:

En Compatibilidad con varias marcas FreeNac solo soporta dispositivos de red Cisco; PacketFence soporta varios dispositivos de Diferentes Marcas.

En el subparametro de Registro de Eventos tanto como FreeNac como PacketFence guardan los archivos de eventos o sucesos pero no como administrarlos.

Para el Asignamiento dinámico de Vlans ambas herramientas tienen una calificación alta debido a la eficacia de estas, a pesar de que estas trabajen con diferentes modos de asignación ya que FreeNac trabaja con VMPS y PacketFence con su propio servicio de administración de los equipos.

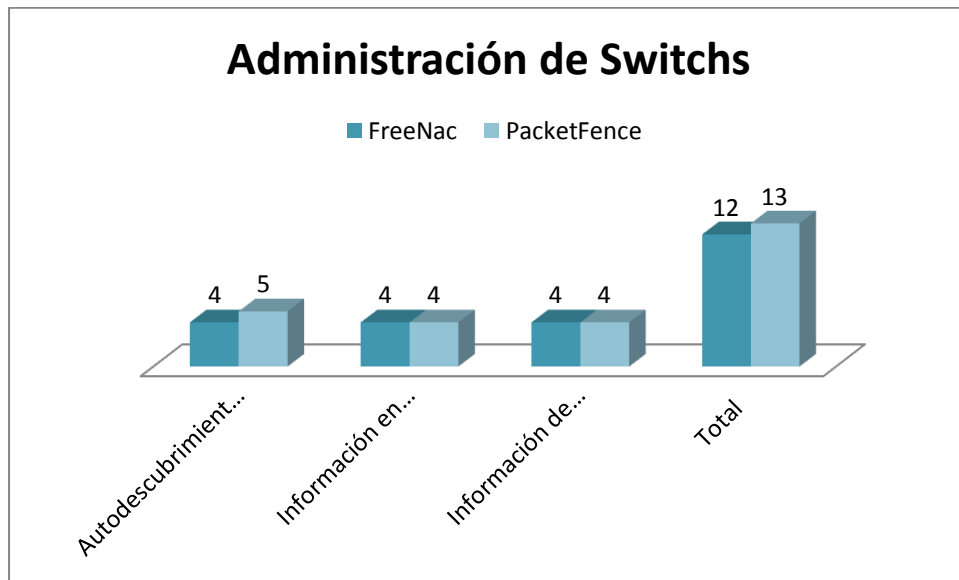


Fig.III.56 Grafica de Resultados de Administración de Switchs

▪ **Autodescubrimiento de Dispositivos y Recolección de Información en Tiempo Real**

Tabla III.XI: Autodescubrimiento Dispositivos y Recolección de Información en Tiempo Real.

	FreeNac	PacketFence
Autodescubrimiento de Dispositivos	Medio Alto	Alto
Información en intervalo de 1 a 3 minutos	Medio Alto	Medio Alto
Información de intervalo de 3 a 5 minutos	Medio Alto	Medio Alto
Total	12	13

En autodescubrimiento de dispositivos observamos que la herramienta FreeNac tiene una calificación media alta debido a que realiza el descubrimiento pero no identifica qu

tipo de sistema operativo posee; lo cual PacketFence si posee incluso nos da la información de con que navegador web esta realizando la autenticación de usuario.

En la información recolectada por las herramientas FreeNac y PacketFence en un intervalo de 1 a 3 minutos es media alta porque las dos herramientas a pesar de detectar los dispositivos finales rápidamente, la información de los dispositivos como sistema operativo y usuario que utilizan no es pronta.

Para el intervalo de 3 a 5 minutos las herramientas presenta una información media alta debido a que se observo que el resto de información como usuarios, agentes, direcciones y puertos se actualizaban en ese rango de tiempo; también esta recolección de información también depende de la cantidad de usuarios que se autentiquen y trabajen con la herramienta.

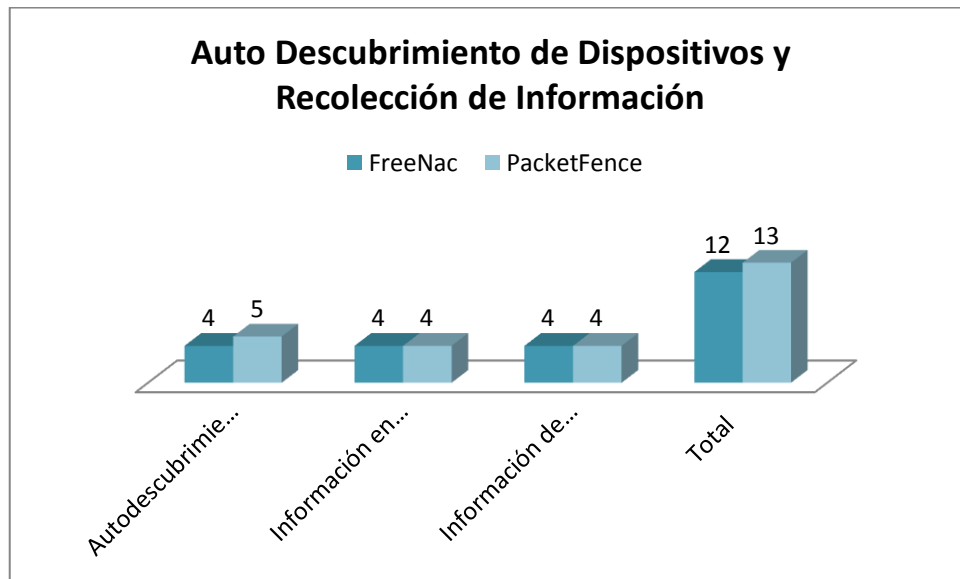


Fig.III.57 Grafica de Resultados de Auto Descubrimiento de Dispositivos.

▪ **Políticas de Red**

Tabla III.XII: Valoración del Parámetro Administración de Switchs.

	FreeNac	PacketFence
Creación o Refuerzo de Políticas de Seguridad de la LAN	Alto	Alto
Aplicación de las Políticas en la Herramienta	Medio	Medio Alto
Políticas de Pre Admisión y Post Admisión	Medio	Alto
Total	11	14

Para el parámetro de políticas de red se obtuvo los siguientes resultados de acuerdo al análisis de las 2 herramientas:

La calificación que obtuvieron las herramientas NAC OpenSource en cuanto a la Creación o Refuerzo de Políticas de Seguridad son altas puesto que las dos herramientas obligan a tener una política de seguridad o mejorarla sin no se la tiene.

Observando la Aplicación de las Políticas en la Herramienta se puede concluir lo siguiente.; La herramienta FreeNac no permite aplicar de una manera completa las políticas de seguridad; En cambio la herramienta PacketFence permite aplicar de una forma más efectiva las políticas de seguridad debido a las diversas herramientas que utiliza para esta solución.

En las Políticas de Pre Admisión y Post Admisión PacketFence tiene una ventaja más clara debido a que para la aplicación de las políticas de pre admisión utiliza Nessus y para la aplicación de las Políticas de Post Admission utiliza Snort; Mientras que FreeNac permite el control de las políticas de Pre Admission mediante simples reglas que controla la herramienta y ayudado por Active Directory, y para Post Admission se controla mediante las reglas del antivirus Mcfee las cuales son propietarias.

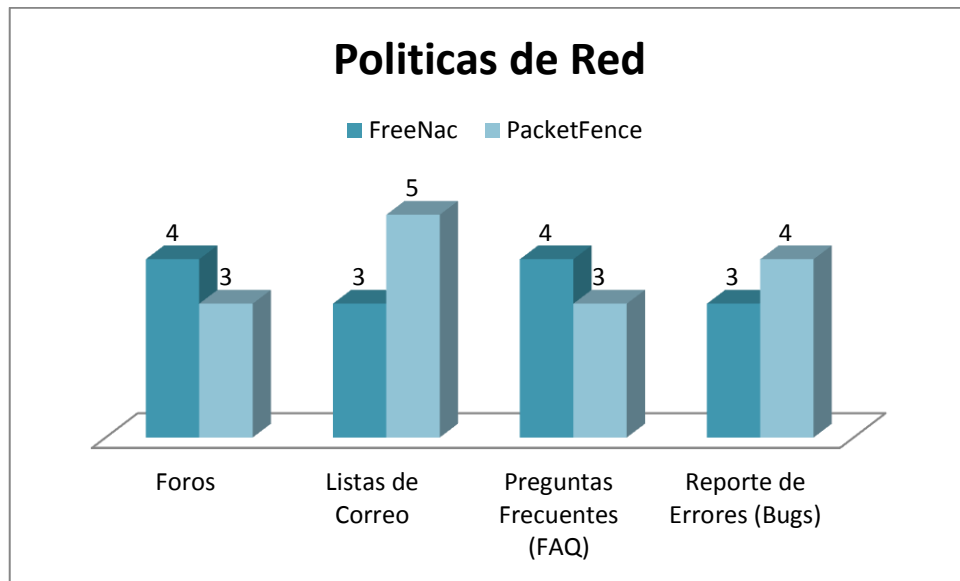


Fig.III.58 Grafica de Resultados del Analisis de Politicas de Red.

▪ **Análisis y Detección de Vulnerabilidades**

Tabla III.XIII: Valoración del Parámetro Análisis y Detección de Vulnerabilidades.

	FreeNac	PacketFence
Analisis Pre Admisión y Post Admisión	Medio	Medio Alto
Detección de Vulnerabilidades	Medio	Medio Alto
Detección de Anomalías	Medio	Alto
Total	9	13

En el Analisis y Detección de Vulnerabilidades se observo lo siguiente:

Analizando las herramientas en el subparametro de Analisis de Pre Admisión y Post Admisión se observo que la herramienta FreeNac no posee muchas opciones para hacer cumplir las políticas de pre admisión y post admisión. Mientras que PacketFence posee herramientas complementarias para el análisis de las políticas de pre admisión y post admisión.

En la Detección de Vulnerabilidades se pudo determinar que la herramienta FreeNac no posee muchos recursos para detectar vulnerabilidades de los dispositivos de finales. PacketFence al integrar la herramienta Nessus puede determinar muchas y un sin numero de vulnerabilidades y dicha herramienta puede ser actualizada constantemente lo cual permite una buena detección de vulnerabilidades.

Refiriendose a la Detección de Anomalías se puede analizar que PacketFence al integrar la herramienta Snort puede detectar un sin numero de vulnerabilidades y además que esta herramienta es OpenSource y puede ser constatemente actualizada se puede detectar un sin número de anomalías; Por otro lado FreeNac no posee una herramienta integrada pero puede integrarse con el antivirus McAfee y su consola EPO para la detección oportuna de anomalías.

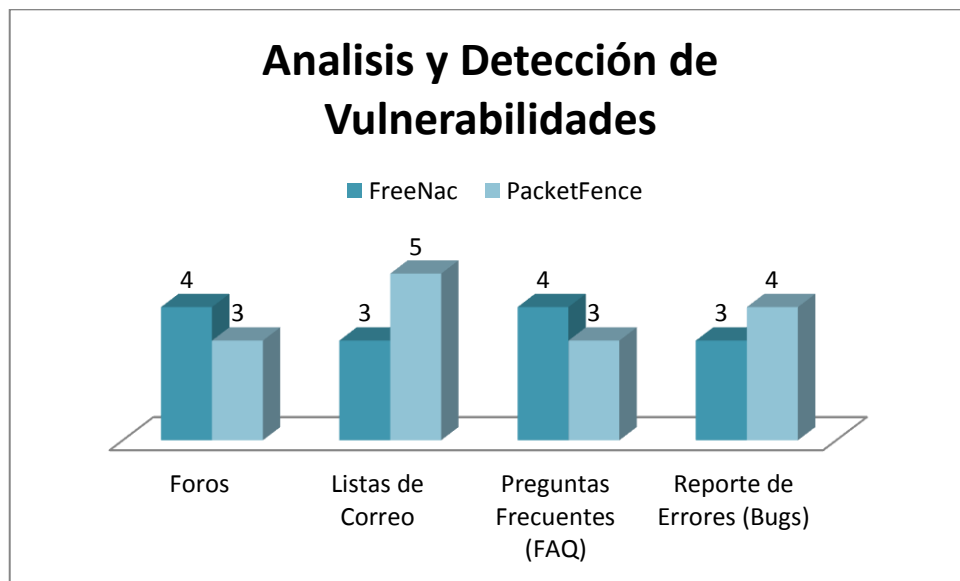


Fig.III.59 Grafica de Resultados del Analisis y Detección de Vulnerabilidades.

▪ **Soporte**

Tabla III.XIV: Valoración del Parámetro Soporte.

	FreeNac	PacketFence
Foros	Medio Alto	Medio
Listas de Correo	Medio	Alto
Preguntas Frecuentes (FAQ)	Medio Alto	Medio
Reporte de Errores (Bugs)	Medio	Medio Alto
Documentación	Medio	Alto
Total	17	20

En el parámetro de Soporte se pudo analizar lo siguiente en las herramientas NAC:

Se pudo observar que la herramienta FreeNac posee un mejor soporte en foros que la herramienta PacketFence puesto que esta prefiere dar soporte por medio de Listas de Correo.

En reporte de errores se pudo observar que PacketFence resolvía más rápidamente los errores en su herramienta que FreeNac debido a que los usuarios reportaban directamente a la Lista de Correo de desarrollo con lo cual los encargados de esta herramienta realizan rápidamente las correcciones necesarias y las publican inmediatamente además que poseen cronogramas de trabajo.

En cuanto a documentación PacketFence posee una documentación más clara y actualiza sus manuales por cada versión que saca de la herramienta; FreeNac ha dejado de lado la actualización de la documentación.

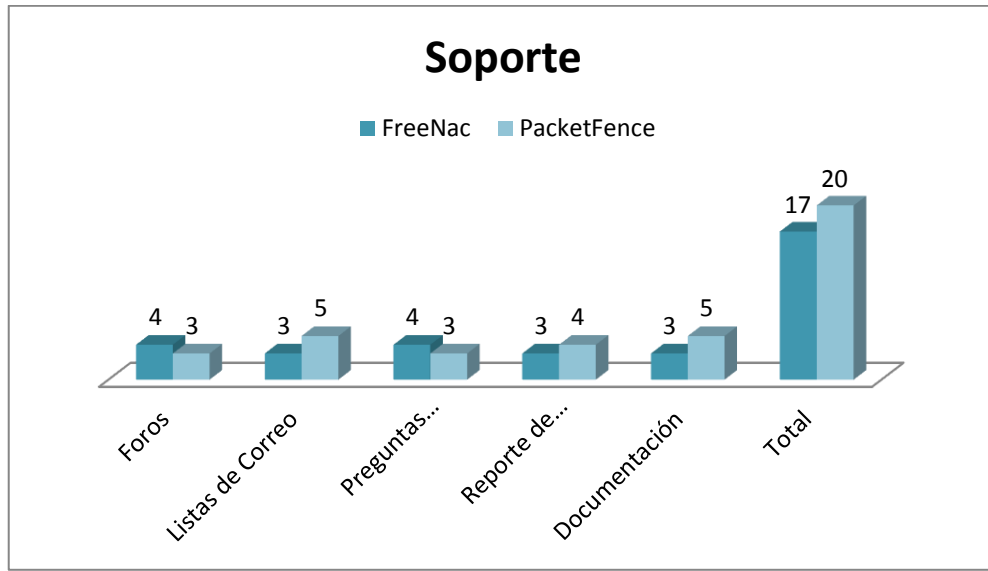


Fig.III.60 Grafica de Resultados del Analisis de Soporte.

▪ **Reportes**

Tabla III.XV: Valoración del Parámetro Reportes.

Herramienta de Administración	FreeNac	PacketFence
Gráficos Estadísticos	Medio Alto	Alto
Eventos	Medio Alto	Alto
Reportes Detallados	Medio Alto	Medio Alto
Total	12	14

En el último parámetro del análisis comparativo de herramientas NAC OpenSource se pudo determinar lo siguiente:

En cuanto a los Gráficos estadísticos PacketFence se le da una alta calificación al generar los gráficos con la librería gráfica de php; mientras que FreeNac posee 2 herramientas gráficas descontinuadas y ni de muy buena calidad.

En el subparámetro Eventos la herramienta FreeNac y PacketFence poseen una calificación alta para manejar los eventos ya que pueden utilizar servicios como rsyslog u otros para generar y presentar los eventos, PacketFence tiene una ligera ventaja

porque también presenta las incidencias como vulnerabilidades, dispositivos puestos en cuarentena automáticamente etc.

En Reportes Detallados PacketFence obtiene una buena calificación debido a la configuración de los reportes los cuales son mucho mas completos debido a que guarda un historial de los dispositivos ingresados a la red, como navegadores web utilizados, puertos a los que se conectaron, violaciones y vulnerabilidades de cada uno de ellos; En cambio FreeNac solo muestra el detalle del equipo y la vulnerabilidad o violación actual.

Resumen Comparativo

Para determinar la herramienta de Control de Admisión a la Red más adecuada se recopiló los resultados obtenidos de cada una de las tablas de los parámetros analizados en una sola tabla, para que de esta manera se pueda realizar la elección de una manera más clara y sencilla los resultados.

Tabla III.XVI: Resumen Comparativo de Herramientas.

PARÁMETROS DE COMPARACIÓN	HERRAMIENTAS NETWORK ADMISSION CONTROL	
	FreeNac	PacketFence
Usabilidad	12	15
Gestión y Administración de Usuarios	11	12
Administración de Switchs	8	13
Autodescubrimiento de Dispositivos y Recolección de Información en Tiempo Real	12	13
Políticas de Red	11	14
Análisis y Detección de Vulnerabilidades	9	13
Soporte	17	20
Reportes	12	14
Total	92	114

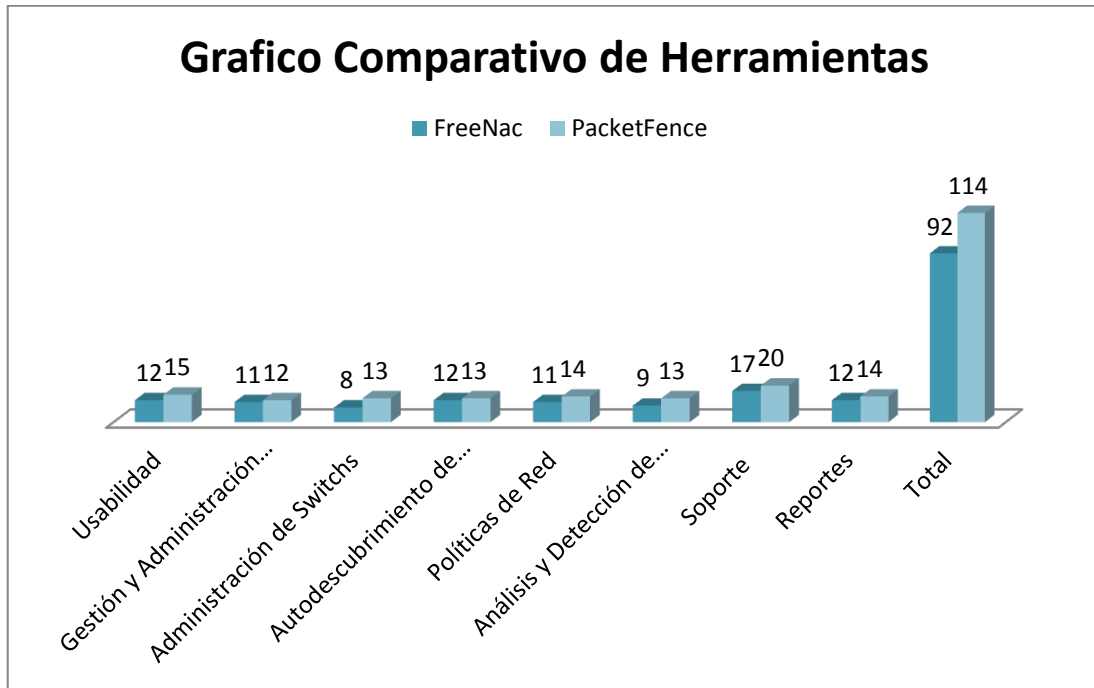


Figura III.61: Grafico Comparativo de Herramientas NAC.

El análisis comparativo de Herramientas NAC OpenSource: PacketFence y FreeNac, realizado en este capítulo nos da como resultados que la herramienta PacketFence con una calificación de 114 sobre la herramienta FreeNac on 92 de calificación, permite obtener las mayores prestaciones de la tecnología NAC y dar solución a los requerimientos del Consejo Nacional de la Judicatura de Chimborazo.

Conclusiones

Las conclusiones que podemos llegar a través del análisis comparativo realizado son las siguientes:

- Instalando las herramientas en el ambiente de pruebas se pudo observar que PacketFence cuenta con mejores características para la administración de la LAN.

- Las dos herramientas cuentan con un buen soporte para la solución y dudas de las preguntas que nacen al implementar la herramienta y recibiendo respuestas inmediatas.
- PacketFence tiene más parámetros dinámicos para la actualización de los datos de la red haciéndola más eficiente en el control de la misma. Además permite una actualización mucha más rápida.
- La herramienta PacketFence es fácil de instalar y configurar debido a que integra otras herramientas OpenSource para administrar la red.
- La administración de Switchs se realiza de diferentes formas en las dos herramientas pero la fortaleza de PacketFence es que tiene compatibilidad con diferentes marcas no solo con los equipos de marca Cisco.
- El análisis y detección de vulnerabilidades es mucho mejor en la herramienta PacketFence ya que permite detectar pre admisión con la herramienta Nessus y post admisión con la herramienta Snort.

CAPITULO IV.

POLÍTICAS DE RED E IMPLEMENTACIÓN DE LA HERRAMIENTA NAC OPENSOURCE EN LA DIRECCIÓN PROVINCIAL DEL CONSEJO DE LA JUDICATURA DE CHIMBORAZO.

4.1 Políticas de Red

Para utilizar correctamente la herramienta NAC es necesario establecer las políticas de seguridad que van a controlar las redes de la institución. Para realizar esto, de acuerdo con el capítulo II, es necesario saber qué es lo se va a proteger, de quien se los va a proteger y como se los va a proteger.

En este capítulo primero se recopila la información acerca del funcionamiento del backbone de la Dirección Provincial del Consejo de la Judicatura de Chimborazo: los recursos conectados a esta, los servicios de Internet que ofrecen sus servidores y las necesidades de la Unidad Informática. Con esta información se establecen las políticas de seguridad a través de un análisis de riesgo de los recursos y el uso y responsabilidades en las redes, para luego diseñar un modelo de seguridad que satisfaga las necesidades de protección de la institución. Después, se establece un plan de acción en caso de que se violen las políticas de seguridad. Para finalmente utilizar esta información para establecer las políticas de seguridad que se implementaran en la herramienta.

4.1.1.1 Recursos conectados al backbone y políticas de funcionamiento.

El Backbone interconecta principalmente a las redes de las dependencias judiciales y administrativas.

La unidad informática es responsable de administrar y operar las redes, de colocar en ellas todos los recursos que consideren necesarios: servidores de servicios de Internet, servidores de información interna, estaciones, impresoras, etc.

Para dar los diferentes servicios de la institución o más específicamente la unidad informática cuenta con algunos servidores para brindar servicios de Internet y aplicaciones. Más tarde en este capítulo se detallaran los servicios que brindan estos hosts.

Existen servidores de aplicaciones (administrativas y de servicio), bases de datos e internet, los cuales representan las herramientas de trabajo tanto para las unidades administrativas como para las dependencias o juzgados de la institución. Debido a la confidencialidad que deben tener los datos, estos servidores son considerados de alto riesgo e importantes para el funcionamiento de la Dirección Provincial del Consejo de la Judicatura de Chimborazo. Por lo tanto, surge la necesidad de utilizar mecanismos de protección que garanticen la integridad de los datos para otorgar confiabilidad a los sistemas.

El backbone continúa físicamente en el edificio ubicado en las calles 10 de Agosto y Pichincha por medio de un enlace de fibra óptica. Actualmente la red LAN posee una conexión a Internet a través del servicio proporcionado por la Corporación Nacional de Telecomunicaciones (CNT).

En el análisis de riesgo se conocerán más detenidamente todos los recursos disponibles. En la figura No. IV.1 se aprecian todos los recursos.

4.1.1.2 Servicios de Red

De acuerdo a las necesidades de la Unidad Informática, estaposee algunos servidores y proveen diferentes servicios:

HP Proliant ML370 (Servidor 1):

Servidor DHCP.

Servidor de Correo electrónico.

Servidor Proxy.

HP Proliant ML370 (Servidor 2):

Servidor Web.

HP Proliant ML370 (Servidor 3):

Servidor del Sistema de Pensiones Alimenticias.

HP DL380G7 X55650 PERF (Servidor 4):

Servidor del Sistema de Trámite Judicial (SATJE).

HP DL380G7 X55650 PERF (Servidor 5):

Servidor para Network Admission Control.

Servidor Proxy.

BLADE S12 (Servidor 6):

Servidor de Nombres de Dominio (DNS).

Servidor de Directorio Activo (Active Directory).

BLADE S12 (Servidor 7):

Servidor del Sistema de Trámite Judicial para los cantones.

HP DX220MT (Servidor 8):

Servidor del Sistema de Relojes.

HP 6000 Pro (Servidor 9):

Servidor de Información del Sistema de Trámite Judicial.

HP COMPAQ 8100 Elite (Servidor 10):

Servidor de Información del Sistema de Trámite Judicial para los Touch Screen.

Más adelante en este capítulo se detallaran los servicios de Internet más comunes, sus vulnerabilidades y los métodos más efectivos para protegerlos.

4.1.2 Análisis de Riesgo

En base al análisis de riesgo revisado en el capítulo II, sección 2.4 los recursos de la institución son evaluados en base al producto de dos factores: riesgo de pérdida (R) e importancia (W).

El resultado de una multiplicación (para obtener el riesgo total) es lo que se desea en la Unidad Informática o lo que se quiere expresar.

Para una mayor visualización de los dos factores involucrados, el factor de riesgo (R) se obtiene a partir del promedio de tres posibles amenazas; y la importancia (W), a partir de tres características intrínsecas que distinguen al recurso.

Las amenazas analizadas para el factor de riesgo son:

- **Accesos No Autorizados:** Solo aquellos usuarios permitidos deben tener acceso a un recurso. Esta es una medida de cuán probable es que un usuario no autorizado ingrese o tome el recurso.

- **Robo de Información:** Es necesario que se ponga a disposición información importante. Esta es una medida de cuan probable es que un usuario obtenga información calificada como confidencial.
- **Negación de Servicio:** Cuán probable es que un servicio este fuera de operación.

Las características analizadas para el factor de importancia son:

- **Disponibilidad:** Cuán importante es tener disponible un recurso todo el tiempo.
- **Integridad:** Cuán importante es que el recurso o los datos que contiene Sean consistentes.
- **Confidencialidad:** Cuan restringido debe ser el acceso a un recurso.

Para calificar a cada una de estas variables se utilizó la siguiente terminología:

Tabla IV.I: Tabla de Terminología.

Riesgo			Importancia		
Acceso No Autorizado	Robo de Información	Negación de Servicios	Disponibilidad	Integridad	Confidencialidad
Ninguno	Ninguno	Ninguno	Ninguna	Ninguna	Ninguna
Bajo	Bajo	Bajo	Baja	Baja	Baja
Moderado	Moderado	Moderado	Moderada	Moderada	Moderada
Alto	Alto	Alto	Alta	Alta	Alta

Cada uno de estas calificaciones fueron proporcionadas por laIngeniería María Cristina Palmay López encargada de la seguridad de la Redes en la Unidad Informática y la Ingeniería Lorena Catalina García encarga de la Unidad Informática. Cabe destacar que se consideró los criterios de las personas anteriormente nombradas debido a que manejan diariamente los equipos y sistemas proporcionados por la Unidad Informática de la institución y por lo tanto son las másidóneas para proporcionar este tipo de

información. Por cada fuente se realizó un análisis de riesgo por separado para luego contrastar los resultados de ambos.

A cada recurso conectado al backbone se le ha asignado un número identificador y una pequeña descripción, las cuales se pueden observar en el siguiente gráfico.

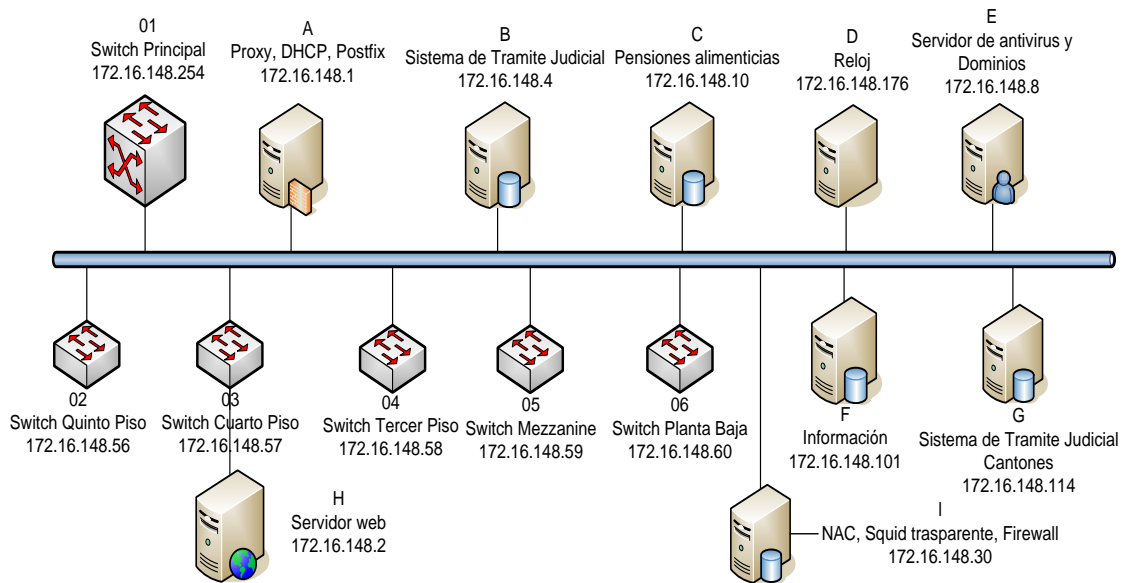


Figura IV.1: Backbone Edificio Principal de la Institución.

El desarrollo de los procedimientos del análisis de riesgo se encuentra en el Anexo A. Los resultados de riesgos totales por cada recurso conectado en el backbone de la institución son:

Tabla IV.II: Resultados del Análisis de Riesgo del Backbone.

RECURSOS		Riesgo Total
No.	Nombre o Descripción	RxW
Equipos de Red		
01	Switch Principal (4503 Capa 3)	70
02	Switch Quinto Piso (2960 Capa 2)	81
03	Switch Cuarto Piso (2960 Capa 2)	81
04	Switch Tercer Piso (2960 Capa 2)	81
05	Switch Mezanine (2960 Capa 2)	81

06	Switch Planta Baja (2960 Capa 2)	81
Servidores		
A	Servidor DHCP, Postfix	90
B	Servidor de Aplicaciones Satje	100
C	Servidor de Pensiones Alimenticias	90
D	Servidor de Reloj	64
E	Servidor de Antivirus y Dominios	72
F	Servidor de Información	81
G	Servidor de Trámite Judicial	90
H	Servidor Web	80
I	Servidor NAC, Squid Transparente, Router	56

Los valores se evaluarán en una escala del 0 al 100. Donde 0 representará ningún riesgo y 100 un riesgo alto.

4.1.3 Conclusiones del Análisis de Riesgos.

Los riesgos han sido calificados en base a tres categorías:

- **ALTO (+):** El riesgo es muy alto. Se tomó el rango de 90 a 100.
- **ALTO (-):** El riesgo es alto, pero tiene un grado de moderado que lo hace menos alto. A esta categoría se la puede denominar “riesgo alto moderado”. Se tomó el rango de 75 a 89.
- **MODERADO (+):** El riesgo es moderado. Se tomó el rango de 65 a 74.
- **MODERADO (-):** El riesgo es moderado con un grado de bajo. A esta categoría se la puede denominar “riesgo casi bajo”. Se tomó el rango de 50 a 64.

El detalle de la obtención de un criterio para la calificación final de los recursos se encuentra en el Anexo A.

La mayoría de los recursos conectados al backbone poseen un “riesgo alto moderado”, es decir no existe alguno que no posea ningún riesgo y que no sea importante. De acuerdo a la tabla anterior, los recursos hallados más críticos, es decir de muy alto riesgo, es el servidor del sistema judicial: Hardware, Sistema Operativo y Base de Datos. El recurso de riesgo “casi bajo” es el servidor de NAC.

Dado estos resultados, todos los recursos necesitan protección, unos más que otros dependiendo de la categoría en que se encuentren. Las medidas de protección que se pueden tomar para cada uno de los recursos se encuentran en el modelo de seguridad.

4.1.4 Usos y Responsabilidades de la Redes Institucionales.

Para establecer el uso y responsabilidades en las redes de la institucional es necesario seguir los siguientes pasos:

4.1.4.1 Identificando los Usuarios.

Básicamente existen 2 tipos de usuarios: usuarios internos y externos. Dentro de los usuarios internos existen los siguientes tipos:

Administrador: Las personas que laboran en la unidad informática de redes de la Dirección Provincial del Consejo de la Judicatura de Chimborazo. Estos son usuarios con privilegios especiales sobre todos los sistemas de la institución conectados al backbone.

Personal administrativo: Se refiere a todas las personas vinculadas a la institución que no se dedican a las actividades judiciales. Dentro de este grupo pueden existir subgrupos dependiendo de las necesidades de los mismos. Ej. Director, Analistas de las Unidades Financieras y Administrativas.

Funcionarios Judiciales: Todas las personas que trabajan en la institución. También pueden tener subgrupos de acuerdo a los cargos que ocupan. Ej. Jueces, Secretarios y Ayudantes Judiciales.

Usuarios Externos: Son aquellos usuarios que provienen de Internet.

Usuarios Invitados: Son los usuarios externos a la institución pero que utilizan los recursos internos de la institución Ej. Conferencistas, Analistas de otras provincias, Capacitadores de Aplicaciones, etc.

Los tipos de acceso posibles son:

Lectura: El usuario solo puede leer

Escritura: El usuario puede escribir

Ejecución: El usuario puede ejecutar cualquier programa.

Total: Acceso físico, archivos del sistema: lectura, escritura y ejecución

Cuando se habla de acceso a todo tipo de usuarios, se incluye al usuario administrador con todo tipo de acceso.

4.1.4.2 Uso Apropiado de los Recursos de la Red

En todos los recursos a los que solo tiene acceso el usuario administrador este debe detallar cuál es el uso apropiado de los mismos. Por su propia naturaleza, todos estos recursos son restringidos para los demás usuarios, es decir, no deben estar al alcance de los usuarios no autorizados ya que según los resultados del análisis de riesgo son de mucha importancia y alto riesgo.

Para el caso de los usuarios del Servidor Satje, se define como uso aceptable de estos recursos lo dispuesto en las normas y reglamentos que la institución ha dispuesto para el correcto uso de los servicios de Internet. Las contravenciones a estos reglamentos serán considerados como usos inaceptables y propios para sanciones.

Tabla IV.II: Usuarios autorizados para utilizar los recursos.

RECURSOS		Tipo de Acceso	Tipo de Usuario
No.	Nombre o Descripción		
Equipos de Red			
01	Switch Principal (4503 Capa 3)	Total	Administradores
02	Switch Quinto Piso (2960 Capa 2)	Total	Administradores
03	Switch Cuarto Piso (2960 Capa 2)	Total	Administradores
04	Switch Tercer Piso (2960 Capa 2)	Total	Administradores
05	Switch Mezanine (2960 Capa 2)	Total	Administradores
06	Switch Planta Baja (2960 Capa 2)	Total	Administradores
Servidores			
A	Servidor DHCP, Postfix (Correo Electrónico)	Total	Administradores
B	Servidor de Aplicaciones Satje	Ejecución de Aplicación	Todos los Usuarios Excepto Externos e Invitados
		Total	Administradores
C	Servidor de Pensiones Alimenticias	Ejecución de Aplicación	Personal Administrativo
		Total	Administradores
D	Servidor de Reloj	Total	Administradores
E	Servidor de Antivirus y Dominios	Total	Administradores
F	Servidor de Información	Ejecución de Aplicación	Todos los usuarios excepto externos e invitados
		Total	Administradores
G	Servidor de Trámite Judicial de los Cantones	Ejecución de Aplicación	Todos los usuarios excepto externos e invitados
		Total	Administradores
H	Servidor Web	Ejecución de Aplicación Web	Todos los Usuarios.
		Total	Administradores.
I	Servidor NAC, Squid Transparente, Router	Total	Administradores

Las aplicaciones administrativas son de uso restringido, tan solo usuarios de tipo administrativo tienen acceso, y estos a su vez, tienen acceso de acuerdo a los módulos de seguridad (tipos de usuarios) de las aplicaciones.

Cualquier acción en contra de la confidencialidad e integridad de los datos que manejan estas aplicaciones será considerada inaceptable y propia para sanción.

Para las redes conectadas al backbone, los administradores de las mismas se encargaran de dictar el uso apropiado de cada uno de sus recursos teniendo como objetivo no causar problemas que afecten a los recursos del backbone. Por ejemplo, el uso no apropiado de una maquina cliente de una aplicación administrativa puede ocasionar accesos no autorizados al servidor de la aplicación y causar un perjuicio a la institución debido a la información sensible que contienen los servidores.

4.1.4.3 Determinación de quien está autorizado para otorgar acceso y aprobar el uso.

La Unidad informática podrá disponer de sus redes y proveer a sus usuarios de todos los servicios que ofrece el backbone. Los administradores de la red definen los usuarios de sus servidores, sus características y privilegios.

La Unidad Informática es la entidad encargada para otorgar acceso de las redes y aprobar el correcto uso de estas.

4.1.4.4 Determinación de las responsabilidades de los usuarios.

Las aplicaciones administrativas y sistemas judiciales poseen módulos de seguridad en los cuales se definen los tipos de usuarios y las responsabilidades de cada uno de acuerdo a la función que desempeñan.

Todas las judicaturas tendrán que acatar las normas y reglas para conectarse a la red según lo que disponga la Unidad Informática.

Los administradores serán responsables de proteger todos los recursos en la red institucional, publicar sus propias políticas de seguridad y proceder ante posibles violaciones de seguridad.

4.1.4.5 Determinación de las Responsabilidades de los Administradores

La Unidad Informática es la entidad encargada de determinar cuál es el alcance de los usuarios administradores. Los usuarios administradores tienen acceso a todos los recursos conectados al backbone y a los recursos de cada red conectada al backbone. Para esto, los administradores deben poseer la cuenta y contraseña de cada uno de los recursos conectados al backbone.

4.1.4.6 Información Sensible

Las máquinas que contienen información sensible son los servidores de las aplicaciones, bases de datos y equipos de red, a las cuales tienen acceso solo los usuarios autorizados de las aplicaciones administrativas, judiciales y financieras. Estos usuarios son divididos en varios subtipos dependiendo de las funciones que realizan y el grado de accesibilidad a los datos (escritura, lectura, ejecución de procesos). Pero como se advirtió anteriormente, estas aplicaciones poseen módulos de seguridad en los que se definen a los usuarios autorizados y las acciones que estos pueden realizar.

4.1.5 Plan de acción ante violación de políticas de seguridad.

En esta sección se asume que las redes interconectadas en el backbone poseen la protección adecuada. De acuerdo con la sección 2.6. Plan de acción, cuando las políticas de seguridad son violadas, una organización se puede acoger a dos estrategias:

- Proteger y proceder.
- Perseguir y acusar.

Antes de presentar un plan de acción ante una eventual violación de políticas de seguridad en la institución es necesario evaluar las condiciones para ambas estrategias:

4.1.5.1 Condiciones para proteger y proceder

Esta estrategia consiste en proteger los recursos de la red y restaurar cualquier daño ocasionado por un ataque. Se debe adoptar esta estrategia si se cumplen las siguientes condiciones aplicadas para las redes de la institución:

Que los recursos estén protegidos: Para el caso de la institución no se cumple esta condición debido a que los recursos si están bien protegidos de acuerdo al modelo de seguridad presentado. Los recursos del backbone más importantes poseen hasta 3 niveles de redundancia (servidores de aplicaciones y bases de datos).

Que una actividad intrusa continuamente ocasione un gran daño y riesgo financiero: Si se presentasen actividades intrusas en los recursos del backbone, estas ocasionarían daños que pudieran ser fácilmente recuperables (por ejemplo: servidor web, correo electrónico.). En el caso de los servidores de aplicaciones y bases de datos, los riesgos financieros serían cuantiosos. Esta condición se cumple a medias.

Que exista un considerable riesgo para los usuarios de la red: Los usuarios internos de la institución, en su mayoría empleados judiciales, siempre van a estar expuestos a las capturas de contraseñas de cuentas. No se cumple esta condición.

Que el costo de una persecución a un intruso sea muy alto: El costo de persecución es alto debido a que los firewalls internos y externo deben poseer mecanismos o trampas para capturar a un intruso. Si se cumple esta condición.

4.1.5.2 Condiciones para perseguir y acusar

Esta estrategia consiste en perseguir a los intrusos, obtener pruebas de los ataques que han ocasionado y acusarlos ante una agencia de leyes. Se debe adoptar esta estrategia si se cumplen las siguientes condiciones aplicadas para las redes de la institución:

Que los recursos y sistemas estén bien protegidos: Los recursos conectados al backbone son bien protegidos. Se cumple esta condición.

Que la red haya sido centro de ataques de intrusos y estos no dejan de hacerlo: Por su concepción de entidad académica abierta a Internet, la probabilidad de ser blanco de ataques es alta. Se cumple esta condición.

Que el local sea apropiado para incurrir el riesgo de un acceso no autorizado: Al poseer redundancia en seguridad para cada recurso, si se puede correr el riesgo de permitir a los intrusos continuar. Se cumple con la condición.

Que las herramientas de monitoreo y registro puedan archivar bastante información: Capacidades de registro y monitoreo son requerimientos para el firewall que la institución decida adquirir. Se cumple con la condición.

Que exista disponibilidad para acusar: En Ecuador no existe ninguna ley para condenar las actividades intrusas realizadas por medios computacionales. Sin embargo, existen entidades internacionales que ayudan dando consejos a las partes involucradas para resolver este tipo de problemas. Estas entidades no tienen jurisdicción en Ecuador, pero no se puede descartar las posibles soluciones que estas planeen. La condición se cumple parcialmente.

4.1.6 Conclusiones

Se podría pensar que la estrategia “perseguir y acusar” es la estrategia más adecuada para la institución debido a que se cumplen la mayoría de sus condiciones; sin embargo, no sirve de mucho adquirir mecanismos sofisticados para capturar a hackers si no existen leyes que condenen estas acciones. Estos mecanismos servirían nada más para obtener información de cómo penetraron, quienes son y cuáles fueron sus intenciones.

En el caso eventual de que la violación suceda por mala configuración de las seguridades, se corre peligro a pesar de tener redundancia de seguridad en los recursos. Estas brechas pueden producir otras brechas y así sucesivamente hasta que un recurso quede totalmente desprotegido. En este caso sería urgente adoptar una estrategia de “proteger y proceder”.

Dado lo anterior, no se puede pensar en adoptar una sola estrategia de respuesta para la institución. Es necesario llegar a un punto de equilibrio entre ambas estrategias de tal manera que se proteja y recupere, pero también se persiga y acuse. Entonces, en el caso de incidentes que violen las políticas de seguridad en el backbone, las actividades a realizar serían las siguientes:

1. Determinar qué políticas han sido violadas y evaluar la situación.
2. Investigar cómo y cuándo se violó la o las políticas de seguridad.
3. Descubrir quien violó las políticas de seguridad.
4. Corregir los errores y aplicar las sanciones respectivas a los culpables dependiendo del tipo de violación y del tipo de usuario.

En el caso de que los atacantes sean usuarios internos, las sanciones son determinadas en base a los reglamentos que dispone la institución. En el caso de que usuarios externos violen los sistemas internos es necesario tener soporte por parte de entidades (agencias de leyes) encargadas de resolver este tipo de problemas.

En el caso de que usuarios internos violen sistemas de organizaciones externas, y estas lo notifiquen y prueben estas acciones ante la Unidad Informática, será necesario establecer nuevas sanciones en los reglamentos de la institución en común acuerdo con las sanciones que las agencias de leyes recomienden.

4.2 Implementación De La Herramienta Y Su Aplicación A La Dirección Provincial Del Consejo De La Judicatura De Chimborazo.

La herramienta PacketFence fue implementada en el Sistema Operativo Centos 5.6. La instalación, implementación y configuración de la herramienta se encuentra detallada en el Anexo C.

4.2.1 Administración de la Herramienta.

Antes de iniciar con el proceso de monitoreo de los diferentes dispositivos, en la herramienta Packetfence, se debe configurar los equipos de red en nuestro caso Switchs.

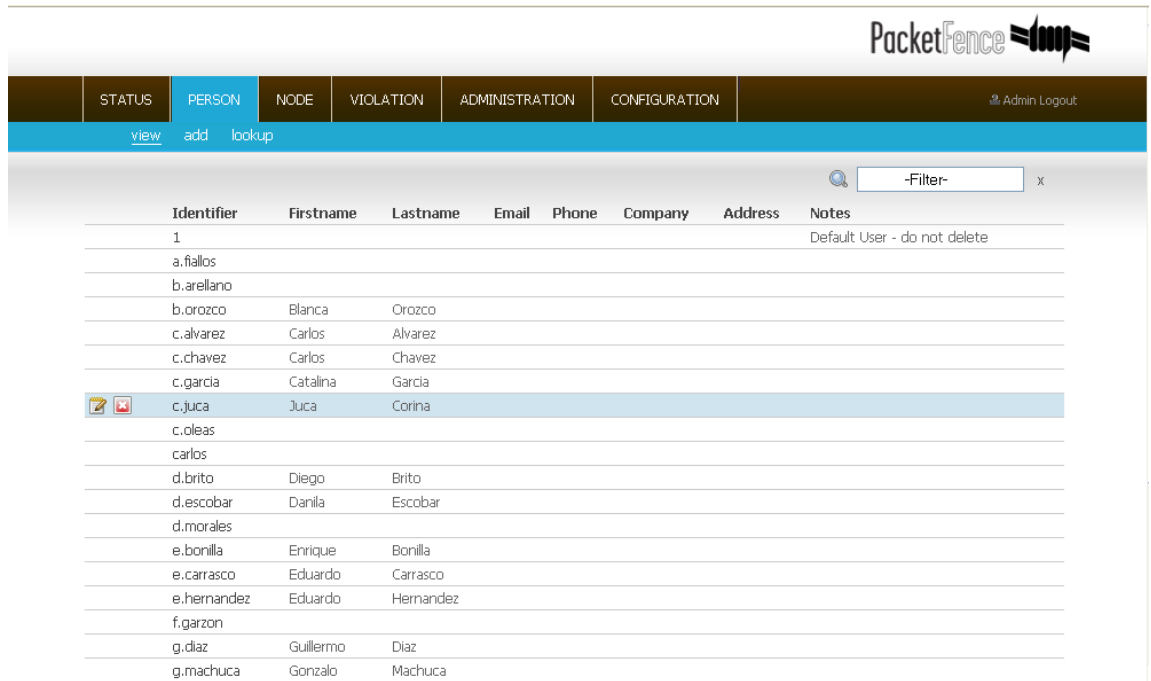
4.2.1.1 Administración de Usuarios

La herramienta ofrece varias formas de administrar usuarios para el registro y posterior acceso a la Red LAN; La opción que se eligió fue de forma manual debido a conflictos con el dominio.

Para agregar un usuario puede ser directamente en un archivo de texto creado con el comando:

```
htpasswd /usr/local/pf/conf/user.conf
```

A través del sitio web en la opción de Person podemos visualizar los usuarios ya registrados en la herramienta.



The screenshot shows the PacketFence user management interface. At the top right is the PacketFence logo. Below it is a navigation bar with tabs: STATUS, PERSON (selected), NODE, VIOLATION, ADMINISTRATION, and CONFIGURATION. Under the PERSON tab, there are links for 'view', 'add', and 'lookup'. A search bar with '-Filter-' and a magnifying glass icon is present. The main content is a table of users with the following columns: Identifier, Firstname, Lastname, Email, Phone, Company, Address, and Notes. The user 'c.juca' is highlighted in blue.



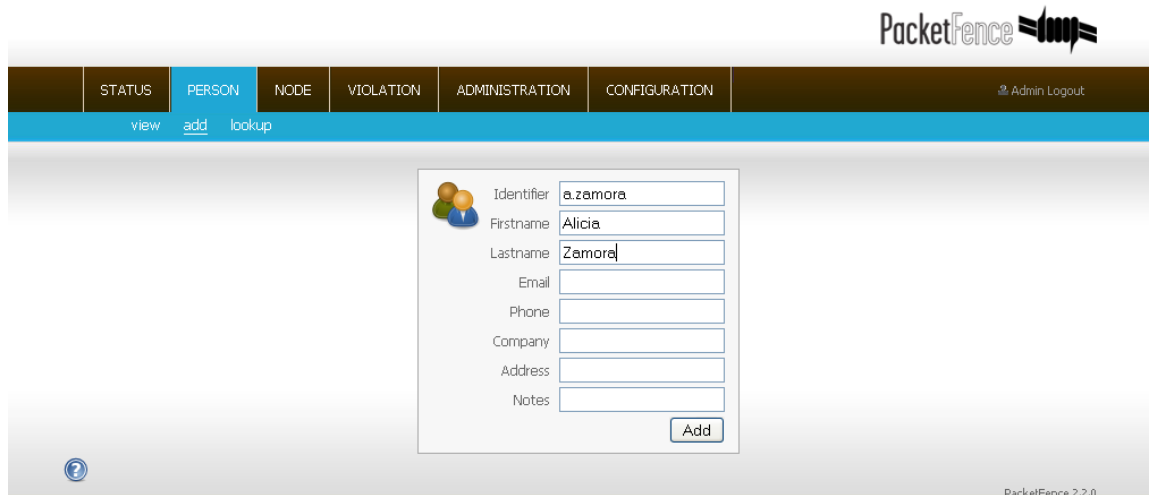
Identifier	Firstname	Lastname	Email	Phone	Company	Address	Notes
1							Default User - do not delete
a.fiallos							
b.arellano							
b.orozco	Blanca	Orozco					
c.alvarez	Carlos	Alvarez					
c.chavez	Carlos	Chavez					
c.garcia	Catalina	Garcia					
  c.juca	Juca	Corina					
c.oleas							
carlos							
d.brito	Diego	Brito					
d.escobar	Danila	Escobar					
d.morales							
e.bonilla	Enrique	Bonilla					
e.carrasco	Eduardo	Carrasco					
e.hernandez	Eduardo	Hernandez					
f.garzon							
g.diaz	Guillermo	Diaz					
g.machuca	Gonzalo	Machuca					

Figura IV.2: Interfaz principal para la administración de usuarios.

Para agregar un usuario vamos a la opción Add dentro de la interfaz Person, luego podemos llenar los datos siendo el campo más importante el id.



The screenshot shows the PacketFence 'Add User' form. At the top right is the PacketFence logo. Below it is a navigation bar with tabs: STATUS, PERSON (selected), NODE, VIOLATION, ADMINISTRATION, and CONFIGURATION. Under the PERSON tab, there are links for 'view', 'add' (selected), and 'lookup'. The main content is a form with the following fields: Identifier (a.zemora), Firstname (Alicia), Lastname (Zemora), Email, Phone, Company, Address, and Notes. An 'Add' button is at the bottom right of the form.

Identifier	<input type="text" value="a.zemora"/>
Firstname	<input type="text" value="Alicia"/>
Lastname	<input type="text" value="Zemora"/>
Email	<input type="text"/>
Phone	<input type="text"/>
Company	<input type="text"/>
Address	<input type="text"/>
Notes	<input type="text"/>

Figura IV.3: Añadir usuarios.

También podemos revisar las direcciones MAC asociados a una persona por ejemplo:

The screenshot shows the PacketFence web interface. At the top right is the PacketFence logo. Below it is a navigation bar with tabs: STATUS, PERSON (selected), NODE, VIOLATION, ADMINISTRATION, and CONFIGURATION. There is also an 'Admin Logout' link. Below the navigation bar are links for 'view', 'add', and 'lookup'. The main content area is titled 'Lookup a PID' and contains a search form with 'j.coello' entered and a 'Lookup' button. To the right of the search form, the results for 'Pid: j.coello' are displayed. The results are organized into two sections, each listing 'MACs associated with this PID' and providing detailed information for each MAC address.

Lookup a PID
PID:

Pid: j.coello

MACs associated with this PID:

MAC: 00:0f:fe:05:9e:a0
Computer Name: V3AUX3ADNINEZ1
Category: ninez
Status: reg
VoIP: no
Detect Date: 2011-10-18 09:41:14
Reg Date: 2011-10-25 14:26:55
Last connection: Wired SNMP
Last Switch: 172.16.148.61
Last Port: 10011
Last VLAN: 3
User-Agent: Mozilla 5.0 Windows; U; Windows NT 5.1; es-ES; rv:1.9.2.13 Gecko 20101203 Firefox 3.6.13
OS (dhcp): 1,15,3,6,44,46,47,31,33,249,43
Last DHCP Time: 2012-02-24 10:20:21
OS Class: Microsoft Windows XP
MAC: 00:0f:fe:cfc4:bd
Computer Name: V3SECRADNINEZ1
Category: ninez

Reg Date: 2011-10-25 14:26:55
Last connection: Wired SNMP
Last Switch: 172.16.148.61
Last Port: 10011
Last VLAN: 3
User-Agent: Mozilla 5.0 Windows; U; Windows NT 5.1; es-ES; rv:1.9.2.13 Gecko 20101203 Firefox 3.6.13
OS (dhcp): 1,15,3,6,44,46,47,31,33,249,43
Last DHCP Time: 2012-02-24 10:20:21
OS Class: Microsoft Windows XP
MAC: 00:0f:fe:cfc4:bd
Computer Name: V3SECRADNINEZ1
Category: ninez
Status: reg
VoIP: no
Detect Date: 2011-08-23 07:55:14
Reg Date: 2011-10-25 14:36:56
Last connection: Wired SNMP
Last Switch: 172.16.148.61
Last Port: 10029
Last VLAN: 3
User-Agent: Mozilla 5.0 Windows NT 6.1; rv:5.0 Gecko 20100101 Firefox 5.0
OS (dhcp): 1,15,3,6,44,46,47,31,33,121,249,43
Last DHCP Time: 2012-02-24 15:52:27
OS Class: Microsoft Windows Vista/7 or Server 2008

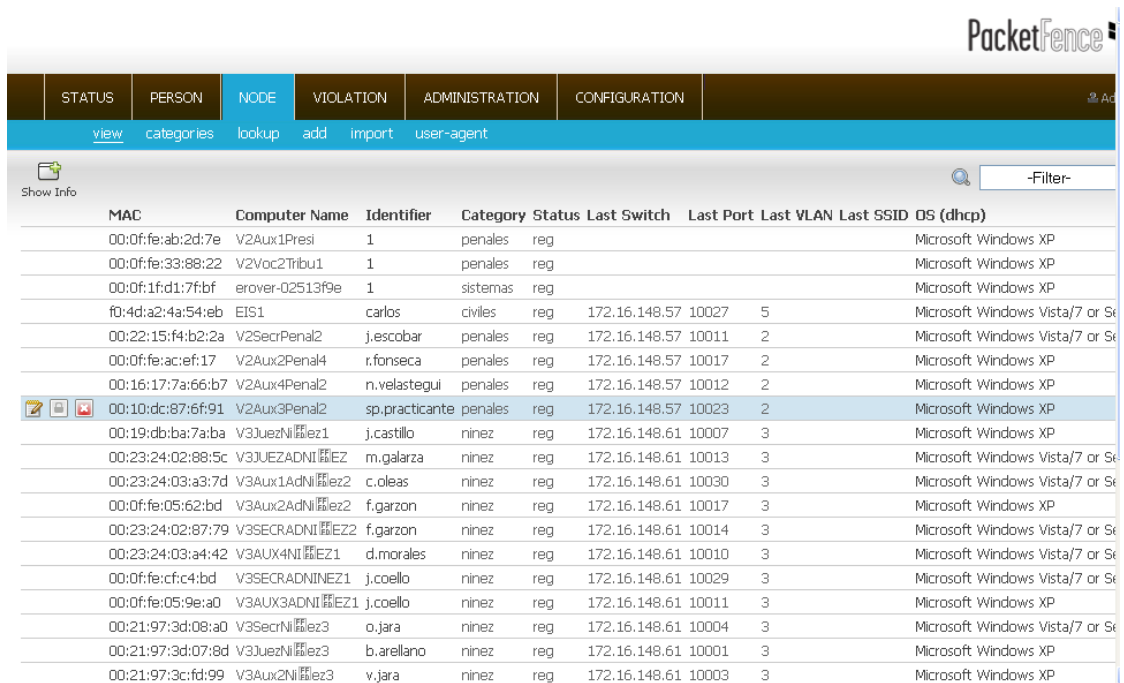
PacketFence 2.2.0

Figura IV.4: Información detallada de usuarios.

4.2.1.2 Administración de Dispositivos

PacketFence ofrece la opción de administrar dispositivos en forma manual, permitiendo tener un dispositivo previamente configurado y listo para que ingrese a la red LAN, sin tener que pasar por el registro en el portal captivo.

Para acceder a esta opción ingresamos en el sitio de administración de la herramienta y escogemos la opción Node; En la figura de abajo podemos ver todos los dispositivos que ha detectado la herramienta sean ya registrados o no; así como otras características de los dispositivos como son MAC, Nombre del Computador, Usuario, Categoría, Estado, Ultimo Switch, Ultimo puerto conocido en el Switch, Ultima Vlan y Sistema Operativo. Además se puede acceder a otras opciones desde esta misma interfaz.



MAC	Computer Name	Identifier	Category	Status	Last Switch	Last Port	Last VLAN	Last SSID	OS (dhcp)
00:0f:fe:ab:2d:7e	V2Aux1Presi	1	penales	reg					Microsoft Windows XP
00:0f:fe:33:88:22	V2Voc2Tribu1	1	penales	reg					Microsoft Windows XP
00:0f:1f:d1:7f:bf	erover-02513f9e	1	sistemas	reg					Microsoft Windows XP
f0:4d:a2:4a:54:eb	EIS1	carlos	civiles	reg	172.16.148.57	10027	5		Microsoft Windows Vista/7 or Se
00:22:15:f4:b2:2a	V2SecrPenal2	j.escobar	penales	reg	172.16.148.57	10011	2		Microsoft Windows Vista/7 or Se
00:0f:fe:ac:ef:17	V2Aux2Penal4	r.fonseca	penales	reg	172.16.148.57	10017	2		Microsoft Windows XP
00:16:17:7a:66:b7	V2Aux4Penal2	n.velastegui	penales	reg	172.16.148.57	10012	2		Microsoft Windows XP
00:10:dc:87:6f:91	V2Aux3Penal2	sp.practicante	penales	reg	172.16.148.57	10023	2		Microsoft Windows XP
00:19:db:ba:7a:ba	V3JuezNiñez1	j.castillo	ninez	reg	172.16.148.61	10007	3		Microsoft Windows XP
00:23:24:02:88:5c	V3JUEZADNIÑEZ	m.galarza	ninez	reg	172.16.148.61	10013	3		Microsoft Windows Vista/7 or Se
00:23:24:03:a3:7d	V3Aux1AdNiñez2	c.oleas	ninez	reg	172.16.148.61	10030	3		Microsoft Windows Vista/7 or Se
00:0f:fe:05:62:bd	V3Aux2AdNiñez2	f.garzon	ninez	reg	172.16.148.61	10017	3		Microsoft Windows XP
00:23:24:02:87:79	V3SECRADNIÑEZ2	f.garzon	ninez	reg	172.16.148.61	10014	3		Microsoft Windows Vista/7 or Se
00:23:24:03:a4:42	V3AUX4NIÑEZ1	d.morales	ninez	reg	172.16.148.61	10010	3		Microsoft Windows Vista/7 or Se
00:0f:fe:cf:c4:bd	V3SECRADNINEZ1	j.coello	ninez	reg	172.16.148.61	10029	3		Microsoft Windows Vista/7 or Se
00:0f:fe:05:9e:a0	V3AUX3ADNIÑEZ1	j.coello	ninez	reg	172.16.148.61	10011	3		Microsoft Windows XP
00:21:97:3d:08:a0	V3SecrNiñez3	o.jara	ninez	reg	172.16.148.61	10004	3		Microsoft Windows Vista/7 or Se
00:21:97:3d:07:8d	V3JuezNiñez3	b.arellano	ninez	reg	172.16.148.61	10001	3		Microsoft Windows XP
00:21:97:3c:fd:99	V3Aux2Niñez3	v.jara	ninez	reg	172.16.148.61	10003	3		Microsoft Windows XP

Figura IV.5: Interfaz principal para la administración de dispositivos.

En la opción Categories podemos visualizar como se organizo las categorías para clasificar a los dispositivos finales.

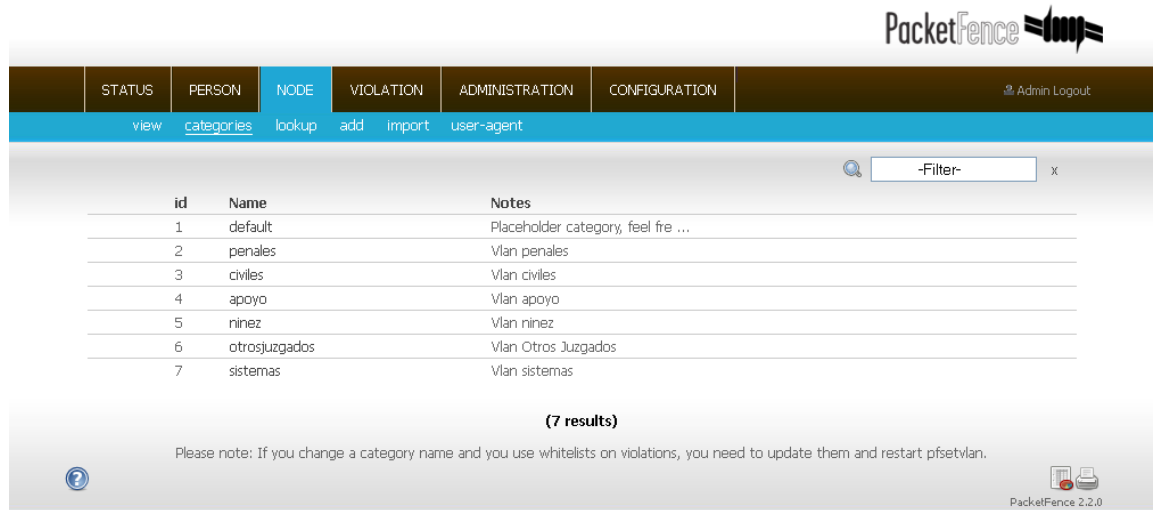


Figura IV.6: Categorías de dispositivos finales.

Las categorías fueron divididas de acuerdo a las Vlans a las que pertenecen; Las cuales son: penales, civiles, apoyo, ninez, otrosjuzgados, sistemas. De esta forma se puede asignar a un grupo y configurar automáticamente la Vlan a la que pertenece cada equipo.

Para editar las categorías se debe hacer click en una de ellas y aparece una opción en la parte izquierda de la selección para realizar esta operación.

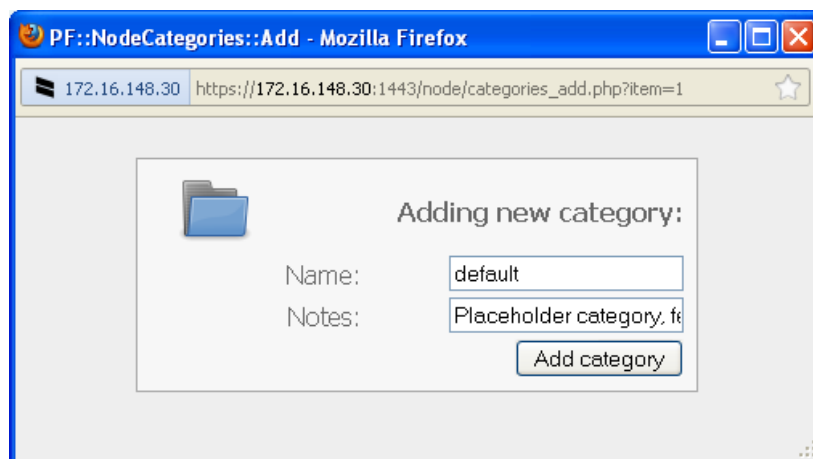


Figura IV.7: Edición de Categorías.

De la misma forma que se agrego las categorías se debe hacer click en una de ellas y aparece una opción en la parte izquierda de la selección para realizar esta operación.

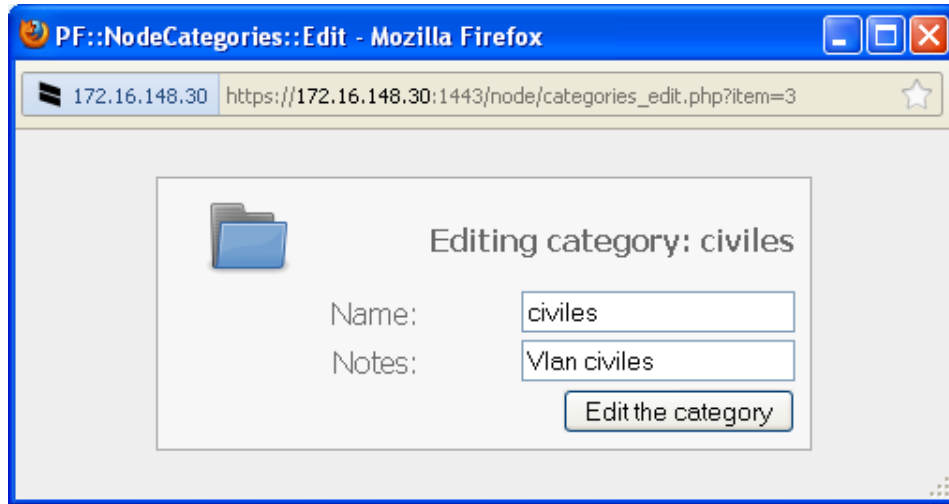


Figura IV.8: Edición de Categorías.

Se puede también eliminar las categorías que no se necesiten o estén mal configuradas de la misma manera que se agrego o edito las categorías; luego se da click en el botón aceptar para completar la operación.

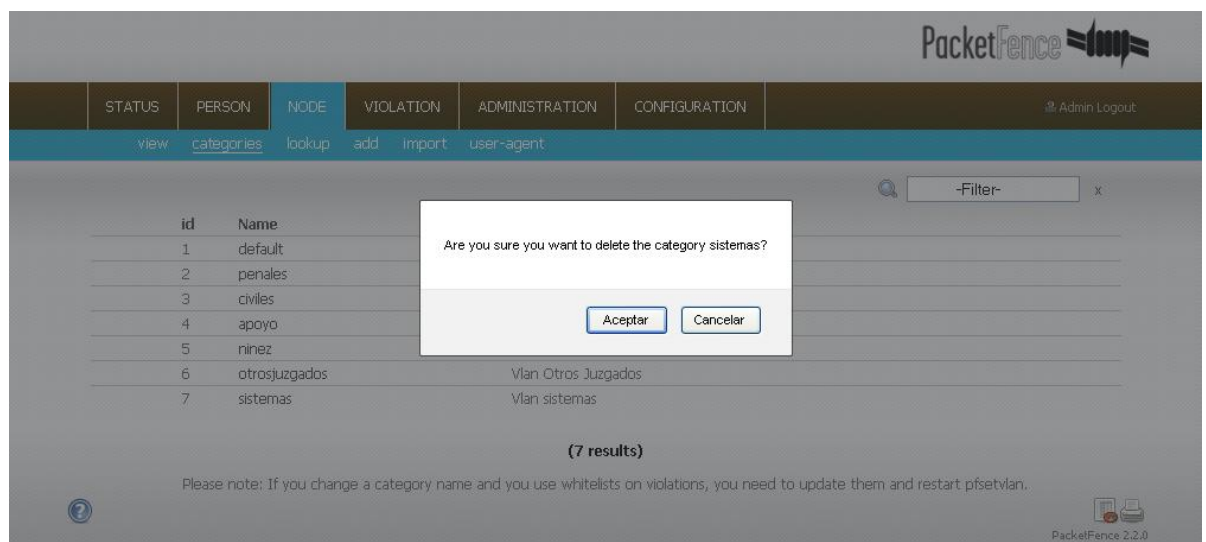


Figura IV.9: Eliminación de Categorías.

Podemos visualizar la información de cada dispositivo en la opción lookup; para esto debemos poner la dirección MAC del dispositivo que necesitamos detallar la información.

The screenshot shows the PacketFence web interface. At the top right is the PacketFence logo. Below it is a navigation bar with tabs: STATUS, PERSON, NODE, VIOLATION, ADMINISTRATION, CONFIGURATION, and Admin Logout. Under the NODE tab, there are sub-links: view, categories, lookup, add, import, and user-agent. The main content area features a 'Lookup a MAC' form with a text input field containing '00:22:15:f4:b2:2a' and a 'Lookup' button. Below the form, the system displays detailed information for the device with the following text:

```
MAC Address      : 00:22:15:f4:b2:2a
IP Address       : 172.16.144.237 (active)
IP Info          : IP active since 2012-02-19 11:11:24
Owner            : j.escobar
Category         : penales
Status           : registered
Name             : V2SecrPenal2
MAC Vendor       : ASUSTek COMPUTER INC.
VoIP             : no

NODE USER-AGENT INFORMATION
Raw User-Agent   : Mozilla 5.0 Windows; U; Windows NT 6.0; es-MX; rv:1.9.2.8 Gecko 20100722 Firefox 3.6.8 .NET CLR 3.5.30729
Browser          : Firefox
OS               : WinVista
Is a device?     : no
Is a mobile?     : no

NODE DHCP INFORMATION
OS               : Microsoft Windows Vista/7 or Server 2008
DHCP Info        : Last DHCP request at 2012-02-22 13:11:41
Location         : port 10011 (vlan 2) on switch 172.16.148.57
Connection type: Wired SNMP
802.1X Username :
Wireless SSID   :
Last activity    : UNKNOWN
```

At the bottom left of the interface is a help icon, and at the bottom right is the version number 'PacketFence 2.2.0'.

Figura IV.10: Visualización de información de los dispositivos.

Otra opción que tenemos en las opciones de dispositivos es la de agregar manualmente un dispositivo final. No es recomendable hacer esto, es mejor dejar que la herramienta detecte al dispositivo. Para esto se debe ingresar la dirección MAC del dispositivo, el id del usuario, la categoría y el estado.

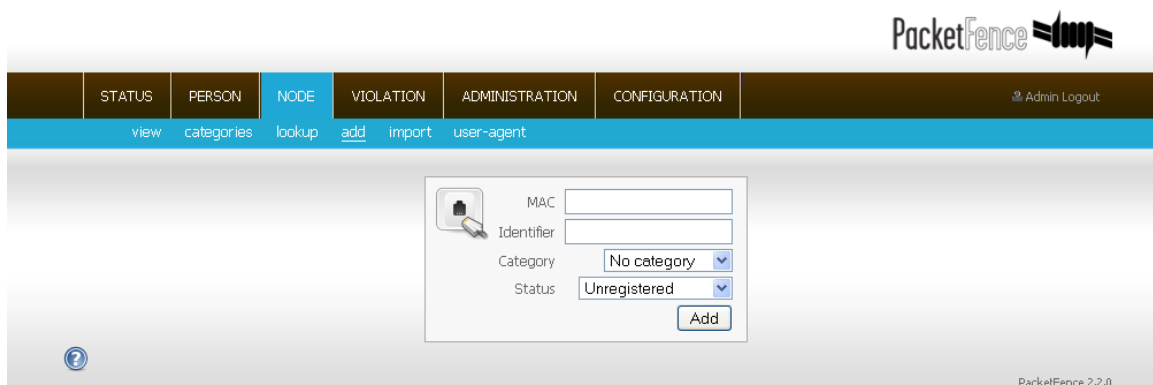


Figura IV.11: Agregación manual de los dispositivos.

La opción de user-agent nos permite observar que equipos se han conectado y con que navegador web fue con el que se registro.

The screenshot shows the PacketFence web interface with a table of devices. The table has the following columns:

- MAC
- Identified Browser
- Identified OS
- Device
- is a device
- is a mobile
- Raw User-Agent

 The table contains 20 rows of data. The 10th row is highlighted in blue. A search filter '-Filter-' is visible in the top right of the table area. The PacketFence logo is in the top right corner, and 'Admin Logout' is in the top right of the navigation bar. The version 'PacketFence 2.2.0' is visible in the bottom right corner.


MAC	Identified Browser	Identified OS	Device	is a device	is a mobile	Raw User-Agent
f0:4d:a2:4a:54:eb	Firefox	Win7		no	no	Mozilla 5.0 Windows NT 6.1; W ...
00:22:15:f4:b2:2a	Firefox	WinVista		no	no	Mozilla 5.0 Windows; U; Windo ...
00:0f:fe:ac:ef:17	Firefox	WinXP		no	no	Mozilla 5.0 Windows; U; Windo ...
00:16:17:7a:66:b7	Firefox	WinXP		no	no	Mozilla 5.0 Windows; U; Windo ...
00:10:dc:87:6f:91	Firefox	WinXP		no	no	Mozilla 5.0 Windows; U; Windo ...
00:19:db:ba:7a:ba	Firefox	WinXP		no	no	Mozilla 5.0 Windows; U; Windo ...
00:23:24:02:88:5c	Firefox	Win7		no	no	Mozilla 5.0 Windows; U; Windo ...
00:23:24:03:a3:7d	Firefox	Win7		no	no	Mozilla 5.0 Windows; U; Windo ...
00:0f:fe:05:62:bd	MSIE	WinXP		no	no	Mozilla 4.0 compatible; MSIE ...
00:23:24:02:87:79	Firefox	Win7		no	no	Mozilla 5.0 Windows; U; Windo ...
00:23:24:03:a4:42	Firefox	Win7		no	no	Mozilla 5.0 Windows NT 6.1; r ...
00:0f:fe:cf:c4:bd	Firefox	Win7		no	no	Mozilla 5.0 Windows NT 6.1; r ...
00:0f:fe:05:9e:a0	Firefox	WinXP		no	no	Mozilla 5.0 Windows; U; Windo ...
00:21:97:3d:08:a0	Firefox	WinXP		no	no	Mozilla 5.0 Windows; U; Windo ...
00:21:97:3d:07:8d	MSIE	WinXP		no	no	Mozilla 4.0 compatible; MSIE ...
00:21:97:3c:fd:99	Firefox	WinXP		no	no	Mozilla 5.0 Windows; U; Windo ...
00:21:97:3d:05:8b	Firefox	WinXP		no	no	Mozilla 5.0 Windows; U; Windo ...
00:19:db:c3:20:68	MSIE	WinXP		no	no	Mozilla/4.0 (compatible; MSIE ...
00:1c:c0:b8:51:1c	MSIE			no	no	Mozilla/4.0 (compatible; MSIE ...
00:0f:fe:ac:ee:ff	MSIE	WinXP		no	no	Mozilla/4.0 (compatible; MSIE ...

Figura IV.12: Visualización navegadores utilizados por los dispositivos finales.

Para Editar un dispositivo y pre configurar para el ingreso a la red lo hacemos seleccionando uno de estos, en la parte izquierda del dispositivo seleccionado

aparecen 3 opciones como observamos en la figura IV.9; para editar escogemos la primera opción.

148.30 https://172.16.148.30:1443/node/edit.php?item=00:0f:fe:ab:2d:7e

 Editing: 00:0f:fe:ab:2d:7e

Computer Name:

Identifier:


Category: ▼


Status: ▼

Bypass VLAN:

VoIP: ▼

Detect Date:

Reg Date: 

Unregdate: 

Last connection:

Last Switch:

Last Port:

Last VLAN:

Last SSID:

Last 802.1X Username:

User-Agent:

OS (dhcp):

Last Arp Time:

Last DHCP Time:

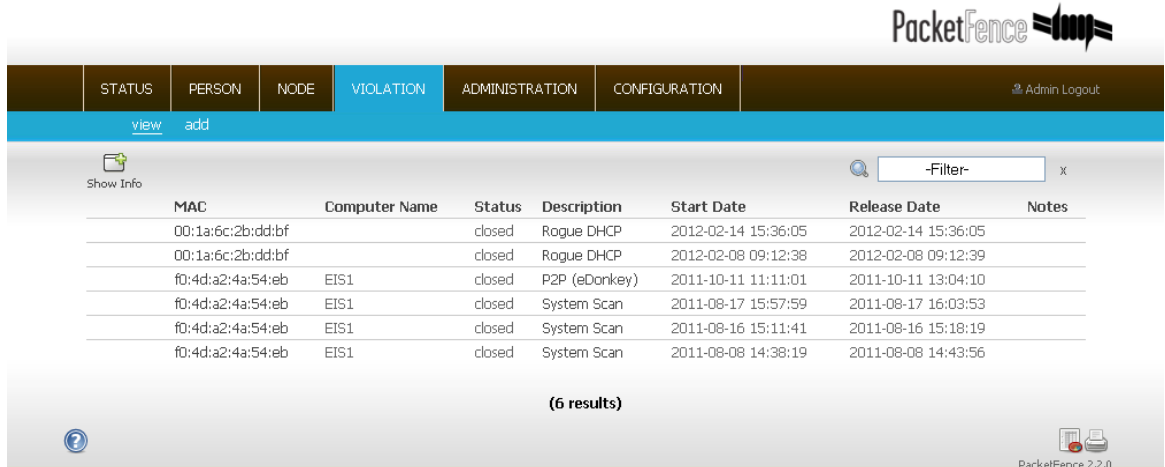
Lastskip:

Notes:

Figura IV.13: Página para la edición de dispositivos.

4.2.1.3 Administración de Violaciones

Las violaciones a las políticas de seguridad se pueden visualizar en la opción de Violation.



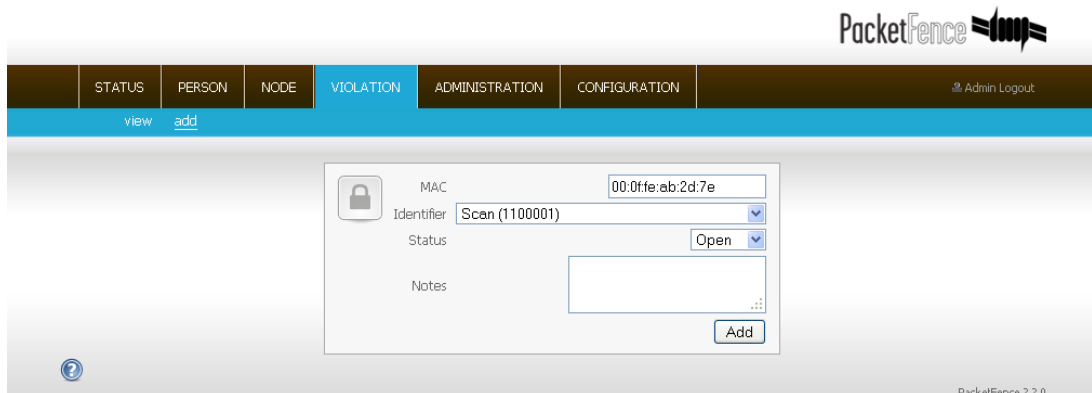
The screenshot shows the PacketFence web interface with the 'VIOLATION' tab selected. A table displays a list of violations with columns for MAC, Computer Name, Status, Description, Start Date, Release Date, and Notes. There are 6 results shown.

MAC	Computer Name	Status	Description	Start Date	Release Date	Notes
00:1a:6c:2b:dd:bf		closed	Rogue DHCP	2012-02-14 15:36:05	2012-02-14 15:36:05	
00:1a:6c:2b:dd:bf		closed	Rogue DHCP	2012-02-08 09:12:38	2012-02-08 09:12:39	
f0:4d:a2:4a:54:eb	EIS1	closed	P2P (eDonkey)	2011-10-11 11:11:01	2011-10-11 13:04:10	
f0:4d:a2:4a:54:eb	EIS1	closed	System Scan	2011-08-17 15:57:59	2011-08-17 16:03:53	
f0:4d:a2:4a:54:eb	EIS1	closed	System Scan	2011-08-16 15:11:41	2011-08-16 15:18:19	
f0:4d:a2:4a:54:eb	EIS1	closed	System Scan	2011-08-08 14:38:19	2011-08-08 14:43:56	

Figura IV.14: Interfaz principal de violaciones de seguridad.

Si el estado es open es decir abierto la violación de a las políticas de seguridad todavía persiste por el contrario si el estado es closed significa que la violación ha sido corregida.

Se puede configurar una violación de forma manual para algún dispositivo que la herramienta no haya podido detectar. Se debe poner en los campos la dirección MAC del dispositivo al cual queremos añadir la violación, la identificación de la violación, el estado de la violación y alguna nota aunque este campo no es obligatorio.



The screenshot shows the PacketFence web interface with the 'VIOLATION' tab selected. A form is displayed for adding a new violation. The form includes fields for MAC (00:0ffe:ab:2d:7e), Identifier (Scan (1100001)), Status (Open), and Notes. An 'Add' button is visible at the bottom right of the form.

Figura IV.15: Añadir violaciones de forma manual.

4.2.1.4 Administración de Servicios

PacketFence ofrece la administración de los servicios que maneja la herramienta a través de la interfaz haciéndonos más fácil la vida.

The screenshot displays the PacketFence web interface for service administration. The top navigation bar includes 'NODE', 'VIOLATION', 'ADMINISTRATION' (selected), and 'CONFIGURATION'. The main content area is titled 'Services' and contains a table with the following data:

Service	Expected Status	Actual Status	Action
pfdetect	Running	Running (pid: 13016)	Stop, Refresh
pfdhcpdlistener	Running	Running (pid: 13036 13034 13033 13032 13031 13030 13029 13028 13027 13026 13025 13024 13022 13021 13020 13019 13018)	Stop, Refresh
pfmon	Running	Running (pid: 13035)	Stop, Refresh
pfredirect	Stopped	Stopped	Start, Refresh
named	Running	Running (pid: 12852)	Stop, Refresh
dhcpcd	Running	Running (pid: 12882)	Stop, Refresh
pfsetvlan	Running	Running (pid: 13017)	Stop, Refresh
snmptrapd	Running	Running (pid: 12886)	Stop, Refresh
snort	Running	Running (pid: 13062)	Stop, Refresh
All Services			Stop

Below the table, a 'Configuration check-up' section shows a warning: 'WARNING - pfcmd needs setuid and setgid bit set to run properly. Fix with chmod ug+s pfcmd'.

Figura IV.16: Administración de Servicios.

En la figura IV.20 se puede visualizar los servicios administrados y el estado de los mismos.

Los servicios que maneja la herramienta se dividen en dos grupos; el primer grupo son los servicios propios de la herramienta los cuales son: pfdetect (Para detectar las violaciones), pfdhcpdlistener (Para detectar dispositivos finales y sus características), pfmon (Para la administración de la herramienta y tareas programadas) y pfredirect (Este se activa de acuerdo a las peticiones de las herramientas); El segundo grupo son los servicios complementarios a la herramienta como son named (Servidor DNS), dhcpcd (Servidor dhcp), pfsetvlan (Cuando se usa administración por Vlans que es el caso sirve para automáticamente cambiar las Vlans), snmptrapd (Captura las demandas snmp de los Switchs configurados) y snort (Para la detección de violaciones en la red).

4.2.1.5 Administración de Configuraciones

Se puede hacer cambios en las configuraciones directamente por la interfaz web. Para acceder a esta opción damos un click en Configuration. Como página principal de la opción de configuraciones muestra las configuraciones principales.

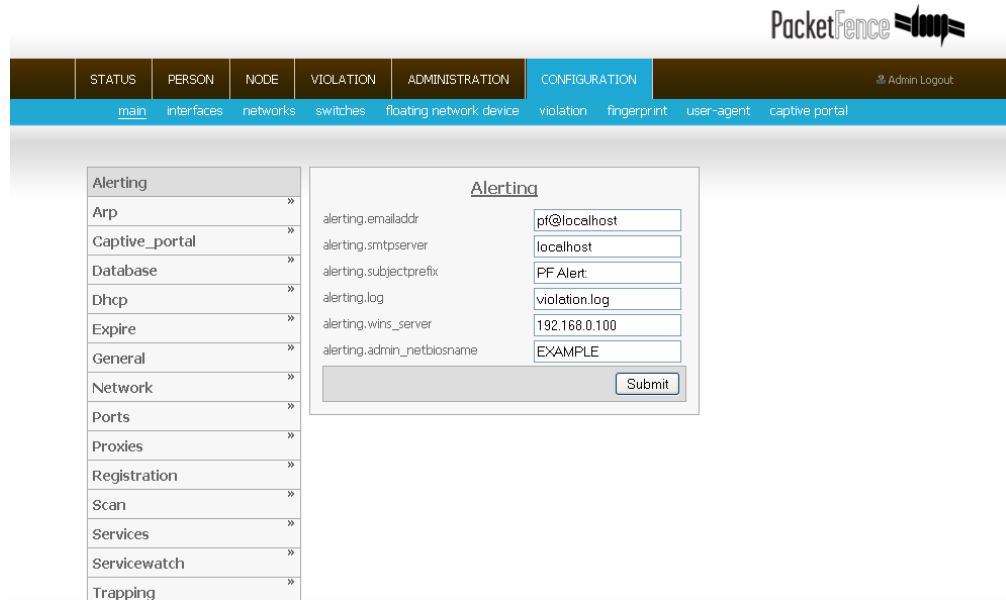


Figura IV.17: Configuraciones de Alertas.

La siguiente opción es la configuración ARP y los parámetros de búsqueda de equipos.

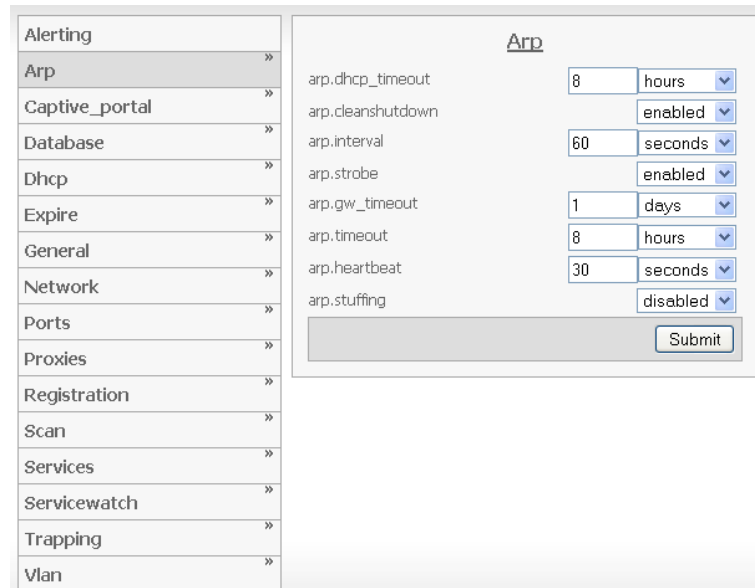


Figura IV.18: Configuraciones ARP.

Se puede configurar un portal captivo externo si el de la herramienta no funciona o deja de funcionar. Se dejo la dirección del portal captivo de la página oficial de PacketFence.

The screenshot shows the configuration page for the 'Captive portal' in PacketFence. On the left is a navigation menu with the following items: Alerting, Arp, Captive_portal (highlighted), Database, Dhcp, Expire, General, Network, Ports, Proxies, Registration, Scan, Services, Servicewatch, Trapping, and Vlan. The main content area is titled 'Captive portal' and contains a single configuration field: 'captive_portal.network_detection_ip' with the value '67.205.85.245'. A 'Submit' button is located at the bottom right of the configuration area.

Figura IV.19: Configuración de la dirección del Portal Captivo.

La siguiente configuración es la administración de la conexión a la base de datos.

The screenshot shows the configuration page for the 'Database' in PacketFence. On the left is a navigation menu with the following items: Alerting, Arp, Captive_portal, Database (highlighted), Dhcp, Expire, General, Network, Ports, Proxies, Registration, Scan, Services, Servicewatch, Trapping, and Vlan. The main content area is titled 'Database' and contains five configuration fields: 'database.pass' (masked with dots), 'database.db' (value 'pf'), 'database.user' (value 'pf'), 'database.port' (value '3306'), and 'database.host' (value 'localhost'). A 'Submit' button is located at the bottom right of the configuration area.

Figura IV.20: Configuración de la conexión a la Base de Datos.

Se puede configurar el servicio Dhcp con los parámetros de asignación de direcciones ip en la red de cuarentena y de registro.

Alerting	»
Arp	»
Captive_portal	»
Database	»
Dhcp	»
Expire	»
General	»
Network	»
Ports	»
Proxies	»
Registration	»
Scan	»
Services	»
Servicewatch	»
Trapping	»
Vlan	»

Dhcp

dhcp.isolation_lease 2 minutes

dhcp.unregistered_lease 2 minutes

dhcp.registered_lease 2 hours

Submit

Figura IV.21: Configuración del servicio DHCP.

La configuración de los parámetros de red son de cómo va ha funcionar la herramienta el intervalo de detección y las opciones de activar la detección y el registro de detecciones.

Alerting	»
Arp	»
Captive_portal	»
Database	»
Dhcp	»
Expire	»
General	»
Network	»
Ports	»
Proxies	»
Registration	»
Scan	»
Services	»
Servicewatch	»
Trapping	»
Vlan	»

Network

network.mode vlan

network.rogueinterval 10

network.dhcpdetector enabled

network.dhcpoption82logger disabled

Submit

Figura IV.22: Configuración de parámetros de red.

Con la configuración de puertos se puede administrar cuales son los puertos que se van a re direccionar al portal captivo, cuales se van a escuchar por violaciones de seguridad y el puerto con el que se va administrar la herramienta por interfaz web.

Alerting	»
Arp	»
Captive_portal	»
Database	»
Dhcp	»
Expire	»
General	»
Network	»
Ports	»
Proxies	»
Registration	»
Scan	»
Services	»
Servicewatch	»
Trapping	»
Vlan	»

Ports

ports.redirect: 80/tcp,110/tcp,143/tcp

ports.listeners: imap, pop3

ports.admin: 1443

Figura IV.23: Configuración de puertos de Red.

La herramienta ofrece una solución de McAfee para resolver los problemas con detecciones de virus y esto se configura como se muestra en la siguiente figura.

Alerting	»
Arp	»
Captive_portal	»
Database	»
Dhcp	»
Expire	»
General	»
Network	»
Ports	»
Proxies	»
Registration	»
Scan	»
Services	»
Servicewatch	»
Trapping	»
Vlan	»

Proxies

proxies.tools/stinger.exe: http://download.nai.com

Figura IV.24: Configuración de dirección de antivirus.

Las configuraciones principales del registro son: el rango en el cual se va a trabajar, si se desea saltarse el registro, el tipo de autenticación, se deshabilito la expiración del registro y se configuro el texto del botón de registro.

Alerting	»
Arp	»
Captive_portal	»
Database	»
Dhcp	»
Expire	»
General	»
Network	»
Ports	»
Proxies	»
Registration	»
Scan	»
Services	»
Servicewatch	»
Trapping	»
Vlan	»

Registration

registration.range: 172.16.144.0/20

registration.skip_mode: disabled

registration.skip_deadline: Mon Nov 12 12:00:00 ES

registration.skip_window: 14 days

registration.skip_reminder: 1 days

registration.auth: email, local, ldap, radius

registration.expire_mode: disabled

registration.expire_deadline: Mon Nov 12 12:00:00 ES

registration.expire_window: 52 weeks

registration.expire_session: 5 minutes

registration.maxnodes: 0

registration.button_text: Registrar

registration.nbregpages: 1

Submit

Figura IV.25: Configuración de las opciones de registro.

Para realizar las configuraciones del escaneo pre registro se debe configurar las conexiones a la herramienta Nessus y cuál es la política que se va ha utilizar para el escaneo.

Alerting	»
Arp	»
Captive_portal	»
Database	»
Dhcp	»
Expire	»
General	»
Network	»
Ports	»
Proxies	»
Registration	»
Scan	»
Services	»
Servicewatch	»
Trapping	»
Vlan	»

Scan

scan.ssl: enabled

scan.pass:

scan.user: admin

scan.port: 1241

scan.host: 127.0.0.1

scan.registration: disabled

scan.live_tids: 54615

scan.nessusclient_file: remotescan.nessus

scan.nessusclient_policy: RemoteScan

scan.duration: 60 seconds

Submit

Figura IV.26: Configuración de las opciones de Escaneo.

La ubicación de los servicios pueden ser también configurados para el correcto funcionamiento de la herramienta.

Alerting	»
Arp	»
Captive_portal	»
Database	»
Dhcp	»
Expire	»
General	»
Network	»
Ports	»
Proxies	»
Registration	»
Scan	»
Services	»
Servicewatch	»
Trapping	»
Vlan	»

Services	
services.snort	<input type="text" value="/usr/sbin/snort"/>
services.httptd	<input type="text" value="/usr/sbin/httptd"/>
services.dhcpd	<input type="text" value="/usr/sbin/dhcpd"/>
services.named	<input type="text" value="/usr/sbin/named"/>
services.snmptrapd	<input type="text" value="/usr/sbin/snmptrapd"/>
<input type="button" value="Submit"/>	

Figura IV.27: Configuración de ubicaciones de servicios.

El servicio de vigilancia puede ser activado para el envío de alertas al correo electrónico.

Alerting	»
Arp	»
Captive_portal	»
Database	»
Dhcp	»
Expire	»
General	»
Network	»
Ports	»
Proxies	»
Registration	»
Scan	»
Services	»
Servicewatch	»
Trapping	»
Vlan	»

Servicewatch	
servicewatch.email	<input type="text" value="enabled"/>
servicewatch.restart	<input type="text" value="disabled"/>
<input type="button" value="Submit"/>	

Figura IV.28: Configuración del servicio de vigilancia.

La configuración de de captura de dispositivos puede ser habilitada para vigilar la red en un modo estricto, se define el rango, los registros, se puede bloquear o no la captura de dispositivos. También se puede redireccionar a una página después de la captura de datos.

The screenshot shows the 'Trapping' configuration page. On the left is a sidebar menu with options: Alerting, Arp, Captive_portal, Database, Dhcp, Expire, General, Network, Ports, Proxies, Registration, Scan, Services, Servicewatch, Trapping (selected), and Vlan. The main content area is titled 'Trapping' and contains the following settings:

- trapping.testing: disabled
- trapping.range: 172.16.144.0/20
- trapping.registration: enabled
- trapping.immediate: enabled
- trapping.redirecttimer: 20 seconds
- trapping.passthrough: disabled
- trapping.blacklist: (empty text area)
- trapping.whitelist: (empty text area)
- trapping.redirecturl: http://www.google.com.ec
- trapping.always_use_redirecturl: disabled
- trapping.detection: enabled

A 'Submit' button is located at the bottom right of the configuration area.

Figura IV.29: Configuración del servicio de captura de dispositivos.

El ajuste de las configuraciones de las Vlans se puede hacer a través de esta opción. Se ajusta el script para la administración de las Vlans y los servicios.

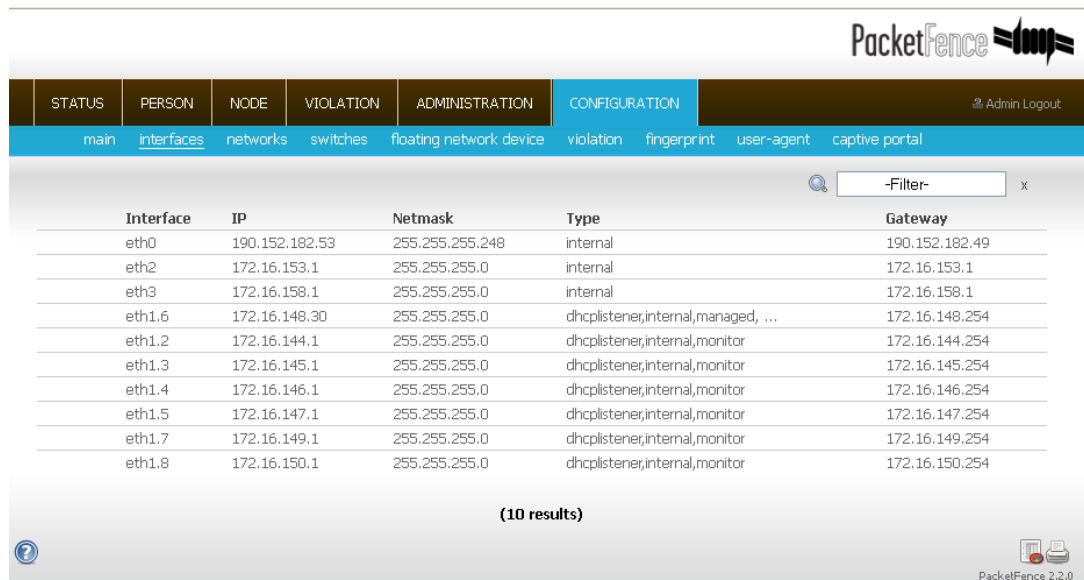
The screenshot shows the 'Vlan' configuration page. On the left is a sidebar menu with options: Alerting, Arp, Captive_portal, Database, Dhcp, Expire, General, Network, Ports, Proxies, Registration, Scan, Services, Servicewatch, Trapping, and Vlan (selected). The main content area is titled 'Vlan' and contains the following settings:

- vlan.adjustswitchportvlanreasons: node_modify, manage_register, manage_deregister, manage_vcloses
- vlan.adjustswitchportvlangscript: flip.pl
- vlan.closelocationlogonstop: disabled
- vlan.dhcpd: enabled
- vlan.named: enabled
- vlan.nbtraphandlerthreads: 20
- vlan.nbtrapparserthreads: 5
- vlan.bounce_duration: 4 seconds

A 'Submit' button is located at the bottom right of the configuration area.

Figura IV.30: Configuración de la administración de Vlans.

La configuración de las interfaces puede ser automáticamente hecha por las herramientas o agregando de forma manual las interfaces. En la figura IV.35 se puede observar las configuraciones de las interfaces que se aplico en la implementación de la herramienta.



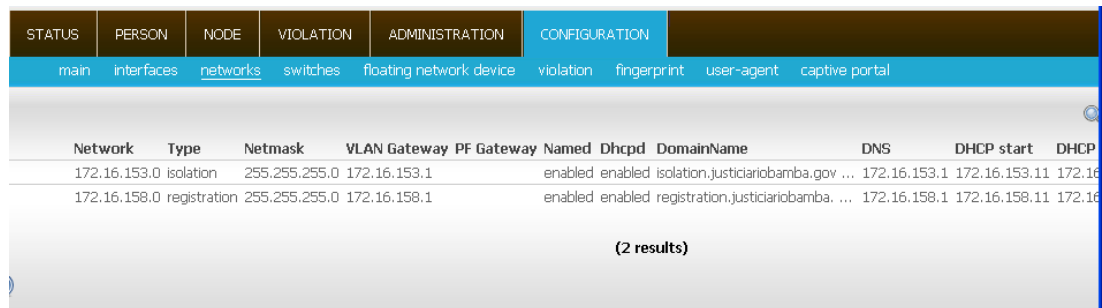
The screenshot shows the PacketFence web interface. The top navigation bar includes 'STATUS', 'PERSON', 'NODE', 'VIOLATION', 'ADMINISTRATION', and 'CONFIGURATION'. The 'CONFIGURATION' menu is expanded to show 'main', 'interfaces', 'networks', 'switches', 'floating network device', 'violation', 'fingerprint', 'user-agent', and 'captive portal'. The 'interfaces' sub-menu is selected. A search filter is set to '-Filter-'. The main content area displays a table with 10 results for network interfaces.

Interface	IP	Netmask	Type	Gateway
eth0	190.152.182.53	255.255.255.248	internal	190.152.182.49
eth2	172.16.153.1	255.255.255.0	internal	172.16.153.1
eth3	172.16.158.1	255.255.255.0	internal	172.16.158.1
eth1.6	172.16.148.30	255.255.255.0	dhcplistener;internal,managed, ...	172.16.148.254
eth1.2	172.16.144.1	255.255.255.0	dhcplistener;internal,monitor	172.16.144.254
eth1.3	172.16.145.1	255.255.255.0	dhcplistener;internal,monitor	172.16.145.254
eth1.4	172.16.146.1	255.255.255.0	dhcplistener;internal,monitor	172.16.146.254
eth1.5	172.16.147.1	255.255.255.0	dhcplistener;internal,monitor	172.16.147.254
eth1.7	172.16.149.1	255.255.255.0	dhcplistener;internal,monitor	172.16.149.254
eth1.8	172.16.150.1	255.255.255.0	dhcplistener;internal,monitor	172.16.150.254

(10 results)

Figura IV.31: Configuración de las interfaces de red.

Para agregar las configuraciones de las redes de cuarentena y registro se realiza la agregación de estas y sus parámetros como se muestra en la siguiente figura.



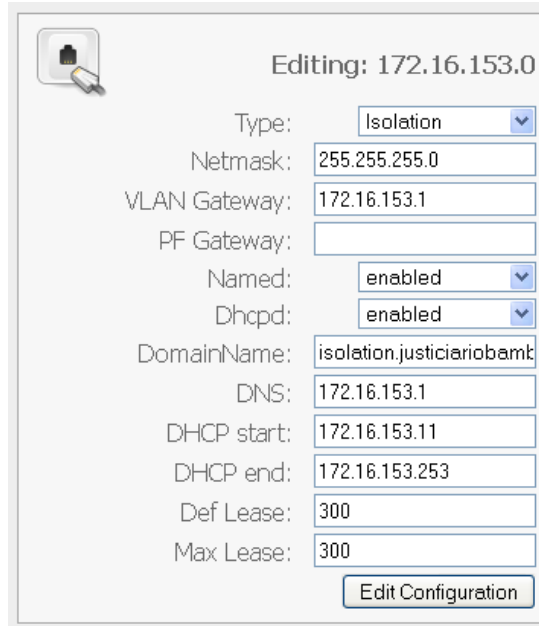
The screenshot shows the PacketFence web interface with the 'networks' sub-menu selected. A search filter is set to '-Filter-'. The main content area displays a table with 2 results for network configurations.

Network	Type	Netmask	VLAN Gateway	Pf Gateway	Named	Dhcpd	DomainName	DNS	DHCP start	DHCP
172.16.153.0	isolation	255.255.255.0	172.16.153.1		enabled	enabled	isolation.justiciariobamba.gov ...	172.16.153.1	172.16.153.11	172.16.153.11
172.16.158.0	registration	255.255.255.0	172.16.158.1		enabled	enabled	registration.justiciariobamba. ...	172.16.158.1	172.16.158.11	172.16.158.11

(2 results)

Figura IV.32: Configuración de redes de cuarentena y registro.

Para la edición de las redes lo que se debe hacer es seleccionar una de estas y presionar en el botón de edición y podremos cambiar los parámetros de las redes de violación y registro.

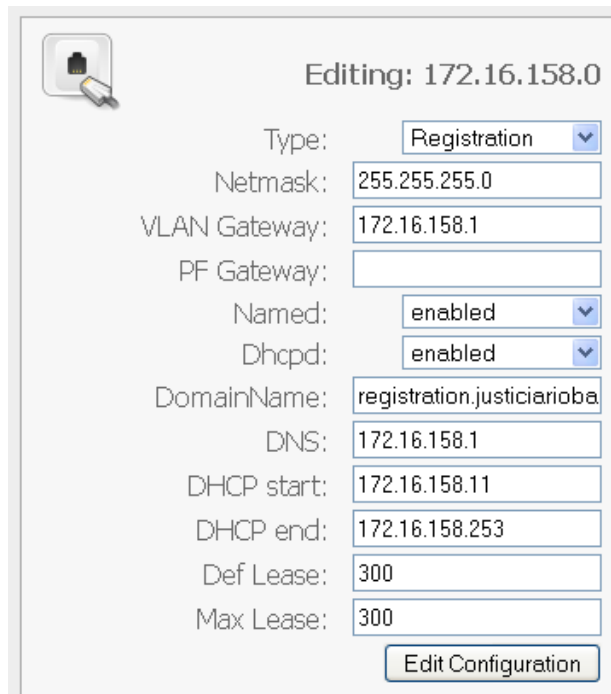


The screenshot shows a network configuration window titled "Editing: 172.16.153.0". It contains the following fields and values:

Type:	Isolation
Netmask:	255.255.255.0
VLAN Gateway:	172.16.153.1
PF Gateway:	
Named:	enabled
Dhcpd:	enabled
DomainName:	isolation.justiciariobank
DNS:	172.16.153.1
DHCP start:	172.16.153.11
DHCP end:	172.16.153.253
Def Lease:	300
Max Lease:	300

An "Edit Configuration" button is located at the bottom right of the form.

Figura IV.33: Edición de configuración de la red de cuarentena.



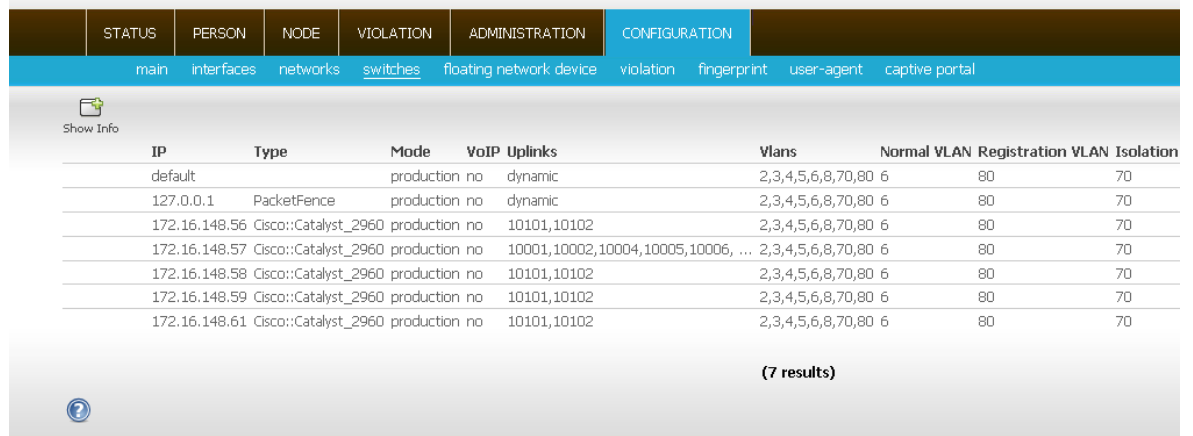
The screenshot shows a network configuration window titled "Editing: 172.16.158.0". It contains the following fields and values:

Type:	Registration
Netmask:	255.255.255.0
VLAN Gateway:	172.16.158.1
PF Gateway:	
Named:	enabled
Dhcpd:	enabled
DomainName:	registration.justiciarioba
DNS:	172.16.158.1
DHCP start:	172.16.158.11
DHCP end:	172.16.158.253
Def Lease:	300
Max Lease:	300

An "Edit Configuration" button is located at the bottom right of the form.

Figura IV.34: Edición de configuración de la red de registro.

A los Switchs hay que configurar algunas opciones para que funcione correctamente la herramienta. Para esto accedemos a la opción de Switchs.



The screenshot shows a web-based configuration interface for switches. The top navigation bar includes tabs for STATUS, PERSON, NODE, VIOLATION, ADMINISTRATION, and CONFIGURATION. Under CONFIGURATION, there are sub-tabs for main, interfaces, networks, switches, floating network device, violation, fingerprint, user-agent, and captive portal. The 'switches' sub-tab is active. Below the navigation is a 'Show Info' button and a table with the following columns: IP, Type, Mode, VoIP, Uplinks, Vlans, Normal VLAN, Registration VLAN, and Isolation. The table contains 7 rows of configuration data.

IP	Type	Mode	VoIP	Uplinks	Vlans	Normal VLAN	Registration VLAN	Isolation
default		production	no	dynamic	2,3,4,5,6,8,70,80	6	80	70
127.0.0.1	PacketFence	production	no	dynamic	2,3,4,5,6,8,70,80	6	80	70
172.16.148.56	Cisco::Catalyst_2960	production	no	10101,10102	2,3,4,5,6,8,70,80	6	80	70
172.16.148.57	Cisco::Catalyst_2960	production	no	10001,10002,10004,10005,10006, ...	2,3,4,5,6,8,70,80	6	80	70
172.16.148.58	Cisco::Catalyst_2960	production	no	10101,10102	2,3,4,5,6,8,70,80	6	80	70
172.16.148.59	Cisco::Catalyst_2960	production	no	10101,10102	2,3,4,5,6,8,70,80	6	80	70
172.16.148.61	Cisco::Catalyst_2960	production	no	10101,10102	2,3,4,5,6,8,70,80	6	80	70

(7 results)

Figura IV.35: Interfaz principal de configuración de switchs.

Al igual que en las anteriores configuraciones para editar los atributos de los Switch's debemos seleccionar uno de estos y configurar los diferentes parámetros de estos.

Los principales parámetros son: El tipo de dispositivo, el modo en que operara para que entre en completa operación la opción es production, si es que el dispositivo maneja voz ip, uplinks es la opción para no tomar en cuenta las interfaces se toma los índices snmp que muestra el Switch para identificar las interfaces de red, también se configura las Vlans que van a servir para el funcionamiento de la herramienta para esto configuramos las Vlans que se utilizaran y que han sido ya creadas previamente por la institución para el funcionamiento de la red;

Otros parámetros son la configuración de las diferentes Vlans como son: normal, registro, violación, detección de mac, invitados, las Vlans por defecto que se van a utilizar.

Una opción importante es la configuración de los parámetros de conectividad de la herramienta con el Switch como son: tipo, contraseña vty, contraseña enable, versión y la comunidad SNMP que se va a utilizar.

The image shows a configuration interface for a switch, titled "Editing: 172.16.148.56". The interface is divided into two main sections. The top section contains general switch configuration options, and the bottom section contains SNMP-related settings.

Type:	Cisco Catalyst 2960
Mode:	production
VoIP:	No
Uplinks:	10101, 10102
Vlans:	2, 3, 4, 5, 6, 8, 70, 80
Normal VLAN:	6
Registration VLAN:	80
Isolation VLAN:	70
MAC Detect VLAN:	4
Guest VLAN:	80
Voice VLAN:	
Custom VLAN 1:	2
Custom VLAN 2:	3
Custom VLAN 3:	4
Custom VLAN 4:	5
Custom VLAN 5:	8
CLI Transport:	Telnet
CLI User:	
SNMP Trap Community:	nac
SNMP Username Trap:	
SNMP AuthProto Trap:	
SNMP AuthPass Trap:	
SNMP PrivProto Trap:	
SNMP PrivPass Trap:	
SNMP Version:	2c
SNMP Read Community:	nac
SNMP Write Community:	nac
SNMP Engine ID:	
SNMP Username Read:	
SNMP AuthProto Read:	
SNMP AuthPass Read:	
SNMP PrivProto Read:	
SNMP PrivPass Read:	
SNMP Username Write:	
SNMP AuthProto Write:	
SNMP AuthPass Write:	
SNMP PrivProto Write:	
SNMP PrivPass Write:	
MAC Searches Max:	50
MAC Searches Sleep:	2

At the bottom right of the form, there is a button labeled "Edit Configuration".

Figura IV.36: Interfaz principal de configuración de switches.

PacketFence ofrece la posibilidad de tener dispositivos móviles o inalámbricos dentro de la red. En nuestro caso no se necesita esta opción debido a que la institución no posee red LAN inalámbrica.

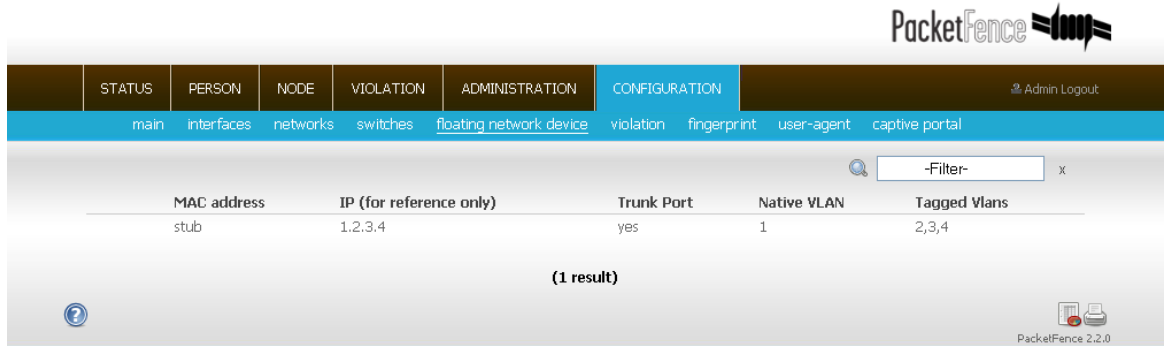


Figura IV.37: Configuración de dispositivos de acceso móvil.

Una de las principales configuraciones son las políticas de post ingreso a la red. Estas políticas son las que se van a utilizar en la herramienta SNORT estas vienen ya predefinidas por la herramienta pero se puede adaptar a las necesidades de la institución. La mayoría de estas políticas fueron aplicadas a la institución. Si necesitamos añadir políticas nuevas se debe hacer desde esta interfaz ya que si se usa la herramienta SNORT y su propia configuración no funcionara.

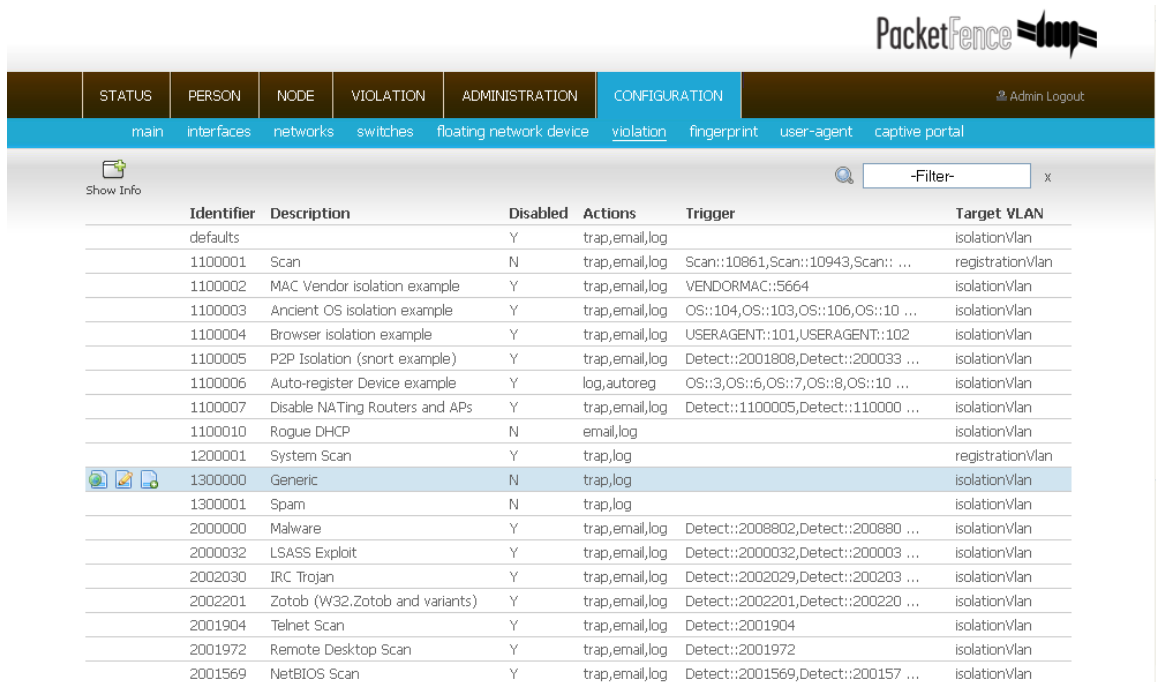


Figura IV.38: Configuración de políticas de seguridad.

La opción fingerprint se utiliza para actualizar las firmas de los sistemas operativos de muchos dispositivos finales y así poder detectar hasta el último que haya salido al mercado.

ID	OS Class ID	OS Class	Operating System	Fingerprint
100	1	Windows	Microsoft Windows XP	15,3,6,44,46,47,31,33,249,43,2 ...
105	1	Windows	Microsoft Windows NT 4	1,15,3,44,46,47,6
100	1	Windows	Microsoft Windows XP	15,3,6,44,46,47,31,33,249,43,2 ...
100	1	Windows	Microsoft Windows XP	28,2,3,15,6,12,44,47
105	1	Windows	Microsoft Windows NT 4	1,2,3,6,12,15,26,28,85,86,87,8 ...
101	1	Windows	Microsoft Windows 2000	1,15,3,6,44,46,47,31,33,43
101	1	Windows	Microsoft Windows 2000	1,15,3,6,44,46,47,31,33,43,252
106	1	Windows	Microsoft Windows 98SE	1,15,3,6,44,46,47,43,77
101	1	Windows	Microsoft Windows 2000	1,15,3,6,44,46,47,31,33,43,252 ...
101	1	Windows	Microsoft Windows 2000	15,3,6,44,46,47,31,33,43
106	1	Windows	Microsoft Windows 98SE	1,15,3,6,44,46,47,43,77,252
101	1	Windows	Microsoft Windows 2000	15,3,6,44,46,47,31,33,43,252
102	1	Windows	Microsoft Windows ME	1,15,3,6,44,46,47,31,33,43,77
106	1	Windows	Microsoft Windows 98SE	15,3,6,44,46,47,43,77
102	1	Windows	Microsoft Windows ME	15,3,6,44,46,47,31,33,43,77
106	1	Windows	Microsoft Windows 98SE	15,3,6,44,46,47,43,77,252

Figura IV.39: Actualización de firmas de sistemas operativos.

La opción user-agent en realidad no es una configuración estos vienen predefinidos por la herramienta y no son administrables. Los agentes de usuarios son los navegadores web reconocidos por la herramienta para el portal captivo.

ID	Property	Description
1	mosaic	
2	netscape	
3	firefox	
4	chrome	
5	safari	
6	ie	
7	opera	
8	lynx	
9	links	
10	elinks	
11	neoplanet	
12	neoplanet2	
13	avantgo	
14	emacs	
15	mozilla	
16	konqueror	
17	r1	

Figura IV.40: Interfaz de agentes de usuario.

La última opción de la administración de configuraciones es la edición de las plantillas para el portal captivo.

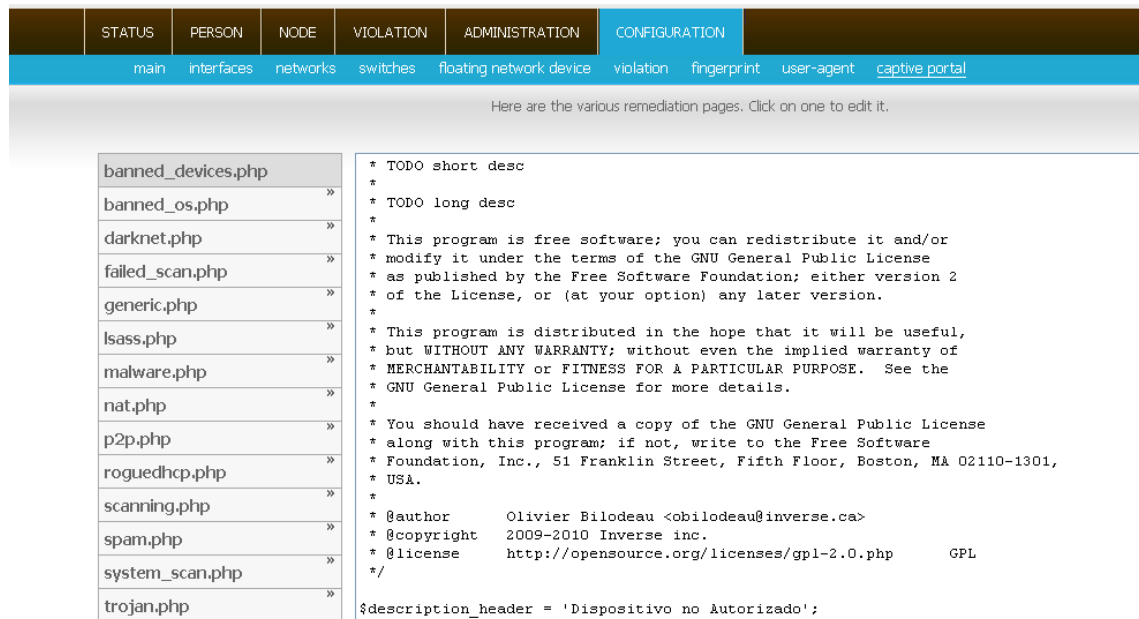


Figura IV.41: Configuración de plantillas del portal captivo.

4.2.1.6 Reportes

Para acceder a los reportes se ingresa por la opción status y luego en reports. En la pantalla principal se puede ver varias opciones de reportes, estos pueden ser estáticos o dinámicos.

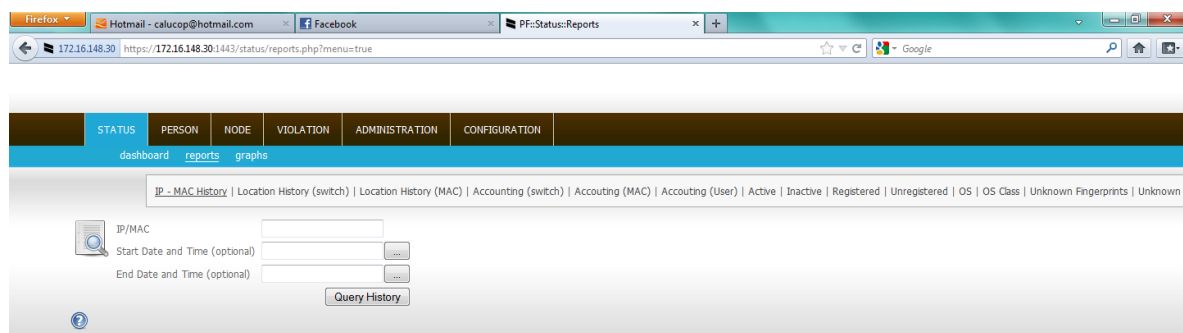


Figura IV.42: Pantalla principal de reportes.

El de los reportes es la historia de la dirección MAC y las direcciones IP's asignadas al equipo.

MAC	IP	Start Time
f0:4d:a2:4a:54:eb	172.16.148.120	2011-12-20 10:...
f0:4d:a2:4a:54:eb	172.16.148.120	2011-12-20 10:...
6c:62:6d:b0:9a:50	172.16.148.120	2011-09-23 15:...
6c:62:6d:b0:9a:50	172.16.148.120	2011-09-23 15:...
6c:62:6d:b0:9a:50	172.16.148.120	2011-09-19 07:...
6c:62:6d:b0:9a:50	172.16.148.120	2011-09-12 08:...
6c:62:6d:b0:9a:50	172.16.148.120	2011-09-12 08:...
6c:62:6d:b0:9a:50	172.16.148.120	2011-09-04 08:...
6c:62:6d:b0:9a:50	172.16.148.120	2011-08-31 18:...
6c:62:6d:b0:9a:50	172.16.148.120	2011-08-31 18:...
6c:62:6d:b0:9a:50	172.16.148.120	2011-08-30 18:...

Figura IV.43: Reporte de direcciones IP's asignadas a una dirección MAC.

El reporte de la historia de localización de una dirección se muestra de la siguiente forma. En esta podemos ver cuales son los Switchs a los que se ha conectado y a que interfaz.

MAC	Switch	ifIndex	VLAN	Type of connection	802.1X
f0:4d:a2:4a:54:eb	172.16.148.57	10027	5	Wired SNMP	
f0:4d:a2:4a:54:eb	172.16.148.57	10027	6	Wired SNMP	
f0:4d:a2:4a:54:eb	172.16.148.57	10027	5	Wired SNMP	
f0:4d:a2:4a:54:eb	172.16.148.57	10027	6	Wired SNMP	
f0:4d:a2:4a:54:eb	172.16.148.57	10027	5	Wired SNMP	
f0:4d:a2:4a:54:eb	172.16.148.57	10027	6	Wired SNMP	
f0:4d:a2:4a:54:eb	172.16.148.57	10027	5	Wired SNMP	
f0:4d:a2:4a:54:eb	172.16.148.57	10027	80	Wired SNMP	
f0:4d:a2:4a:54:eb	172.16.148.57	10027	5	Wired SNMP	
f0:4d:a2:4a:54:eb	172.16.148.57	10027	6	Wired SNMP	
f0:4d:a2:4a:54:eb	172.16.148.57	10027	6	Wired SNMP	
f0:4d:a2:4a:54:eb	172.16.148.57	10027	6	Wired SNMP	

Figura IV.44: Reporte de localización de un equipo por dirección MAC.

Podemos ver un reporte de los dispositivos activos dentro de la red LAN. Ingresando a la opción Active.

MAC	IP	Identifier	Regdate	Unregdate	Last Skip	Status	User Agent	Computer
00:0f:fe:05:62:bd	172.16.145.192	f.garzon	2011-10-26 09:47:00			reg	Mozilla 4.0 compatible; MSIE ...	V3Aux
00:0f:fe:05:62:bd	172.16.145.192	f.garzon	2011-10-26 09:47:00			reg	Mozilla 4.0 compatible; MSIE ...	V3Aux
00:0f:fe:33:88:22	172.16.144.200	1	2012-02-22 13:54:14			reg		V2Voc
00:0f:fe:ab:2d:7e	172.16.144.192	1	2012-02-22 13:54:40			reg		V2Aux
00:0f:fe:ab:2d:7e	172.16.144.192	1	2012-02-22 13:54:40			reg		V2Aux
00:0f:fe:ac:ef:17	172.16.144.249	r.fonseca	2011-12-20 14:50:23			reg	Mozilla 5.0 Windows; U; Windo ...	V2Aux
00:0f:fe:ac:ef:17	172.16.144.249	r.fonseca	2011-12-20 14:50:23			reg	Mozilla 5.0 Windows; U; Windo ...	V2Aux
00:0f:fe:cf:c4:bd	172.16.145.225	j.coello	2011-10-25 14:36:56			reg	Mozilla 5.0 Windows NT 6.1; r ...	V3SEC
00:19:db:ba:7a:ba	172.16.145.252	j.castillo	2011-10-26 11:17:29			reg	Mozilla 5.0 Windows; U; Windo ...	V3Juez
00:21:97:3d:05:8b	172.16.145.237	a.fiallos	2011-10-25 13:41:02			reg	Mozilla 5.0 Windows; U; Windo ...	v3aux1
00:21:97:3d:05:8b	172.16.145.237	a.fiallos	2011-10-25 13:41:02			reg	Mozilla 5.0 Windows; U; Windo ...	v3aux1
00:21:97:3d:07:8d	172.16.145.239	b.arellano	2011-10-25 13:59:28			reg	Mozilla 4.0 compatible; MSIE ...	V3Juez
00:21:97:3d:08:a0	172.16.145.196	o.jara	2011-10-25 14:06:27			reg	Mozilla 5.0 Windows; U; Windo ...	V3Sec
00:21:97:3d:08:a0	172.16.145.196	o.jara	2011-10-25 14:06:27			reg	Mozilla 5.0 Windows; U; Windo ...	V3Sec
00:22:15:f4:b2:2a	172.16.144.237	j.escobar	2011-12-20 15:06:36			reg	Mozilla 5.0 Windows; U; Windo ...	V2Sec
00:23:24:02:87:79	172.16.145.234	f.garzon	2011-10-26 09:23:25			reg	Mozilla 5.0 Windows; U; Windo ...	V3SEC

Figura IV.45: Reporte de dispositivos activos.

Se puede también generar un reporte de dispositivos inactivos.

MAC	IP	Identifier	Regdate	Unregdate	Last Skip	Status	User Agent	Computer
00:0f:1f:d1:7f:bf	1		2012-02-22 13:28:51			reg		erover-02E
00:0f:fe:05:9e:a0		j.coello	2011-10-25 14:26:55			reg	Mozilla 5.0 Windows; U; Windo ...	V3AUX3AC
00:10:dc:87:6f:91		sp.practicante	2011-12-20 14:13:48			reg	Mozilla 5.0 Windows; U; Windo ...	V2Aux3Pe
00:16:17:7a:66:b7		n.velastegui	2011-12-20 14:41:22			reg	Mozilla 5.0 Windows; U; Windo ...	V2Aux4Pe
00:21:97:3c:fd:99		v.jara	2011-10-25 13:51:47			reg	Mozilla 5.0 Windows; U; Windo ...	V3Aux2Ni
f0:4d:a2:4a:54:eb		carlos	2012-02-16 08:34:45			reg	Mozilla 5.0 Windows NT 6.1; W ...	EIS1
00:00:aa:c0:98:a9	1		2011-10-11 15:47:22			unreg		
00:03:d6:01:5f:c4	1					unreg		XT1000_C
00:0c:29:08:9f:2b	1					unreg		
00:0c:29:34:24:81	1					unreg		wxp-d92a
00:0c:29:5e:99:f3	1					unreg		pc
00:0c:29:68:05:67	1					unreg		pc
00:0c:29:c5:2c:af	1					unreg		
00:0c:29:da:7d:bf	1					unreg		pc
00:0c:29:db:de:46	1					unreg		
00:0c:29:ef:66:81	1					unreg		

Figura IV.46: Reporte de dispositivos inactivos.

Se puede generar el reporte del tipo de conexiones que existen. Aunque en nuestro caso este no aporta con mucha información debido a que toda la infraestructura es cableada.

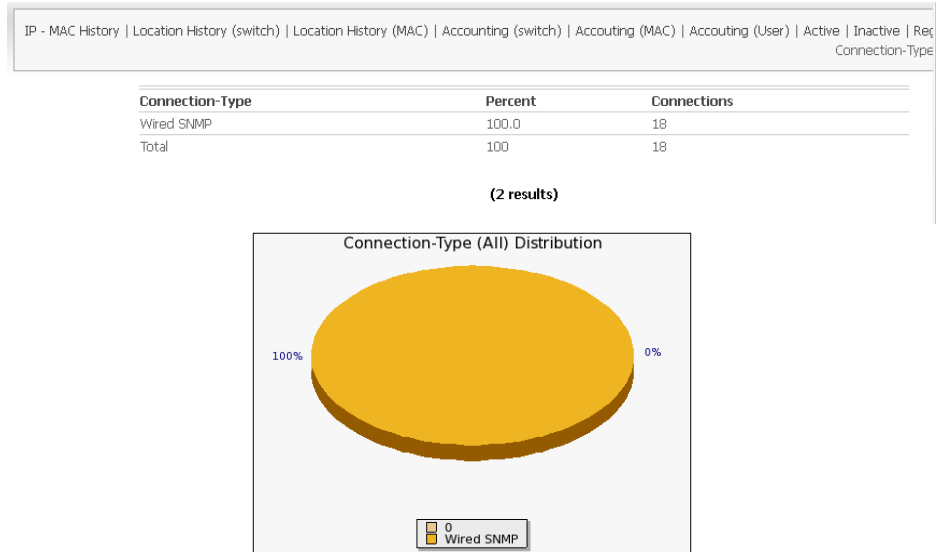


Figura IV.47: Reporte de tipo de conexiones.

4.2.1.7 Gráficos

PacketFence también genera gráficos estadísticos del estado de la herramienta y los dispositivos de la red.

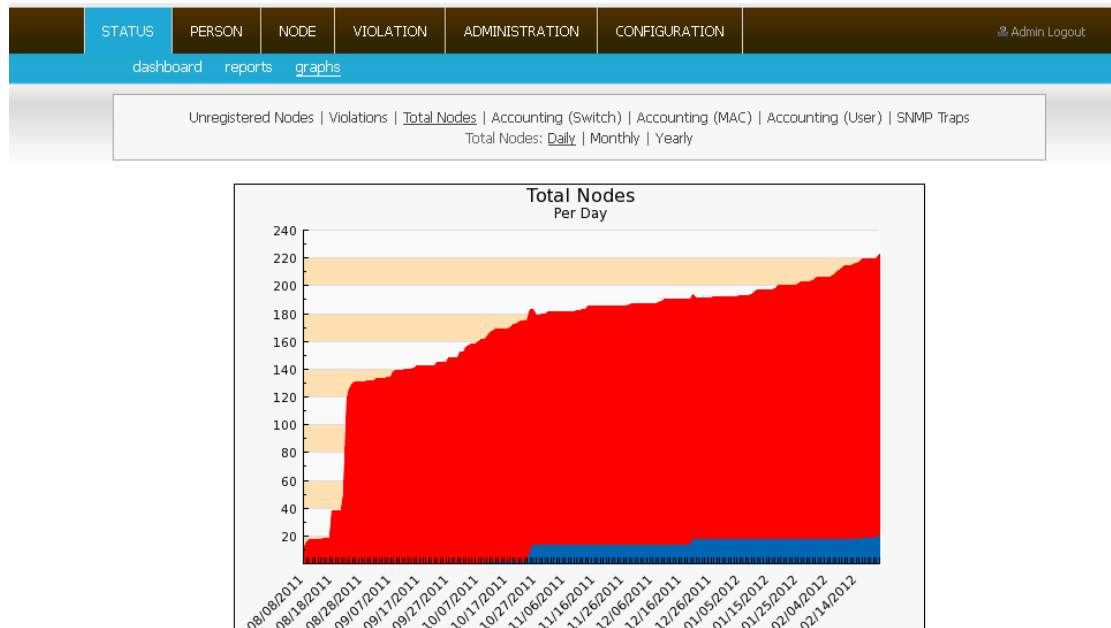


Figura IV.48: Grafico de dispositivos totales.

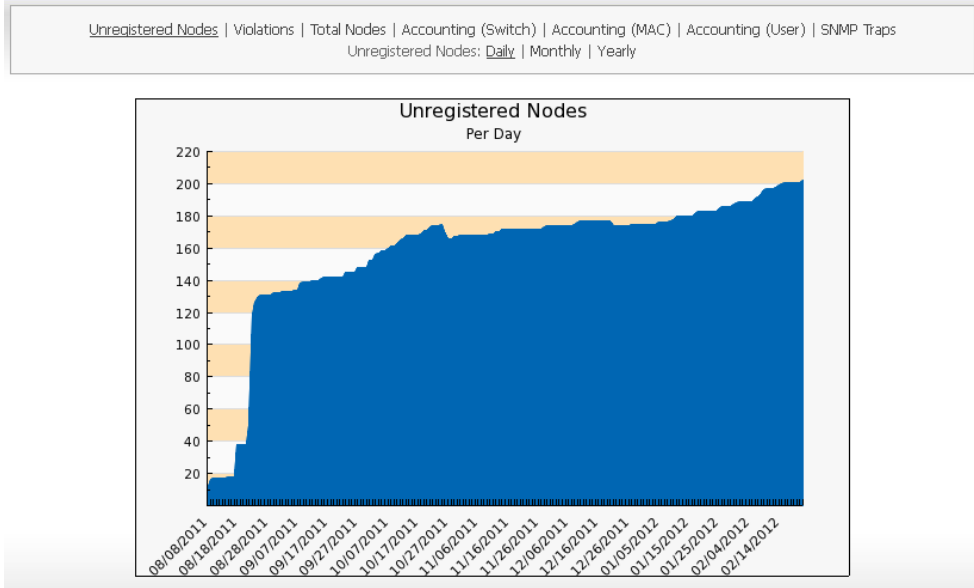


Figura IV.49: Grafico de nodos no registrados.

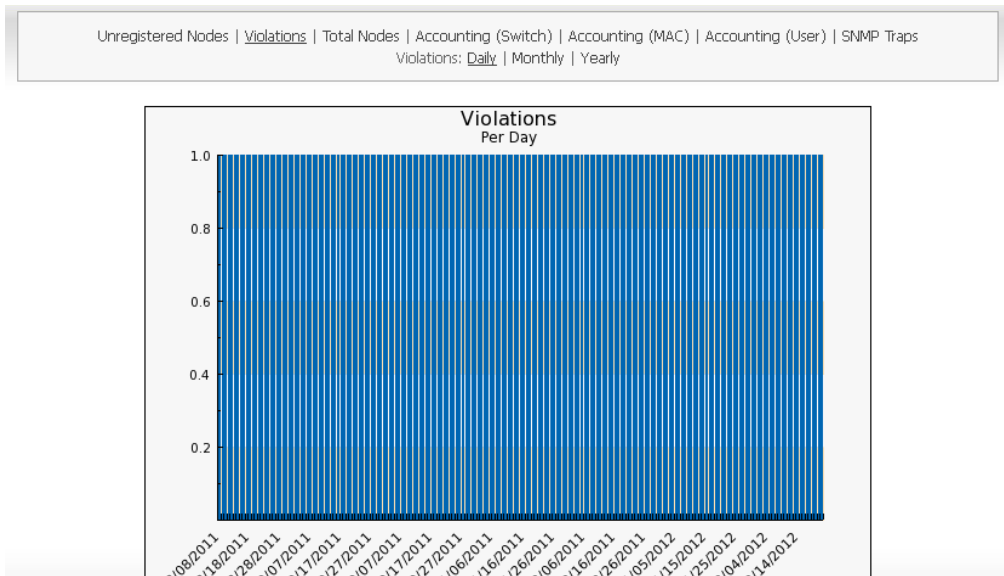


Figura IV.50: Grafico de violaciones.

4.3 COMPROBACIÓN DE LA HIPÓTESIS

4.3.1 Hipótesis de investigación

La utilización de herramientas Network Admission Control OpenSource en la Dirección Provincial del Consejo de la Judicatura de Chimborazo mejorara el control de admisión a los recursos críticos de la LAN.

4.3.2 Tipo de Hipótesis

Hipótesis de Investigación

4.3.3 Población y Muestra

La encuesta (Ver Anexo E) se la aplicó a todo el personal del departamento de informática de la Dirección Provincial del Consejo de la Judicatura de Chimborazo, además al personal que se encuentra a cargo de la administración en las otras dependencias, siendo realizadas 10 encuestas en su totalidad.

4.3.4 Determinación de Variables

Variable Independiente:

Herramientas Network Admission Control OpenSource.

Variable Dependiente:

Control de admisión a los recursos críticos de la LAN.

Operacionalización Conceptual

Tabla IV.IV: Operacionalización Conceptual.

Variable	Tipo	Concepto
Herramientas Network Admission Control OpenSource.	Independiente	Proporcionan una forma de aplicar las políticas de seguridades dentro de la red LAN, además de detectar los dispositivos finales así como las vulnerabilidades y violaciones que puedan tener los mismos.
Control de admisión a los recursos críticos de la LAN.	Dependiente	Capacidad de controlar los dispositivos que ingresan a la red LAN.

Operacionalización metodológica

Tabla IV.V: Operacionalización metodológica.

Variable	Categoría	Indicadores	Técnicas	Fuentes de Verificación
Herramientas Network Admission Control OpenSource.	Requerimientos de Utilización.	<ul style="list-style-type: none"> • Herramienta PacketFence. • Herramienta Snort. • Herramienta Nessus. 	<ul style="list-style-type: none"> • Utilización Directa . • Revisión de documentos. 	<ul style="list-style-type: none"> • Internet • Manuales • Tutoriales • Listas de Correo.
Control de admisión a los recursos críticos de la LAN.		<ul style="list-style-type: none"> • Violaciones de Seguridad. • Vulnerabilidades de los dispositivos finales. 	<ul style="list-style-type: none"> • Observación. • Comparaciones de violaciones y vulnerabilidades. 	<ul style="list-style-type: none"> • Reportes • Gráficos Estadísticos. • Aplicación de las políticas de seguridad.

4.3.5 Comprobación de la hipótesis de investigación

4.3.5.1 Planteamiento de la hipótesis:

Hi: Mediante el análisis de herramientas Network Admission Control OpenSource aplicado a la Dirección Provincial del Consejo de la Judicatura de Chimborazo mejorara el control de admisión a los recursos críticos de la red LAN.

Ho: Mediante el análisis de herramientas Network Admission Control OpenSource aplicado a la Dirección Provincial del Consejo de la Judicatura de Chimborazo no mejorara el control de admisión a los recursos críticos de la red LAN.

4.3.5.2 Nivel de Significancia

El nivel de significancia, que en este análisis se utilizará un nivel de significación estadística de $\alpha = 0.05$, dado que es probable que la herramienta elegida en el análisis para la implementación no se pueda usar en toda la red LAN institucional.

4.3.5.3 Criterio

De acuerdo al análisis desarrollado en la presente investigación, se ha seleccionado como estadístico de prueba de hipótesis la técnica "*chi-cuadrado*". La fórmula que da el estadístico es la siguiente:

$$x^2 = \sum_i \frac{(\text{observada}_i - \text{esperada}_i)^2}{\text{esperada}_i}$$

Para conocer las frecuencias teóricas o esperadas, se calculan a través del producto de los totales marginales (*total del renglón x total de columna*), dividido por el número total de casos (*gran total*):

$$fe = \frac{(total\ del\ renglón) * (total\ de\ la\ columna)}{gran\ total}$$

En la **tabla** se pueden observar los resultados de los cálculos, tanto de la frecuencia esperada, como la del valor de " $X^2_{calculado}$ ", luego de haber aplicado las fórmulas anteriores. Ahora es necesario determinar el **criterio de decisión**. Entonces se acepta **H₀** cuando:

$$X^2_{calculado} < X^2_{tabla}, \text{ en caso contrario se rechaza } H_0.$$

Donde el valor de X^2_{tabla} representa el valor proporcionado por la tabla de "distribución X^2 ", según el nivel de significación elegido y los grados de libertad. El nivel de significancia adoptado para esta investigación es de $\alpha = 0,05$. Para la determinación de los grados de libertad (**gl**) se debe aplicar la siguiente fórmula:

$$gl = (r - 1) * (k - 1)$$

Tabla IV.VI: Distribución de X.

Degrees of Freedom	Possibility of Chance Occurrence in Percentage (5% or Less Considered Significant)								
	90%	80%	70%	50%	30%	20%	10%	5%	1%
1	0.016	0.064	0.148	0.455	1.074	1.642	2.706	3.841	6.635
2	0.211	0.446	0.713	1.386	2.408	3.219	4.605	5.991	9.210
3	0.584	1.005	1.424	2.366	3.665	4.642	6.251	7.815	11.341
4	1.064	1.649	2.195	3.357	4.878	5.989	7.779	9.488	13.277
5	1.610	2.343	3.000	4.351	6.064	7.289	9.236	11.070	15.086
6	2.204	3.070	3.828	5.348	7.231	8.558	10.645	12.592	16.812
7	2.833	3.822	4.671	6.346	8.383	9.083	12.017	14.067	18.475
8	3.490	4.594	5.527	7.344	9.524	11.030	13.362	15.507	20.090
9	4.168	5.380	6.393	8.343	10.656	12.242	17.684	16.919	21.666

4.3.5.4 Cálculos

Los resultados de la investigación realizadase resumen en las tablas mostradas a continuación:

Tabla IV.VII: Resultados de Factibilidad.

FACTIBILIDAD		
PREGUNTA	MEJORA	NO MEJORA
PREGUNTA 1	5	0
PREGUNTA 7	5	0
TOTAL	10	0

Tabla IV.VIII: Resultados de Gestión.

GESTIÓN		
PREGUNTA	MEJORA	NO MEJORA
PREGUNTA 2	4	1
PREGUNTA 6	4	1
TOTAL	8	2

Tabla IV.IX: Resultados de Usabilidad.

USABILIDAD		
PREGUNTA	MEJORA	NO MEJORA
PREGUNTA 3	4	1
TOTAL	4	1

Tabla IV.X: Resultados de Seguridad.

SEGURIDAD		
PREGUNTA	MEJORA	NO MEJORA
PREGUNTA 4	4	1
PREGUNTA 5	5	0
TOTAL	9	1

Tabla IV.XI: Resultados de Productividad.

PRODUCTIVIDAD		
PREGUNTA	MEJORA	NO MEJORA
PREGUNTA 4	5	0
TOTAL	5	0

La matriz de los resultados obtenidos queda conformada de la siguiente manera:

Tabla IV.XII: Matriz de resultados totales de la encuesta.

Herramientas Network Admission Control OpenSource	Control De Admisión A Los Recursos Críticos De La Red LAN.		
	MEJORA	NO MEJORA	TOTAL
FACTIBILIDAD	10	0	10
GESTIÓN	8	2	10
USABILIDAD	4	1	5
SEGURIDAD	9	1	10
PRODUCTIVIDAD	5	0	5
TOTAL	36	4	40

De la tabla anterior se realiza el cálculo para el grado de libertad.

$$gl = (5-1) * (2-1)$$

$$gl = (4) * (1)$$

$$gl = 4 \text{ grado de libertad}$$

Consultando la tabla estadística de distribución de chi-cuadrado, tomando el valor de significancia 0,05 y grado de libertad 4, el valor $\chi^2_{\text{tabla}} = 9.488$

Tabla IV.XIII: Matriz de resultados esperados.

Herramientas Network Admission Control OpenSource	Control De Admisión A Los Recursos Críticos De La Red LAN.		
	MEJORA	NO MEJORA	TOTAL
FACTIBILIDAD	7	3	10
GESTIÓN	6	4	10
USABILIDAD	3	2	5
SEGURIDAD	6	4	10
PRODUCTIVIDAD	4	1	5
TOTAL	26	14	40

Diseñamos la tabla para aplicar la fórmula de chi-cuadrado:

Tabla IV.XII: Frecuencia observada sobre frecuencia esperada.

	fo	fe	(fo-fe) ² / fe
La Herramienta NAC OpenSource mejora la Factibilidad	10	7	1,29
La Herramienta NAC OpenSource mejora la Gestión	8	6	0,67
La Herramienta NAC OpenSource mejora la Usabilidad	4	3	0,33
La Herramienta NAC OpenSource mejora la Seguridad	9	6	1,5
La Herramienta NAC OpenSource mejora la Productividad	5	4	0,25
La Herramienta NAC OpenSource no mejora la Factibilidad	0	3	3
La Herramienta NAC OpenSource no mejora la Gestión	2	4	1
La Herramienta NAC OpenSource no mejora la Usabilidad	1	2	0,5
La Herramienta NAC OpenSource no mejora la Seguridad	1	4	2,25
La Herramienta NAC OpenSource no mejora la Productividad	0	1	1
TOTAL	40	40	11,79

4.3.5.5 Demostración de la Hipótesis

Como:

$$\mathbf{X^2}_{\text{calculado}} = 11,79\mathbf{y}$$

$$\mathbf{X^2}_{\text{tabla}} = 9,488$$

Entonces:

$$\mathbf{X^2}_{\text{calculado}} > \mathbf{X^2}_{\text{tabla}}$$

Esto significa que $\mathbf{X^2}_{\text{calculado}}$, está en la zona de rechazo de la $\mathbf{H_0}$, entonces se concluye que se rechaza la hipótesis nula y se acepta la de investigación, por lo tanto:

“Mediante el análisis de herramientas Network Admission Control OpenSource aplicado a la Dirección Provincial del Consejo de la Judicatura de Chimborazo mejorara el control de admisión a los recursos críticos de la red LAN.”

CONCLUSIONES

- Para evaluar las herramientas que fueron seleccionadas como objeto de estudio en la presente investigación, se tomó en cuenta varios parámetros para el estudio comparativo, los mismos que fueron seleccionados cuidadosamente, resultando de esta la herramienta seleccionada PacketFence con 92.5%, ya que cumplió con la mayoría de los parámetros propuestos con mayor eficacia.
- El entorno gráfico que brinda PacketFence para la administración de dispositivos se considera como uno de los más agradables e intuitivos en el ambiente “OpenSource” además el constante y robusto sistema de apoyo por parte de entidades como la “comunidad PacketFence” en la elaboración y soporte de utilidades, brindan alta confiabilidad en el momento de buscar ayuda.
- Una vez detectados los problemas de seguridad presentes en la red de la Dirección Provincial del Consejo de la Judicatura de Chimborazo, se los analizó todos y cada uno, como: presencia de virus, caídas inesperadas de enlaces, vulnerabilidades e infracciones de seguridad en la red LAN; se propuso soluciones para contrarrestar los mismos y hacer que la red trabaje bajo normalidad, teniendo pronta respuesta en varios de estas.
- La Implementación de la herramienta PacketFence para la administración de las políticas y el control del acceso a la red de la Dirección Provincial del Consejo de la Judicatura de Chimborazo, resultó de gran utilidad ya que se optimizó la gestión del administrador de la red en cuanto a detección y solución de vulnerabilidades y violaciones en la red LAN, reduciendo de esta forma tiempo y recursos, que se usaban antes de la implementación de la herramienta, además la productividad de la red mejoró haciendo que los dispositivos no presenten demasiados problemas.

RECOMENDACIONES

- Se recomienda al personal de la Unidad Informática de la Dirección Provincial del Consejo de la Judicatura de Chimborazo realizar actualizaciones de las políticas de seguridad y del inventario de dispositivos dentro de la red, constandingo en este, las configuraciones de IP, ubicación de los equipos y correcta aplicación de las políticas, para de esta manera tener organizada y controlada la red LAN.
- A medida que los dispositivos se van renovando o incrementando en la red de la institución es necesario ir añadiéndolos a la herramienta, para de esta forma contar con el monitoreo del estado de los dispositivos de forma centralizada.
- Ser cuidadosos al momento de realizar las actualizaciones de versión de la herramienta y de los componentes de la misma, ya que existe una variación de uso de librerías y configuración de servicios, y hacer mal este proceso puede llevar al mal funcionamiento del servidor.
- Para que la calidad de servicio que brinda la Unidad Informática mejore, es recomendable realizar los cambios en los IOS de los equipos cisco, ya que las actualizaciones a IOS criptográficos sería una ayuda significativa para la seguridad de la red LAN.

RESUMEN

Esta investigación se realizó con el objetivo de seleccionar una herramienta NAC OpenSource para mejorar la seguridad de la red LAN según previo análisis y aplicarla en la Dirección Provincial del Consejo de la Judicatura de Chimborazo.

El método utilizado como guía para la presente investigación fue el analítico e investigativo, además para el desarrollo del análisis se realizó un ambiente de pruebas con los siguientes materiales: una computadora portátil Dell N4010, la aplicación para virtualización VMware Workstation 8 y el sistema operativo Centos 5,6.

Mediante el análisis comparativo de las herramientas NAC OpenSource se logró establecer que la aplicación de estas herramientas mejora el control de acceso a los recursos críticos de la red. Obteniendo como resultados a PacketFence como herramienta NAC OpenSource de mayor eficacia para aplicar las políticas de seguridad y la identificación de vulnerabilidades y amenazas dentro de la red LAN. Con el uso de Chi Cuadrado con un grado de libertad de 4 y un nivel de significancia de 0,05 se pudo demostrar que PacketFence mejora el control de admisión a los recursos críticos de la red LAN.

La implantación de esta herramienta, facilitó el trabajo del administrador de red en cuanto a gestionar la seguridad de la red, uso de tiempo y recursos, además de permitir aplicar las políticas de seguridad.

En la actualidad es recomendable usar herramientas de administración y monitoreo de la red LAN, para así poder tomar medidas preventivas y correctivas para solucionar o controlar problemas en la misma.

ABSTRACT

This research was conducted with the aim of selecting a Tool Open Source Network Admission Control (NAC.), to improve Network Security Local Area Security (LAN), as provided analysis and apply the Provincial Judicial Council of Chimborazo.

The method used to guide this research was the analytical and investigative. In addition, development of analysis was a test environment with the following stuff: a Dell Laptop N4010, the application in order to display and VMware Workstation 8 and Centos 5.6 operating system.

By comparative analysis of the NAC Open Source tools are able to establish that the application of these tools improves control over the critical network resources. As result is obtained a PacketFence Nac Open Source tool more effective to implement security policies and identifying vulnerabilities and threats within the LAN. Using Chi square with one degree of freedom of 4 and a significance level of 0,05 could be demonstrated that enhances PacketFence admission control critical resources of the LAN.

The implementation of this tool facilitated the work of the network administrator as to manage the security of the network, use of time, and resources, beside allowing security policies apply.

At, present, it is recommended to use management tools and LAN Network Monitoring, in order to take preventive and corrective measures to solve, or control network problems Local Area Network (LAN).

ABREVIATURAS Y ACRÓNIMOS

ABREVIATURAS

HW: Hardware

SW: Software

ORG: Organización.

FAQ's: Preguntas frecuentes

ACRÓNIMOS

S.O: Sistema Operativo

DHCP: Dynamic Host Configuration Protocol

NAC: Network Admission Control

DNS: Domain Name System

SNMP: Simple Network Management Protocol

ANEXOS

ANEXO A ANÁLISIS DE RIESGOS

1. Desarrollo del Análisis de Riesgos:

Cada recurso definido en el capítulo II en la sección de políticas de seguridad pasara por el sistema analizador de riesgo. Cada riesgo contiene 6 variables las cuales pueden contener los siguientes valores:

Tabla B.I: Tabla de Términos Lingüísticos.

Variables de Riesgo			Variables de Importancia		
Acceso No Autorizado	Robo de Información	Negación de Servicios	Disponibilidad	Confidencialidad	Integridad
Ninguno	Ninguno	Ninguno	Ninguna	Ninguna	Ninguna
Bajo	Bajo	Bajo	Baja	Baja	Baja
Moderado	Moderado	Moderado	Moderada	Moderada	Moderada
Alto	Alto	Alto	Alta	Alta	Alta

Es necesario que los expertos establezcan los rangos de los valores numéricos en una escala del 0 al 10, donde 0 representa menor riesgo o importancia y 10 mayor riesgo o importancia. Los valores de estas variables, para cada uno de los recursos analizados serán otorgados por los expertos consultados, en este caso las Ingenieras encargadas del Centro de Cómputo.

Riesgos:

Tabla B.II: Tabla de Valores para los Parámetros de Riesgo.

- Acceso no Autorizado:

Nivel del Riesgo	Valor
Ninguno	0
Bajo	9
Moderado	9
Alto	10

- Robo de Información:

Nivel del Riesgo	Valor
Ninguno	0
Bajo	8
Moderado	10
Alto	10

- Negación de Servicios:

Nivel del Riesgo	Valor
Ninguno	0
Bajo	4
Moderado	9
Alto	10

Importancia:

Tabla B.III: Tabla de Valores para los Parámetros de Importancia.

- Disponibilidad:

Nivel de Importancia	Valor
Ninguna	0
Baja	6
Moderada	8
Alta	10

- Confidencialidad:

Nivel de Importancia	Valor
Ninguna	0
Baja	4
Moderada	7
Alta	10

- Integridad:

Nivel de Importancia	Valor
Ninguna	0
Baja	5
Moderada	7
Alta	10

1.1. Calificación de variables por recurso por parte de la encargada de la red institucional:

Una vez que la encargada de Redes definió a juicio personal los valores de las variables se le solicitó que llenara la siguiente tabla:

Tabla B.IV: Cuadro de Calificación de Recursos por parte de la encargada de la Red Informática.

Recursos		Riesgos (Posibles Ataques)			Importancia		
No	Nombre o Descripción	Acceso no Autorizado	Robo de Información	Negación de Servicios	Disponibilidad	Integridad	Confidencialidad
Equipos de Red							
01	Switch Principal (4503 Capa 3)	Bajo	Bajo	Bajo	Alto	Alta	Alta
02	Switch Quinto Piso (2960 Capa 2)	Bajo	Bajo	Moderado	Alta	Moderada	Alta
03	Switch Cuarto Piso (2960 Capa 2)	Bajo	Bajo	Moderado	Alta	Moderada	Alta
04	Switch Tercer Piso (2960 Capa 2)	Bajo	Bajo	Moderado	Alta	Moderada	Alta
05	Switch Mezanine (2960 Capa 2)	Bajo	Bajo	Moderado	Alta	Moderada	Alta
06	Switch Planta Baja (2960 Capa 2)	Bajo	Bajo	Moderado	Alta	Moderada	Alta
Servidores							
A	Servidor DHCP, Postfix	Moderado	Moderado	Moderado	Alta	Alta	Alta
B	Servidor de Aplicaciones Satje	Moderado	Moderado	Alto	Alta	Alta	Alta
C	Servidor de Pensiones Alimenticias	Bajo	Bajo	Moderado	Alta	Alta	Alta
D	Servidor de Reloj	Bajo	Medio	Bajo	Moderada	Alta	Moderada
E	Servidor de Antivirus y Dominios	Medio	Bajo	Moderado	Alta	Moderada	Moderada
F	Servidor de Información	Bajo	Bajo	Moderado	Moderada	Alta	Alta
G	Servidor de Trámite Judicial Cantones	Moderado	Moderado	Alto	Alta	Alta	Alta
H	Servidor Web	Alto	Alto	Alto	Alta	Moderada	Moderada
I	Servidor NAC, Squid Transparente, Router	Bajo	Bajo	Bajo	Alta	Moderada	Moderada

Determinar el riesgo de la red del centro de cómputo

Una vez determinado los valores de los diferentes equipos de red se procede a calcular el Riesgo e Importancia Total para así determinar el Riesgo Total de los equipos de Red de la institución.

Dividimos la Tabla B.IV en dos partes para calcular el Riesgo Total y la Importancia Total de cada Dispositivo de Red. Para esto también reemplazamos los valores numéricos por los valores lingüísticos según se definió anteriormente en las Tablas A.II y A.III.

Tabla B.V: Calculo de los valores de Riesgo Total por Parámetro de Riesgo

Recursos		Riesgos (Posibles Ataques)			
No	Nombre o Descripción	Acceso no Autorizado	Robo de Información	Negación de Servicios	Riesgo Total
Equipos de Red					
01	Switch Principal (4503 Capa 3)	9	8	4	7
02	Switch Quinto Piso (2960 Capa 2)	9	8	9	9
03	Switch Cuarto Piso (2960 Capa 2)	9	8	9	9
04	Switch Tercer Piso (2960 Capa 2)	9	8	9	9
05	Switch Mezanine (2960 Capa 2)	9	8	9	9
06	Switch Planta Baja (2960 Capa 2)	9	8	9	9
Servidores					
A	Servidor DHCP, Postfix	9	10	9	9
B	Servidor de Aplicaciones Satje	9	10	10	10
C	Servidor de Pensiones Alimenticias	9	8	9	9
D	Servidor de Reloj	9	10	4	8
E	Servidor de Antivirus y Dominios	9	8	9	9
F	Servidor de Información	9	8	9	9
G	Servidor de Trámite Judicial Cantones	9	10	10	9
H	Servidor Web	10	10	10	10
I	Servidor NAC, Squid Transparente, Router	9	8	4	7

1.2. Cálculos realizados para el Riesgo de cada parámetro:

Equipos de Red:

01 Switch Principal (4503 Capa 3)

$$\frac{9 + 8 + 4}{3} = 7$$

02 Switch Quinto Piso (2960 Capa 2)

$$\frac{9 + 8 + 9}{3} = 9$$

03 Switch Cuarto Piso (2960 Capa 2)

$$\frac{9 + 8 + 9}{3} = 9$$

04 Switch Tercer Piso (2960 Capa 2)

$$\frac{9 + 8 + 9}{3} = 9$$

05 Switch Mezanine (2960 Capa 2)

$$\frac{9 + 8 + 9}{3} = 9$$

06 Switch Planta Baja (2960 Capa 2)

$$\frac{9 + 8 + 9}{3} = 9$$

Servidores:

A: Servidor DHCP, Postfix

$$\frac{9 + 10 + 9}{3} = 9$$

B: Servidor de Aplicaciones Satje

$$\frac{9 + 10 + 10}{3} = 10$$

C: Servidor de Pensiones Alimenticias

$$\frac{9 + 8 + 9}{3} = 9$$

D: Servidor de Reloj

$$\frac{9 + 10 + 4}{3} = 8$$

E: Servidor de Antivirus y Dominios

$$\frac{9 + 8 + 9}{3} = 9$$

F: Servidor de Información

$$\frac{9 + 8 + 9}{3} = 9$$

G: Servidor de Trámite Judicial Cantones

$$\frac{9 + 10 + 10}{3} = 9$$

H: Servidor Web

$$\frac{10 + 10 + 10}{3} = 10$$

I: Servidor NAC, Squid Transparente, Router

$$\frac{9 + 8 + 4}{3} = 7$$

Tabla B.VI: Calculo de los valores de Importancia Total por Parámetro de Importancia.

Recursos		Importancia			
No.	Nombre o Descripción	Disponibilidad	Integridad	Confidencialidad	Importancia Total
Equipos de Red					
01	Switch Principal (4503 Capa 3)	10	10	10	10
02	Switch Quinto Piso (2960 Capa 2)	10	7	10	9
03	Switch Cuarto Piso (2960 Capa 2)	10	7	10	9
04	Switch Tercer Piso (2960 Capa 2)	10	7	10	9
05	Switch Mezanine (2960 Capa 2)	10	7	10	9
06	Switch Planta Baja (2960 Capa 2)	10	7	10	9
Servidores					
A	Servidor DHCP, Postfix	10	10	10	10
B	Servidor de Aplicaciones Satje	10	10	10	10
C	Servidor de Pensiones Alimenticias	10	10	10	10
D	Servidor de Reloj	8	10	7	8
E	Servidor de Antivirus y Dominios	10	7	7	8
F	Servidor de Información	8	10	10	9
G	Servidor de Trámite Judicial Cantones	10	10	10	10
H	Servidor Web	10	7	7	8
I	Servidor NAC, Squid Transparente, Router	10	7	7	8

1.3. Cálculos realizados para la Importancia de cada parámetro:

Equipos de Red:

01: Switch Principal (4503 Capa 3)

$$\frac{10 + 10 + 10}{3} = 10$$

02: Switch Quinto Piso (2960 Capa 2)

$$\frac{10 + 7 + 10}{3} = 9$$

03: Switch Cuarto Piso (2960 Capa 2)

$$\frac{10 + 7 + 10}{3} = 9$$

04: Switch Tercer Piso (2960 Capa 2)

$$\frac{10 + 7 + 10}{3} = 9$$

05: Switch Mezanine (2960 Capa 2)

$$\frac{10 + 7 + 10}{3} = 9$$

06: Switch Planta Baja (2960 Capa 2)

$$\frac{10 + 7 + 10}{3} = 9$$

Servidores:

A: Servidor DHCP, Postfix

$$\frac{10 + 10 + 10}{3} = 10$$

B: Servidor de Aplicaciones Satje

$$\frac{10 + 10 + 10}{3} = 10$$

C: Servidor de Pensiones Alimenticias

$$\frac{10 + 10 + 10}{3} = 10$$

D: Servidor de Reloj

$$\frac{8 + 10 + 7}{3} = 8$$

E: Servidor de Antivirus y Dominios

$$\frac{10 + 7 + 7}{3} = 8$$

F: Servidor de Información

$$\frac{8 + 10 + 10}{3} = 9$$

G: Servidor de Trámite Judicial Cantones

$$\frac{10 + 10 + 10}{3} = 10$$

H: Servidor Web

$$\frac{10 + 7 + 7}{3} = 8$$

I: Servidor NAC, Squid Transparente, Router

$$\frac{10 + 7 + 7}{3} = 8$$

1.4. Calculo del Riesgo Total

Para determinar el Riesgo Total de los Dispositivos procedemos a utilizar la formula $R \times W$. Los valores resultados de esta operación se evaluarán en el rango del 0 al 100 para poder analizarlos e interpretarlos de mejor manera:

Tabla B.VI: Calculo del Riesgo Total de los Equipos de Red de la Institución.

Recursos		Calculo del Riesgo		
No	Nombre o Descripción	Riesgo (R)	Importancia (W)	Riesgo Total (RxW)
Equipos de Red				
01	Switch Principal (4503 Capa 3)	7	10	70
02	Switch Quinto Piso (2960 Capa 2)	9	9	81
03	Switch Cuarto Piso (2960 Capa 2)	9	9	81
04	Switch Tercer Piso (2960 Capa 2)	9	9	81
05	Switch Mezanine (2960 Capa 2)	9	9	81
06	Switch Planta Baja (2960 Capa 2)	9	9	81
Servidores				
A	Servidor DHCP, Postfix	9	10	90
B	Servidor de Aplicaciones Satje	10	10	100
C	Servidor de Pensiones Alimenticias	9	10	90
D	Servidor de Reloj	8	8	64
E	Servidor de Antivirus y Dominios	9	8	72
F	Servidor de Información	9	9	81
G	Servidor de Trámite Judicial Cantones	9	10	90
H	Servidor Web	10	8	80
I	Servidor NAC, Squid Transparente, Router	7	8	56

2. Comparación y conclusión del análisis de riesgos.

Para realizar una comparación y conclusión del análisis de riesgos se realizó una tabla para la interpretación de los valores obtenidos de la Tabla B.VI dándoles un valor lingüístico.

El riesgo total a partir de los resultados obtenidos del análisis, es realizado de la siguiente manera:

Tabla B.VII: Representación de valores lingüísticos.

Valor Numérico	Valor Lingüístico
96-100	Alto+
90-95	Alto-
80-89	Medio+
60-79	Medio-
35-59	Bajo+
10-34	Bajo-
0-9	Ninguno

- **Alto+** Esta calificación nos dice que es un recurso crítico y de alta importancia para la institución.
- **Alto-** Este tipo de recurso es de un riesgo alto moderado lo que significa que tiene una alta importancia
- **Medio+** Este valor lingüístico nos dice que el recurso tiene un valor moderado alto.
- **Medio-** El recurso es de un valor moderado bajo el cual significa que es significativa para la institución.
- **Bajo+** Este valor significa que el riesgo es bajo pero que puede tener algo de importancia para la institución.
- **Bajo-** Es un recurso de bajo riesgo que no es necesario exagerar con las seguridades.
- **Ninguno** El recurso no posee ningún riesgo o es insignificante. Es decir no hay porque proteger ese recurso.

De esta manera los resultados finales son:

Tabla B.VII: Riesgo Total en valores lingüísticos.

Recursos		
No	Nombre o Descripción	Riesgo Total (RxW)
Equipos de Red		
01	Switch Principal (4503 Capa 3)	Medio-
02	Switch Quinto Piso (2960 Capa 2)	Medio+
03	Switch Cuarto Piso (2960 Capa 2)	Medio+
04	Switch Tercer Piso (2960 Capa 2)	Medio+
05	Switch Mezanine (2960 Capa 2)	Medio+
06	Switch Planta Baja (2960 Capa 2)	Medio+
Servidores		
A	Servidor DHCP, Postfix	Alto-
B	Servidor de Aplicaciones Satje	Alto+
C	Servidor de Pensiones Alimenticias	Alto-
D	Servidor de Reloj	Medio-
E	Servidor de Antivirus y Dominios	Medio-
F	Servidor de Información	Medio+
G	Servidor de Trámite Judicial Cantones	Alto-
H	Servidor Web	Medio+
I	Servidor NAC, Squid Transparente, Router	Bajo+

Con estas sencillas operaciones con términos lingüísticos, se ha logrado cuantificar el riesgo en cada recurso conectado al Backbone de la institución. Estos resultados no representan totalmente la realidad ya que los riesgos de ataques son muy variables porque cada año surgen nuevas brechas de seguridad en sistemas de redes de computadoras, y es difícil predecir el comportamiento de las personas que generan los ataques.

Con este estudio, se establece una medida estimativa del riesgo e importancia para clarificar que es lo que se necesita proteger, y cuales recursos son más indispensables de proteger que otros. A partir de estas conclusiones ya se pueden generar políticas de seguridad.

ANEXO B

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1. Documentación de la Política de Seguridad de la Información

El objetivo es proporcionar a la Dirección Provincial del Consejo de la Judicatura de Chimborazo apoyo a la seguridad de la información en concordancia con los requerimientos, leyes y regulaciones relevantes.

1.1. Documentar política de seguridad de información

La Dirección Provincial debe aprobar un documento de políticas de seguridad, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.

1.2. Revisión de la política de seguridad de la información

La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad. Se recomienda que la revisión sea cada 3 meses.

2. Organización de la seguridad de la información

2.1. Organización Interna

Objetivo: Manejar la seguridad de la información dentro de la organización.

2.1.1. Compromiso de la Dirección Provincial con la seguridad de la información.

La Dirección Provincial debe apoyar activamente la seguridad dentro de la institución a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.

2.1.2. Coordinación de la seguridad de información

Las actividades de seguridad de la información deben ser coordinadas por la Unidad Informática en concordancia y respaldo de la Dirección Provincial.

2.1.3. Asignación de responsabilidades de la seguridad de la información

La seguridad de la información debe ser responsable de la Unidad Informática y del personal responsable de esta función.

2.1.4. Proceso de autorización para los medios de procesamiento de información.

La Unidad Informática será la encargada de la autorización para los medios de procesamiento previo informe a la Dirección Provincial si fuese necesario.

2.1.5. Acuerdos de confidencialidad

Se deben identificar y revisar cada 3 meses los requerimientos de confidencialidad o los acuerdos de no divulgación reflejando las necesidades de la institución para la protección de la información.

2.1.6. Contacto con autoridades

Se debe mantener los contactos con autoridades en el ámbito de la seguridad informática.

2.1.7. Contacto con grupos de interés especial

Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.

2.1.8. Revisión independiente de la seguridad la información

El enfoque de la institución para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.

2.2. Entidades Externas

Objetivo: Mantener la seguridad de la información de la institución y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.

2.2.1. Identificación de riesgos relacionados con entidades externas

Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.

2.2.2. Tratamiento de la seguridad cuando se trabaja con clientes

Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes accesos a la información o activos de la organización.

2.2.3. Tratamiento de la seguridad en contratos con terceras personas.

Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.

3. Gestión de los Activos

3.1. Responsabilidad por los Activos

Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales.

3.1.1. Inventarios de activos

Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.

3.1.2. Propiedad de los activos

Toda la información y los activos asociados con los medios de procesamiento de la información deben ser ‘propiedad’¹ de una parte designada de la organización.

3.1.3. Uso aceptable de los activos

Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.

3.2. Clasificación de la información

Objetivo: Asegurar que a información reciba un nivel de protección apropiado.

3.2.1. Lineamientos de clasificación

La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.

3.2.2. Etiquetado y manejo de la información

Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.

4. Seguridad de los Recursos Humanos

4.1. Antes del empleo²

Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.

¹ El término ‘propietario’ identifica a una persona o entidad que tiene la responsabilidad administrativa aprobada para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término ‘propietario’ no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

² La palabra ‘empleo’ se utiliza para abarcar todas las siguientes situaciones diferentes: empleo de personas (temporal o larga duración), asignación de roles laborales, cambios de trabajo, asignación de contratos y la terminación de cualquiera de estos acuerdos.

4.1.1. Roles y responsabilidades

Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la institución.

4.1.2. Selección

Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

4.1.3. Términos y condiciones de empleo.

Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.

4.2. Durante el Empleo

Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones y que estén equipados para apoyar la política de seguridad institucional en el curso de su trabajo normal, y reducir los riesgos de error humano.

4.2.1. Gestión de responsabilidades

La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.

4.2.2. Capacitación y educación en seguridad de la información

Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.

4.2.3. Proceso disciplinario

Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.

4.3. Terminación o cambio del Empleo

Objetivo: Asegurar que los empleados, contratistas y terceros salgan de la institución o cambien de empleo de una manera ordenada.

4.3.1. Responsabilidades de terminación

Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo.

4.3.2. Devolución de activos

Todos los empleados, contratistas y terceros deben devolver todos los activos de la institución que estén en su posesión a la terminación de su empleo, contrato o acuerdo.

4.3.3. Eliminación de derechos de acceso

Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.

5. Seguridad Física Y Ambiental

5.1. Áreas Seguras

Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.

5.1.1. Perímetro seguridad física

Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.

5.1.2. Controles de entrada físicos

Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.

5.1.3. Seguridad de oficinas, habitaciones y medios

Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.

5.1.4. Protección contra amenazas externas y ambientales

Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.

5.1.5. Trabajo en áreas seguras

Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.

5.1.6. Áreas de acceso público, entrega y carga

Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a las unidades, juzgados, etc. y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.

5.2. Seguridad del Equipo

Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la institución.

5.2.1. Ubicación y protección de los equipos

Los equipos deben estar ubicados o protegidos para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.

5.2.2. Servicios Públicos

El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.

5.2.3. Seguridad en el cableado

El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la interceptación o daño.

5.2.4. Mantenimiento de equipo

El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.

5.2.5. Seguridad del equipo fuera-del-local

Se debe aplicar seguridad al equipo fuera-del-local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la institución.

5.2.6. Eliminación seguro o re-uso del equipo

Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.

5.2.7. Traslado de Propiedad

Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.

6. Gestión de las comunicaciones y operaciones

6.1. Procedimientos y responsabilidades operacionales

Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información.

6.1.1. Procedimientos de operación documentados

Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.

6.1.2. Gestión de cambio

Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.

6.1.3. Segregación de deberes

Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la institución.

6.1.4. Separación de los medios de desarrollo y operacionales

Se deben separar los medios de desarrollo, prueba y para reducir los riesgos de operacionales accesos no-autorizados o cambios en el sistema de operación.

6.2. Gestión de la entrega del servicio de terceros

Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.

6.2.1. Entrega del servicio

Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega del servicio de terceros.

6.2.2. Monitoreo y revisión de los servicios de terceros

Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente.

6.2.3. Manejar los cambios en los servicios de terceros

Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la re-evaluación de los riesgos.

6.3. Planeación y aceptación del sistema

Objetivo: Minimizar el riesgo de fallas en los sistemas.

6.3.1. Gestión de capacidad

Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.

6.3.2. Aceptación del sistema

Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.

6.4. Protección contra software malicioso y código móvil

Objetivo: Proteger la integridad del software y la información.

6.4.1. Controles contra software malicioso

Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos maliciosos y se deben implementar procedimientos de conciencia apropiados.

6.4.2. Controles contra códigos móviles

Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no-autorizado.

6.5. Respaldo (back-up)

Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.

6.5.1. Back-up o respaldo de la información

Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.

6.6. Gestión de seguridad de redes

Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

6.6.1. Controles de red

Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.

6.6.2. Seguridad de los servicios de red

Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en “casa” o sean abastecidos externamente.

6.7. Gestión de medios

Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no autorizada de los activos; y la interrupción de las actividades comerciales.

6.7.1. Gestión de los medios removibles

Deben existir procedimientos para la gestión de medios removibles.

6.7.2. Eliminación de medios

Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere.

6.7.3. Procedimientos de manejo de la información

Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.

6.7.4. Seguridad de documentación del sistema

Se debe proteger la documentación de un acceso no autorizado.

6.8. Intercambio de información

Objetivo: Mantener la seguridad de la información y software intercambiados

6.8.1. Procedimientos y políticas de información y software

Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación dentro de una organización y con cualquier entidad externa.

6.8.2. Acuerdos de intercambio

Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.

6.8.3. Medios físicos en tránsito

Los medios que contienen información deben ser protegidos contra un acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de la institución.

6.8.4. Mensajes electrónicos

Se debe proteger adecuadamente los mensajes electrónicos.

6.8.5. Sistemas de información comercial

Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.

6.9. Monitoreo

Objetivo: Detectar actividades de procesamiento de información no autorizadas.

6.9.1. Registro de auditoria

Se deben producir registros de la actividades de auditoria, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.

6.9.2. Uso del sistema de monitoreo

Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.

6.9.3. Protección de la información del registro

Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no autorizado.

6.9.4. Registros del administrador y operador

Se deben registrar las actividades del administrador y operador del sistema.

6.9.5. Registro de fallas

Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.

6.9.6. Sincronización de relojes

Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.

7. Control de acceso

7.1. Requerimiento institucional para el control del acceso

Objetivo: Controlar acceso a la información

7.1.1. Política de control de acceso

Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y institucionales.

7.2. Gestión del acceso del usuario

Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.

7.2.1. Inscripción del usuario

Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.

7.2.2. Gestión de privilegios

Se debe restringir y controlar la asignación y uso de los privilegios.

7.2.3. Gestión de la clave del usuario

La asignación de claves se debe controlar a través de un proceso de gestión formal.

7.2.4. Revisión de los derechos de acceso del usuario

La gerencia debe revisar los derechos de acceso del de los usuarios a intervalos regulares utilizando usuario un proceso formal.

7.3. Responsabilidades del usuario

Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.

7.3.1. Uso de clave

Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.

7.3.2. Equipo de usuario desatendido

Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido.

7.3.3. Política de pantalla y escritorio limpio

Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.

7.4. Control de acceso a redes

Objetivo: Evitar el acceso no autorizado a los servicios en red.

7.4.1. Política sobre el uso de servicios en red

Los usuarios sólo deben tener acceso a los en red servicios para los cuales han sido específicamente autorizados a usar.

7.4.2. Autenticación del usuario para conexiones externas

Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.

7.4.3. Identificación del equipo en red

Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.

7.4.4. Protección del puerto de diagnóstico remoto

Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.

7.4.5. Segregación en redes

Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.

7.4.6. Control de conexión de redes

Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aplicaciones comerciales.

7.4.7. Control de enrutamiento de redes

Se deben implementar controles para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones.

7.5. Control de acceso al sistema de operación

Objetivo: Evitar acceso no autorizado a los sistemas operativos.

7.5.1. Procedimientos de registro en el terminal

Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro.

7.5.2. Identificación y autenticación del usuario

Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.

7.5.3. Sistema de Gestión de Claves

Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.

7.5.4. Uso de utilidades del sistema

Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.

7.5.5. Sesión inactiva

Las sesiones inactivas deben cerrarse después de un período de inactividad definido.

7.5.6. Limitación de tiempo de conexión

Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.

7.6. Control de acceso a la aplicación e información

Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

7.6.1. Restricción al acceso a la información

Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.

7.6.2. Aislamiento del sistema sensible

Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).

8. Gestión de incidentes en la seguridad de la información

8.1. Reporte de eventos y debilidades en la seguridad de la información

Objetivo: Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.

8.1.1. Reporte de eventos en la seguridad de la información

Los eventos de seguridad de la información deben reportarse a través de los canales administrativos apropiados lo más rápidamente posible.

8.1.2. Reporte de debilidades en la seguridad

Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.

8.2. Gestión de incidentes y mejoras en la seguridad de la información

Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.

8.2.1. Responsabilidades y procedimientos

Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.

8.2.2. Aprendizaje de los incidentes en la información

Deben existir mecanismos para permitir la seguridad de cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.

8.2.3. Recolección de evidencia

Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o

criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.

9. Gestión de la continuidad comercial

9.1. Aspectos de la seguridad de la información de la gestión de la continuidad comercial

Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

9.1.1. Incluir seguridad de la información en el proceso de gestión de continuidad comercial.

Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la institución para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la institución.

9.1.2. Continuidad Comercial y evaluación del riesgo.

Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.

9.1.3. Desarrollar e implementar planes de continuidad incluyendo seguridad de la información

Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.

9.1.4. Marco referencial para la planeación de la continuidad comercial

Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente

los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.

9.1.5. Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales

Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.

10. Cumplimiento

10.1. Cumplimiento con requerimientos legales

Objetivo: Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad.

10.1.1. Identificación de legislación aplicable

Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.

10.1.2. Derechos de propiedad

Se deben implementar los procedimientos intelectual (IPR) apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.

10.1.3. Protección los registros organizacionales

Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.

10.1.4. Protección de data y privacidad de información personal

Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.

10.1.5. Prevención de mal uso de medios de procesamiento de información

Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no autorizados.

10.1.6. Regulación de controles criptográficos

Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.

10.2. Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico

Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

10.2.1. Cumplimiento con las políticas y estándares de seguridad

Los administradores de la Unidad Informática deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.

10.2.2. Chequeo de cumplimiento técnico

Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.

10.3. Consideraciones de auditoría de los sistema de información

Objetivo: Maximizar la efectividad y minimizar la interferencia del proceso de auditoría de los sistema de información.

10.3.1. Controles de auditoria de información

Se deben planear cuidadosamente los sistemas de requerimientos y actividades de las auditorias que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.

10.3.2. Protección de las herramientas de auditoria de los sistemas de información

Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

ANEXO C

INSTALACIÓN Y CONFIGURACIÓN DE PACKETFENCE

1. Pre Requisitos

Para la instalación de PacketFence debemos instalar las herramientas necesarias para el funcionamiento completo de la misma.

Servidor SNMP

Una de las herramientas fundamentales para la comunicación con los equipos de red y PacketFence es SNMP para esto instalaremos un servidor snmp en el mismo servidor en la cual funciona la herramienta.

- Para la instalación de snmp lo realizamos mediante la línea

```
yum -y install net-snmp net-snmp-utils
```
- Realizado la instalación con la herramienta yum procedemos a la configuración. En el archivo de configuración creamos una comunidad con el nombre nac que es tanto

de lectura como de escritura. El archivo de configuración que debemos modificar se encuentra en el directorio `/etc/snmp/snmpd.conf`

```
# First, map the community name "public" into a "security
name"
#       sec.name  source           community
#com2sec notConfigUser default      public
com2sec local 127.0.0.1/32      nac
com2sec red 172.16.148.0/24      nac

####
# Second, map the security name into a group name:
#       groupName      securityModel securityName
group  gplocal v1          local
group  gplocal v2c        local
group  gplocal usm         local

group  gpred v1           red
group  gpred v2c          red
group  gpred usm          red

####
# Third, create a view for us to let the group have rights
to:
# Make at least snmpwalk -v 1 localhost -c public system fast
again.
#name      incl/excl      subtree          mask(optional)
#view      systemview     included        .1.3.6.1.2.1.1
#view      systemview     included        .1.3.6.1.2.1.25.1.1
view      all      included        .1      80

####
# Finally, grant the group read-only access to the systemview
view.

#group context sec.model sec.level prefix read  write  notif
#access notConfigGroup ""          any          noauth      exact
#systemview none none
access gplocal ""          any          noauth      exact all all all
access gpred ""          any          noauth      exact all all all
```

- Creada la comunidad nac procedemos a levantar el servicio y configurarlo para que inicie con el SO.

```
service snmpd start
chkconfig snmpd on
```

- Para probar el correcto funcionamiento de la comunidad SNMP “nac” que se creó con el siguiente comando.

```
snmpwalk -v 1 172.16.148.57 -c nac system
```

Servidor MYSQL

- La herramienta PacketFence funciona con una base de datos Mysql para eso debemos instalar el servicio con el comando yum.

```
yum install mysql-server mysql.
```

- Se debe levantar el servicio de mysql para la base de datos que va a utilizar la herramienta. Debemos poner contraseña de administración para mysql y configuramos para que siempre inicie el servicio con el sistema operativo.

```
service mysqld start  
mysqladmin -u root password @m@pol@_501  
chkconfig mysqld on
```

Switchs:

- Configuración de SNMP:

Accediendo al switch al que se conectara con PacketFence en modo de configuración realizamos lo siguiente:

```
snmp-server community nac RW 10  
snmp-server enable traps port-security  
snmp-server enable traps port-security trap-rate 1  
snmp-server host 172.16.148.30 version 2c nac port-  
security
```

- Configurando las Interfaces:

Para administrar las interfaces de cada switch se necesita port security en cada interfaz

```

interface FastEthernet0/23
switchport access vlan 80
switchport mode access
switchport port-security maximum 1 vlan access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address 0200.000X.XXX
speed 100
duplex full

```

Nota. X.XXX es el número de ifindex de la interfaz, en este caso sería 1.0023 por la interfaz F 0/23

- **Configuración del Firewall:**

Para que funcione correctamente el portal captivo de la herramienta PacketFence. Se realizó un script para agregar las reglas necesarias para el firewall:

```

#!/bin/sh

##-----LIBERAR REGLAS-----
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t mangle -F

##----POLÍTICA POR DEFECTO DROP (RECHAZAR TODO) -----
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

##-----REGLAS DEL FIREWALL-----

#-----PERMITIR TODO A LOOPBACK-----
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

#-----VLANS PERMITIDAS PARA ACCEDER AL SERVIDOR-----
#Vlan 2
iptables -A INPUT -i eth1.2 -j ACCEPT
iptables -A OUTPUT -o eth1.2 -j ACCEPT
#Vlan 3

```



```

iptables -A INPUT -i eth1.3 -j ACCEPT
iptables -A OUTPUT -o eth1.3 -j ACCEPT
#Vlan 4
iptables -A INPUT -i eth1.4 -j ACCEPT
iptables -A OUTPUT -o eth1.4 -j ACCEPT
#Vlan 5
iptables -A INPUT -i eth1.5 -j ACCEPT
iptables -A OUTPUT -o eth1.5 -j ACCEPT
#Vlan 6
iptables -A INPUT -i eth1.6 -j ACCEPT
iptables -A OUTPUT -o eth1.6 -j ACCEPT
#Vlan 7
iptables -A INPUT -i eth1.7 -j ACCEPT
iptables -A OUTPUT -o eth1.7 -j ACCEPT
#Vlan 8
iptables -A INPUT -i eth1.8 -j ACCEPT
iptables -A OUTPUT -o eth1.8 -j ACCEPT

#-----INTERNET PARA EL SERVIDOR-----
#http
iptables -A INPUT -p tcp -m tcp --sport 80 -m state --state
RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
#https
iptables -A INPUT -p tcp -m tcp --sport 443 -m state --state
RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT

#----CONSULTAS A LOS SERVIDORES DNS DE INTERNET-----

DNS1=200.107.10.52 #Primer Dns externo
DNS2= 200.107.60.58 #Segundo Dns externo

# Permitimos la consulta a un primer DNS desde el firewall
iptables -A INPUT -s $DNS1 -p udp -m udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d $DNS1 -p udp -m udp --dport 53 -j ACCEPT

# Permitimos la consulta a un segundo DNS
iptables -A INPUT -s $DNS2 -p udp -m udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d $DNS2 -p udp -m udp --dport 53 -j ACCEPT

#-----COMUNICACIÓN PARA LAS VLANS-----

#VARIABLES DE LAS VLANS
VLAN2=172.16.144.0/24
VLAN3=172.16.145.0/24
VLAN4=172.16.146.0/24
VLAN5=172.16.147.0/24
VLAN6=172.16.148.0/24

```

VLAN7=172.16.149.0/24
VLAN8=172.16.150.0/24

#FORWARD PARA PERMITIR NAVEGACIÓN POR INTERNET DE LAS VLANS PERMITIDAS
#Las vlans permitidas son de la Vlan 2 a la 8

#-----VLAN 2-----

```
# Forward puerto 80
iptables -t filter -A FORWARD -i eth1.2 -o eth0 -s $VLAN2 -d 0/0 -p
tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.2 -d $VLAN2 -s 0/0 -p
tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
# Forward puerto 53
iptables -t filter -A FORWARD -i eth1.2 -o eth0 -s $VLAN2 -d 0/0 -p
udp --dport 53 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.2 -d $VLAN2 -s 0/0 -p
udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
# Forward puerto 443
iptables -t filter -A FORWARD -i eth1.2 -o eth0 -s $VLAN2 -d 0/0 -p
tcp --dport 443 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.2 -d $VLAN2 -s 0/0 -p
tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT
#Forward a la Vlan de Sistemas
iptables -t filter -A FORWARD -i eth1.2 -o eth1.6 -s $VLAN2 -d $VLAN6
-j ACCEPT
iptables -t filter -A FORWARD -i eth1.6 -o eth1.2 -d $VLAN2 -s $VLAN6
-m state --state RELATED,ESTABLISHED -j ACCEPT
```

#-----VLAN 3-----

```
# Forward puerto 80
iptables -t filter -A FORWARD -i eth1.3 -o eth0 -s $VLAN3 -d 0/0 -p
tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.3 -d $VLAN3 -s 0/0 -p
tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
# Forward puerto 53
iptables -t filter -A FORWARD -i eth1.3 -o eth0 -s $VLAN3 -d 0/0 -p
udp --dport 53 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.3 -d $VLAN3 -s 0/0 -p
udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
# Forward puerto 443
iptables -t filter -A FORWARD -i eth1.3 -o eth0 -s $VLAN3 -d 0/0 -p
tcp --dport 443 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.3 -d $VLAN3 -s 0/0 -p
tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT
#Forward a la Vlan de Sistemas
iptables -t filter -A FORWARD -i eth1.3 -o eth1.6 -s $VLAN3 -d $VLAN6
-j ACCEPT
iptables -t filter -A FORWARD -i eth1.6 -o eth1.3 -d $VLAN3 -s $VLAN6
-m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
#-----VLAN 4-----
```

```
# Forward puerto 80
```

```
iptables -t filter -A FORWARD -i eth1.4 -o eth0 -s $VLAN4 -d 0/0 -p  
tcp --dport 80 -j ACCEPT
```

```
iptables -t filter -A FORWARD -i eth0 -o eth1.4 -d $VLAN4 -s 0/0 -p  
tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
# Forward puerto 53
```

```
iptables -t filter -A FORWARD -i eth1.4 -o eth0 -s $VLAN4 -d 0/0 -p  
udp --dport 53 -j ACCEPT
```

```
iptables -t filter -A FORWARD -i eth0 -o eth1.4 -d $VLAN4 -s 0/0 -p  
udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
# Forward puerto 443
```

```
iptables -t filter -A FORWARD -i eth1.4 -o eth0 -s $VLAN4 -d 0/0 -p  
tcp --dport 443 -j ACCEPT
```

```
iptables -t filter -A FORWARD -i eth0 -o eth1.4 -d $VLAN4 -s 0/0 -p  
tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
#Forward a la Vlan de Sistemas
```

```
iptables -t filter -A FORWARD -i eth1.4 -o eth1.6 -s $VLAN4 -d $VLAN6  
-j ACCEPT
```

```
iptables -t filter -A FORWARD -i eth1.6 -o eth1.4 -d $VLAN4 -s $VLAN6  
-m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
#-----VLAN 5-----
```

```
# Forward puerto 80
```

```
iptables -t filter -A FORWARD -i eth1.5 -o eth0 -s $VLAN5 -d 0/0 -p  
tcp --dport 80 -j ACCEPT
```

```
iptables -t filter -A FORWARD -i eth0 -o eth1.5 -d $VLAN5 -s 0/0 -p  
tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
# Forward puerto 53
```

```
iptables -t filter -A FORWARD -i eth1.5 -o eth0 -s $VLAN5 -d 0/0 -p  
udp --dport 53 -j ACCEPT
```

```
iptables -t filter -A FORWARD -i eth0 -o eth1.5 -d $VLAN5 -s 0/0 -p  
udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
# Forward puerto 443
```

```
iptables -t filter -A FORWARD -i eth1.5 -o eth0 -s $VLAN5 -d 0/0 -p  
tcp --dport 443 -j ACCEPT
```

```
iptables -t filter -A FORWARD -i eth0 -o eth1.5 -d $VLAN5 -s 0/0 -p  
tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
#Forward a la Vlan de Sistemas
```

```
iptables -t filter -A FORWARD -i eth1.5 -o eth1.6 -s $VLAN5 -d $VLAN6  
-j ACCEPT
```

```
iptables -t filter -A FORWARD -i eth1.6 -o eth1.5 -d $VLAN5 -s $VLAN6  
-m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
#-----VLAN 6-----
```

```
# Forward puerto 80
```

```
iptables -t filter -A FORWARD -i eth1.6 -o eth0 -s $VLAN6 -d 0/0 -p  
tcp --dport 80 -j ACCEPT
```

```
iptables -t filter -A FORWARD -i eth0 -o eth1.6 -d $VLAN6 -s 0/0 -p  
tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
# Forward puerto 53
iptables -t filter -A FORWARD -i eth1.6 -o eth0 -s $VLAN6 -d 0/0 -p
udp --dport 53 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.6 -d $VLAN6 -s 0/0 -p
udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
# Forward puerto 443
iptables -t filter -A FORWARD -i eth1.6 -o eth0 -s $VLAN6 -d 0/0 -p
tcp --dport 443 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.6 -d $VLAN6 -s 0/0 -p
tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT
# Forward puerto 1863 (Messenger)
iptables -t filter -A FORWARD -i eth1.6 -o eth0 -s $VLAN6 -d 0/0 -p
tcp --dport 1863 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.6 -d $VLAN6 -s 0/0 -p
tcp --sport 1863 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
#-----VLAN 7-----
```

```
# Forward puerto 80
iptables -t filter -A FORWARD -i eth1.7 -o eth0 -s $VLAN7 -d 0/0 -p
tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.7 -d $VLAN7 -s 0/0 -p
tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
# Forward puerto 53
iptables -t filter -A FORWARD -i eth1.7 -o eth0 -s $VLAN7 -d 0/0 -p
udp --dport 53 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.7 -d $VLAN7 -s 0/0 -p
udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
# Forward puerto 443
iptables -t filter -A FORWARD -i eth1.7 -o eth0 -s $VLAN7 -d 0/0 -p
tcp --dport 443 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.7 -d $VLAN7 -s 0/0 -p
tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT
#Forward a la Vlan de Sistemas
iptables -t filter -A FORWARD -i eth1.7 -o eth1.6 -s $VLAN7 -d $VLAN6
-j ACCEPT
iptables -t filter -A FORWARD -i eth1.6 -o eth1.7 -d $VLAN7 -s $VLAN6
-m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
#-----VLAN 8-----
```

```
# Forward puerto 80
iptables -t filter -A FORWARD -i eth1.8 -o eth0 -s $VLAN8 -d 0/0 -p
tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.8 -d $VLAN8 -s 0/0 -p
tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT
# Forward puerto 53
iptables -t filter -A FORWARD -i eth1.8 -o eth0 -s $VLAN8 -d 0/0 -p
udp --dport 53 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.8 -d $VLAN8 -s 0/0 -p
udp --sport 53 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```

# Forward puerto 443
iptables -t filter -A FORWARD -i eth1.8 -o eth0 -s $VLAN8 -d 0/0 -p
tcp --dport 443 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1.8 -d $VLAN8 -s 0/0 -p
tcp --sport 443 -m state --state RELATED,ESTABLISHED -j ACCEPT
#Forward a la Vlan de Sistemas
iptables -t filter -A FORWARD -i eth1.8 -o eth1.6 -s $VLAN8 -d $VLAN6
-j ACCEPT
iptables -t filter -A FORWARD -i eth1.6 -o eth1.8 -d $VLAN8 -s $VLAN6
-m state --state RELATED,ESTABLISHED -j ACCEPT

#---PERMITIR REENVIÓ DEL SQUID-----

#Permitir el proxy, necesario después del reenvío.

#-----VLAN 2-----
iptables -t filter -A INPUT -p tcp --dport 3128 -i eth1.2 -s $VLAN2 -j
ACCEPT
iptables -t filter -A OUTPUT -p tcp --sport 3128 -o eth1.2 -d $VLAN2 -
m state --state RELATED,ESTABLISHED -j ACCEPT

#-----VLAN 3-----
iptables -t filter -A INPUT -p tcp --dport 3128 -i eth1.3 -s $VLAN3 -j
ACCEPT
iptables -t filter -A OUTPUT -p tcp --sport 3128 -o eth1.3 -d $VLAN3 -
m state --state RELATED,ESTABLISHED -j ACCEPT

#-----VLAN 4-----
iptables -t filter -A INPUT -p tcp --dport 3128 -i eth1.4 -s $VLAN4 -j
ACCEPT
iptables -t filter -A OUTPUT -p tcp --sport 3128 -o eth1.4 -d $VLAN4 -
m state --state RELATED,ESTABLISHED -j ACCEPT

#-----VLAN 5-----
iptables -t filter -A INPUT -p tcp --dport 3128 -i eth1.5 -s $VLAN5 -j
ACCEPT
iptables -t filter -A OUTPUT -p tcp --sport 3128 -o eth1.5 -d $VLAN5 -
m state --state RELATED,ESTABLISHED -j ACCEPT

#-----VLAN 6-----
iptables -t filter -A INPUT -p tcp --dport 3128 -i eth1.6 -s $VLAN6 -j
ACCEPT
iptables -t filter -A OUTPUT -p tcp --sport 3128 -o eth1.6 -d $VLAN6 -
m state --state RELATED,ESTABLISHED -j ACCEPT

#-----VLAN 7-----
iptables -t filter -A INPUT -p tcp --dport 3128 -i eth1.7 -s $VLAN7 -j
ACCEPT
iptables -t filter -A OUTPUT -p tcp --sport 3128 -o eth1.7 -d $VLAN7 -
m state --state RELATED,ESTABLISHED -j ACCEPT

```

```

#-----VLAN 8-----
iptables -t filter -A INPUT -p tcp --dport 3128 -i eth1.8 -s $VLAN8 -j
ACCEPT
iptables -t filter -A OUTPUT -p tcp --sport 3128 -o eth1.8 -d $VLAN8 -
m state --state RELATED,ESTABLISHED -j ACCEPT

#-----NAVEGACIÓN DEL SQUID-----
#Permitir a squid salida.
iptables -A INPUT -p tcp -m tcp --sport 3128 -m state --state
RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 3128 -j ACCEPT

#CONFIGURACIÓN DEL FIREWALL PARA LAS VLANS de NAC
VLAN70=172.16.153.0/24
VLAN80=172.16.158.0/24
IPVLAN70=172.16.153.1
IPVLAN80=172.16.158.1

#Aceptar consultas dns, http y https de las Vlan's 70 y 80

#puerto 53 (dns)
iptables -A INPUT -p udp -m udp --dport 53 -s $VLAN70 -d $IPVLAN70 -i
eth2 -j ACCEPT
iptables -A OUTPUT -p udp -m udp --sport 53 -s $IPVLAN70 -d $VLAN70 -o
eth2 -j ACCEPT
#puerto 80
iptables -A INPUT -p tcp -m tcp --dport 80 -s $VLAN70 -d $IPVLAN70 -i
eth2 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --sport 80 -s $IPVLAN70 -d $VLAN70 -o
eth2 -j ACCEPT
#puerto 443
iptables -A INPUT -p tcp -m tcp --dport 443 -s $VLAN70 -d $IPVLAN70 -i
eth2 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --sport 443 -s $IPVLAN70 -d $VLAN70 -
o eth2 -j ACCEPT
#Vlan 80
#puerto 53(dns)
iptables -A INPUT -p udp -m udp --dport 53 -s $VLAN80 -d $IPVLAN80 -i
eth3 -j ACCEPT
iptables -A OUTPUT -p udp -m udp --sport 53 -s $IPVLAN80 -d $VLAN80 -o
eth3 -j ACCEPT
#puerto 80
iptables -A INPUT -p tcp -m tcp --dport 80 -s $VLAN80 -d $IPVLAN80 -i
eth3 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --sport 80 -s $IPVLAN80 -d $VLAN80 -o
eth3 -j ACCEPT
#puerto 443
iptables -A INPUT -p tcp -m tcp --dport 443 -s $VLAN80 -d $IPVLAN80 -i
eth3 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --sport 443 -s $IPVLAN80 -d $VLAN80 -
o eth3 -j ACCEPT

```

```

#-----CONFIGURACIÓN DE NAT PARA SQUID-----
SQUIDIP=190.152.182.53 # IP de internet

#Nat de Internet hacia la Red Interna de los puertos http(80) y
https(443)
iptables -t nat -A PREROUTING -s $$SQUIDIP -p tcp --dport 80 -j ACCEPT
iptables -t nat -A PREROUTING -s $$SQUIDIP -p tcp --dport 443 -j ACCEPT

#Ruteo de las Red Internas con peticiones http (80)
iptables -t nat -A PREROUTING -s $VLAN2 -p tcp --dport 80 -j DNAT --
to-destination $$SQUIDIP:3128
iptables -t nat -A PREROUTING -s $VLAN3 -p tcp --dport 80 -j DNAT --
to-destination $$SQUIDIP:3128
iptables -t nat -A PREROUTING -s $VLAN4 -p tcp --dport 80 -j DNAT --
to-destination $$SQUIDIP:3128
iptables -t nat -A PREROUTING -s $VLAN5 -p tcp --dport 80 -j DNAT --
to-destination $$SQUIDIP:3128
iptables -t nat -A PREROUTING -s $VLAN6 -p tcp --dport 80 -j DNAT --
to-destination $$SQUIDIP:3128
iptables -t nat -A PREROUTING -s $VLAN7 -p tcp --dport 80 -j DNAT --
to-destination $$SQUIDIP:3128
iptables -t nat -A PREROUTING -s $VLAN8 -p tcp --dport 80 -j DNAT --
to-destination $$SQUIDIP:3128

#Enmascaramiento de las redes internas con permisos de salida a
Internet
iptables -t nat -A POSTROUTING -s $VLAN2 -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s $VLAN3 -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s $VLAN4 -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s $VLAN5 -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s $VLAN6 -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s $VLAN7 -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s $VLAN8 -o eth0 -j MASQUERADE

#Negar el resto peticiones a squid (3128)
iptables -t mangle -A PREROUTING -p tcp --dport 3128 -j DROP

```

2. INSTALACIÓN

Para proceder a la instalación de la herramienta tenemos que seguir los siguientes pasos:

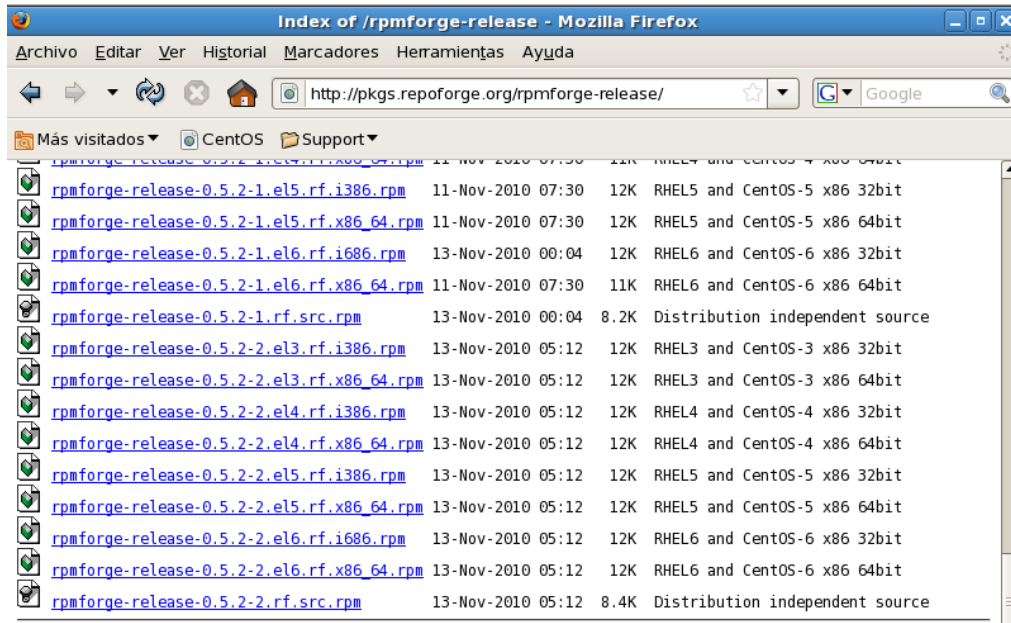
- Importamos la key o llave para poder realizar las descargas del repositorio de DAG el cual contiene un sin número de programas pero el nos interesa es la herramienta Packetfence.

```
wget http://dag.wieers.com/rpm/packages/RPM-GPG-KEY.dag.txt
```

```
rpm --import RPM-GPG-KEY.dag.txt
```

- Descargamos el paquete rpmforge de la siguiente página web. Para nuestro caso utilizamos el paquete rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm.

<http://dag.wieers.com/rpm/packages/rpmforge-release/>



- Instalar el paquete rpmforge.

```
rpm -ivh rpmforge-release-0.5.2-2.el5.rf.x86_64.rpm
```

- Deshabilitar el repositorio por defecto

```
gedit/etc/yum.repos.d/rpmforge.repo
```



```
### Name: RPMforge RPM Repository for RHEL 5 - dag
### URL: http://rpmforge.net/
[rpmforge]
name = RHEL $releasever - RPMforge.net - dag
baseurl = http://apt.sw.be/redhat/el5/en/$basearch/rpmforge
mirrorlist = http://apt.sw.be/redhat/el5/en/mirrors-rpmforge
#mirrorlist = file:///etc/yum.repos.d/mirrors-rpmforge
enabled = 0
protect = 0
gpgkey = file:///etc/pki/rpm-gpg/RPM-GPG-KEY-rpmforge-dag
gpgcheck = 1

[rpmforge-extras]
name = RHEL $releasever - RPMforge.net - extras
baseurl = http://apt.sw.be/redhat/el5/en/$basearch/extras
mirrorlist = http://apt.sw.be/redhat/el5/en/mirrors-rpmforge-extras
#mirrorlist = file:///etc/yum.repos.d/mirrors-rpmforge-extras
enabled = 0
```

- También debemos instalar los repositorios de EPEL

```
rpm -Uvh
http://download.fedora.redhat.com/pub/epel/5/i386/epel-
release-5-4.noarch.rpm
```

- Crear el repositorio para la instalación de Packetfence

```
gedit/etc/yum.repos.d/PackageFence.repo
```

- Dentro del archivo creamos el repositorio poniendo las siguientes líneas:

```
[PackageFence]
name=PackageFence Repository
baseurl=http://inverse.ca/downloads/PackageFence/CentOS5/
$basearch
gpgcheck=0
enabled=0
```

- Instalamos PacketFence mediante la herramienta yum de Centos:

```
yum groupinstall --enablerepo=PackageFence,rpmforge
Packetfence-complete
```

Esto instalara PacketFence con todas las dependencias necesarias para que esta funcione.

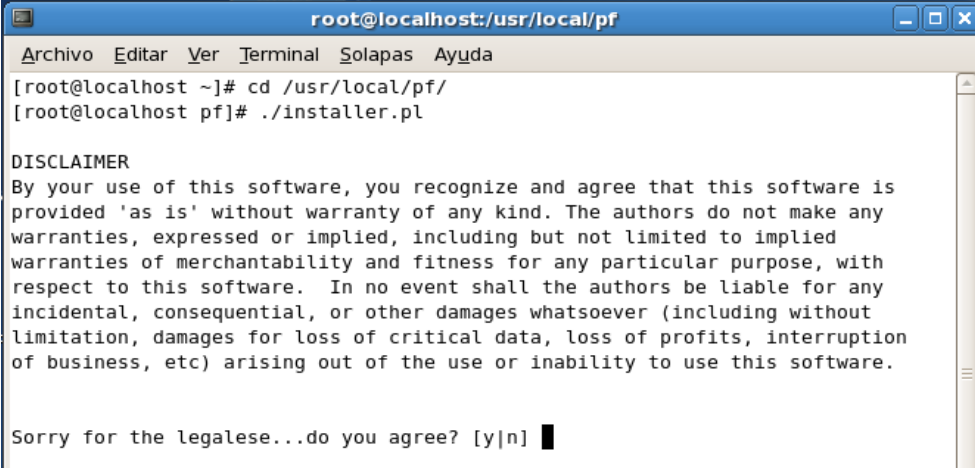
- Accedemos al directorio de PacketFence

```
cd /usr/local/pf/
```

- Completamos la instalación ejecutando el archivo

```
./installer.pl
```

- Al ejecutar el script veremos la siguiente captura en la que renunciamos a pedir garantía por datos perdidos por el uso del software.



```
root@localhost:~/usr/local/pf
Archivo Editar Ver Terminal Solapas Ayuda
[root@localhost ~]# cd /usr/local/pf/
[root@localhost pf]# ./installer.pl

DISCLAIMER
By your use of this software, you recognize and agree that this software is
provided 'as is' without warranty of any kind. The authors do not make any
warranties, expressed or implied, including but not limited to implied
warranties of merchantability and fitness for any particular purpose, with
respect to this software. In no event shall the authors be liable for any
incidental, consequential, or other damages whatsoever (including without
limitation, damages for loss of critical data, loss of profits, interruption
of business, etc) arising out of the use or inability to use this software.

Sorry for the legalese...do you agree? [y|n] █
```

- El siguiente paso es aceptar la creación de la base de datos de PacketFence (Por este motivo hay que iniciar y configurar el servicio de mysql previamente).

```
root@localhost:~/usr/local/pf
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost ~]# cd /usr/local/pf/
[root@localhost pf]# ./installer.pl

DISCLAIMER
By your use of this software, you recognize and agree that this software is
provided 'as is' without warranty of any kind. The authors do not make any
warranties, expressed or implied, including but not limited to implied
warranties of merchantability and fitness for any particular purpose, with
respect to this software. In no event shall the authors be liable for any
incidental, consequential, or other damages whatsoever (including without
limitation, damages for loss of critical data, loss of profits, interruption
of business, etc) arising out of the use or inability to use this software.

Sorry for the legalese...do you agree? [y|n] y

Please note that the ARP-based registration code is currently disabled.

PacketFence requires a MySQL server as a backend. Would you like to create or v
erify the database now? [y|n] 
```

```
root@localhost:~/usr/local/pf
Archivo  Editar  Ver  Terminal  Solapas  Ayuda

DISCLAIMER
By your use of this software, you recognize and agree that this software is
provided 'as is' without warranty of any kind. The authors do not make any
warranties, expressed or implied, including but not limited to implied
warranties of merchantability and fitness for any particular purpose, with
respect to this software. In no event shall the authors be liable for any
incidental, consequential, or other damages whatsoever (including without
limitation, damages for loss of critical data, loss of profits, interruption
of business, etc) arising out of the use or inability to use this software.

Sorry for the legalese...do you agree? [y|n] y

Please note that the ARP-based registration code is currently disabled.

PacketFence requires a MySQL server as a backend. Would you like to create or v
erify the database now? [y|n] y
  MySQL Host [localhost]:
  MySQL Port [3306]:
  Database Name [pf]:
  Current Admin User [root]:
  Current Admin Password:
  PF needs to create the PF database - is that ok? [y|n] 
```

```
root@localhost:/usr/local/pf
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
warranties of merchantability and fitness for any particular purpose, with
respect to this software.  In no event shall the authors be liable for any
incidental, consequential, or other damages whatsoever (including without
limitation, damages for loss of critical data, loss of profits, interruption
of business, etc) arising out of the use or inability to use this software.

Sorry for the legalese...do you agree? [y|n] y

Please note that the ARP-based registration code is currently disabled.

PacketFence requires a MySQL server as a backend.  Would you like to create or v
erify the database now? [y|n] y
  MySQL Host [localhost]:
  MySQL Port [3306]:
Database Name [pf]:
  Current Admin User [root]:
  Current Admin Password:
PF needs to create the PF database - is that ok? [y|n] y
  Loading schema
Do you want to create a database user to access the PF database now? [y|n] y
Username [pf]:
  Password:
  Confirm:
```

- Después pide la creación de certificados digitales para las páginas web de administración y configuración de PacketFence.

```
root@localhost:/usr/local/pf
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
Compiling message catalogue (118n)
  language fr
  language he_IL
  language de
  language it
  language pt_BR
  language nl
  language en
  language es
Would you like me to create a self-signed SSL certificate for the PacketFence web
pages? [y|n] y
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'newkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:
```

- El siguiente paso son datos opcionales sobre todo informativos

```

root@localhost:/usr/local/pf
Archivo Editar Ver Terminal Solapas Ayuda
language es
Would you like me to create a self-signed SSL certificate for the PacketFence web
pages? [y|n] y
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'newkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:EC
State or Province Name (full name) [Berkshire]:Chimborazo
Locality Name (eg, city) [Newbury]:Riobamba
Organization Name (eg, company) [My Company Ltd]:CNJ
Organizational Unit Name (eg, section) []:Unidad Informatica
Common Name (eg, your name or your server's hostname) []:pf
Email Address []:c.palmay@funcionjudicial-chimborazo.gob.ec
Would you like me to create an account for the web administrative interface?
** NOTE: this will overwrite any existing accounts ** [y|n] 

```

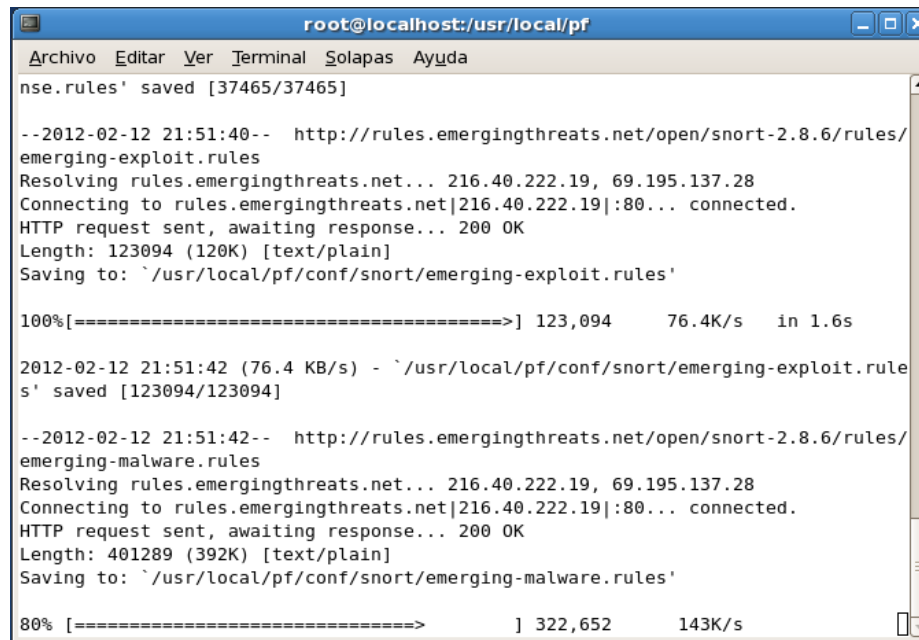
- Continuando con la ejecución del script debemos configurar el usuario administrador.

```

root@localhost:/usr/local/pf
Archivo Editar Ver Terminal Solapas Ayuda
writing new private key to 'newkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:EC
State or Province Name (full name) [Berkshire]:Chimborazo
Locality Name (eg, city) [Newbury]:Riobamba
Organization Name (eg, company) [My Company Ltd]:CNJ
Organizational Unit Name (eg, section) []:Unidad Informatica
Common Name (eg, your name or your server's hostname) []:pf
Email Address []:c.palmay@funcionjudicial-chimborazo.gob.ec
Would you like me to create an account for the web administrative interface?
** NOTE: this will overwrite any existing accounts ** [y|n] y
Username [admin]:
New password:
Re-type new password:
Adding password for user admin
Do you want me to download the latest Emergingthreats rule files ? This is only n
ecessary if you intent to use Snort. [y|n] 

```

- El siguiente paso es actualizar las amenazas que puede detectar la herramienta snort.



```
root@localhost:/usr/local/pf
Archivo Editar Ver Terminal Solapas Ayuda
nse.rules' saved [37465/37465]

--2012-02-12 21:51:40-- http://rules.emergingthreats.net/open/snort-2.8.6/rules/
emerging-exploit.rules
Resolving rules.emergingthreats.net... 216.40.222.19, 69.195.137.28
Connecting to rules.emergingthreats.net|216.40.222.19|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 123094 (120K) [text/plain]
Saving to: `'/usr/local/pf/conf/snort/emerging-exploit.rules'

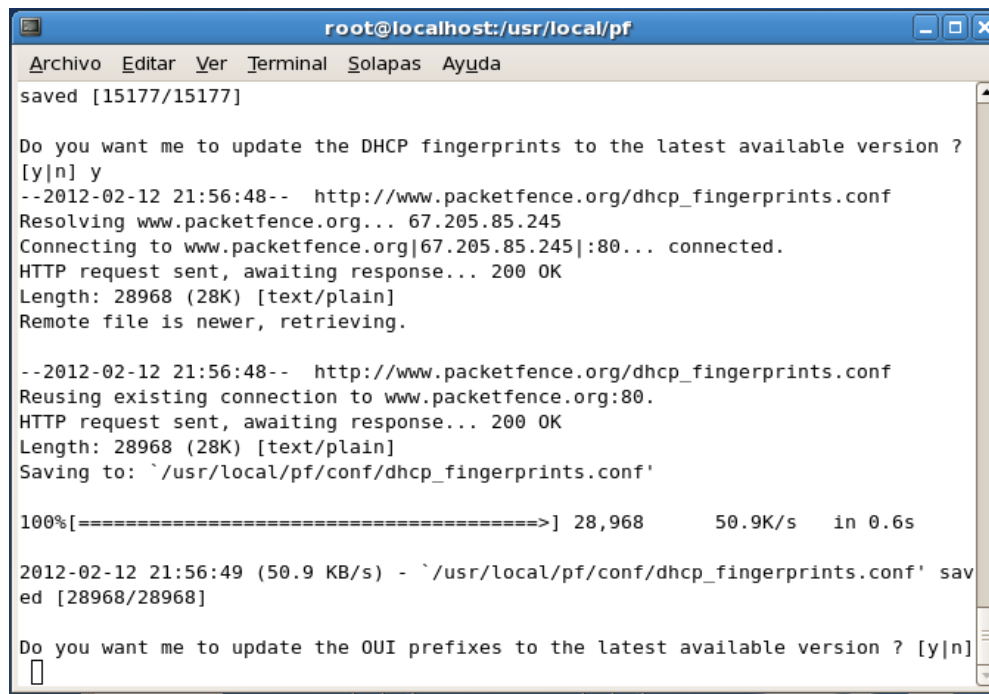
100%[=====] 123,094 76.4K/s in 1.6s

2012-02-12 21:51:42 (76.4 KB/s) - `'/usr/local/pf/conf/snort/emerging-exploit.rules'
s' saved [123094/123094]

--2012-02-12 21:51:42-- http://rules.emergingthreats.net/open/snort-2.8.6/rules/
emerging-malware.rules
Resolving rules.emergingthreats.net... 216.40.222.19, 69.195.137.28
Connecting to rules.emergingthreats.net|216.40.222.19|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 401289 (392K) [text/plain]
Saving to: `'/usr/local/pf/conf/snort/emerging-malware.rules'

80%[=====] 322,652 143K/s
```

- Actualizamos el listado de los diferentes tipos de Sistemas operativos que se pueden detectar con DHCP.



```
root@localhost:/usr/local/pf
Archivo Editar Ver Terminal Solapas Ayuda
saved [15177/15177]

Do you want me to update the DHCP fingerprints to the latest available version ?
[y|n] y
--2012-02-12 21:56:48-- http://www.packetfence.org/dhcp_fingerprints.conf
Resolving www.packetfence.org... 67.205.85.245
Connecting to www.packetfence.org|67.205.85.245|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 28968 (28K) [text/plain]
Remote file is newer, retrieving.

--2012-02-12 21:56:48-- http://www.packetfence.org/dhcp_fingerprints.conf
Reusing existing connection to www.packetfence.org:80.
HTTP request sent, awaiting response... 200 OK
Length: 28968 (28K) [text/plain]
Saving to: `'/usr/local/pf/conf/dhcp_fingerprints.conf'

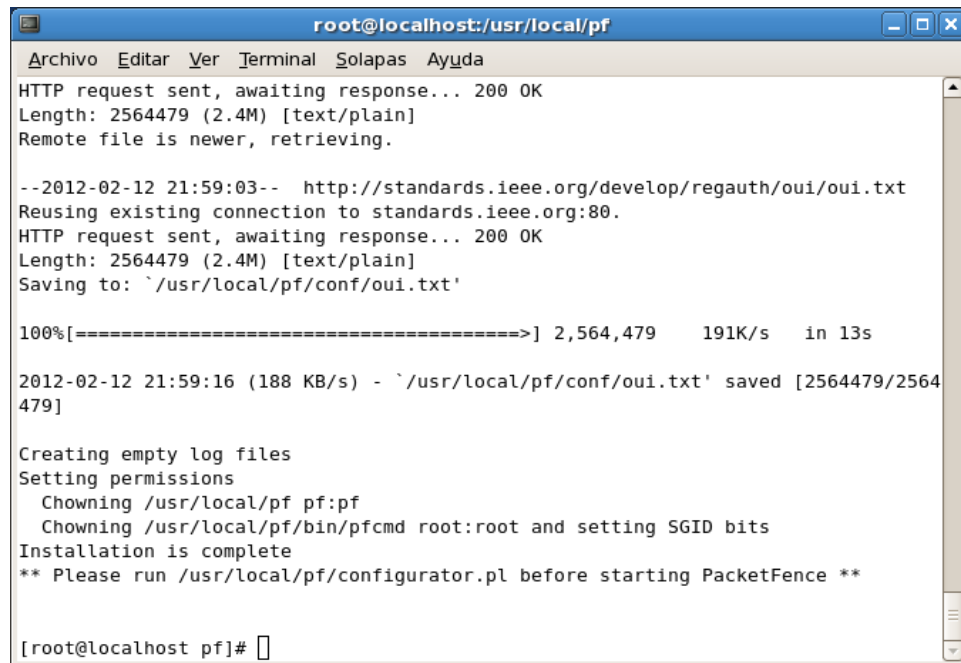
100%[=====] 28,968 50.9K/s in 0.6s

2012-02-12 21:56:49 (50.9 KB/s) - `'/usr/local/pf/conf/dhcp_fingerprints.conf' sav
ed [28968/28968]

Do you want me to update the OUI prefixes to the latest available version ? [y|n]

```

- En el siguiente paso se actualiza los prefijos OUI y con este paso finalizamos con el script de instalación de PacketFence.



```
root@localhost:/usr/local/pf
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
HTTP request sent, awaiting response... 200 OK
Length: 2564479 (2.4M) [text/plain]
Remote file is newer, retrieving.

--2012-02-12 21:59:03-- http://standards.ieee.org/develop/regauth/oui/oui.txt
Reusing existing connection to standards.ieee.org:80.
HTTP request sent, awaiting response... 200 OK
Length: 2564479 (2.4M) [text/plain]
Saving to: `/usr/local/pf/conf/oui.txt'

100%[=====>] 2,564,479    191K/s   in 13s

2012-02-12 21:59:16 (188 KB/s) - `/usr/local/pf/conf/oui.txt' saved [2564479/2564479]

Creating empty log files
Setting permissions
  Chowning /usr/local/pf pf:pf
  Chowning /usr/local/pf/bin/pfcmd root:root and setting SGID bits
Installation is complete
** Please run /usr/local/pf/configurator.pl before starting PacketFence **

[root@localhost pf]#
```

3. Configuración de la herramienta

- Ejecutamos el script para configurar la herramienta ubicada en el directorio raíz de la herramienta.

```
./configurator.pl
```

```

root@localhost:usr/local/pf
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@localhost pf]# ./configurator.pl
Checking for existing PacketFence configuration file...
No existing PacketFence configuration files found; configuring...

Entering PacketFence configuration mode... Be prepared...

The following configuration script will help you configure PacketFence using some
basic predefined templates.
Once done, your PacketFence installation will be fully functional (if everything's
go as expected) and will be ready to use. For more advanced configurations, don't
be shy to take a look at the main configuration file (/usr/local/pf/conf/pf.conf)
and its documentation file /usr/local/pf/conf/documentation.conf

Here are the steps that will be performed:
- Choice of configuration template and enforcement method
- General configuration of the PacketFence server
- Configuration of enforcement networks

*** Please note that the following configuration script can be a bit tedious. If
you get bored, just leave and edit /usr/local/pf/conf/pf.conf directly. ***

```

- El siguiente paso es elegir qué tipo de configuración queremos; para nuestro caso utilizamos la opción template (plantilla) y la opción de registro y detección.

```

[root@pf pf]# ./configurator.pl
Checking existing configuration...
No existing configuration found
Would you like to use a template configuration or custom [t|c] t
Which template would you like:
 1) ARP mode in Testing
 2) ARP mode with Registration
 3) ARP mode with Detection (snort)
 4) ARP mode with Registration and Detection (snort)
 5) ARP mode with Registration, Detection (snort) & Scanning (nessus)
 6) ARP mode with Session-based Authentication
 7) VLAN isolation mode with Registration
 8) VLAN isolation mode with Registration and Detection (snort)
 9) VLAN isolation mode ready for PacketFence ZEN
[1|2|3|4|5|6|7|8|9] 8

```

- El siguiente paso es la configuración general. Primero establecemos el Nombre del Dominio y el nombre del Host.

GENERAL CONFIGURATION

```

DNS Domain Name (current: justiciariobamba.gov.ec, default: example.com [?]):
justiciariobamba.gov.ec - ok? [y|n] y
Host Name (without DNS domain name) (current: pf, default: abc [?]): █

```

- Luego se configura los servidores DNS y DHCP existentes en la red la institución.


```
DNS Servers including PacketFence (comma delimited) (current: 200.107.10.52,200.107.60.58, default: 127.0.0.1 [?]): 200.107.10.52,200.107.60.58,127.0.0.1
200.107.10.52,200.107.60.58,127.0.0.1 - ok? [y|n] y
DHCP Servers including PacketFence (comma delimited) (default: 127.0.0.1 [?]): 127.0.0.1,172.16.148.1
127.0.0.1,172.16.148.1 - ok? [y|n] y
Your isolation mode is vlan. If you are interested in SNMP trap statistics please create the following crontab entry
```

- Enseguida nos pide la interface de red que vamos a utilizar para administración de la herramienta.

```
* /5 * * * * /usr/local/pf/bin/pfcmd traplog update
What is my management interface? (default: <NONE>) [eth3|eth2|eth1|eth0|?]: eth1
eth1 - ok? [y|n] y
What is its IP address? (current: 172.16.148.30, default: <NONE> [?]):
172.16.148.30 - ok? [y|n] y
What is its mask? (current: 255.255.255.0, default: <NONE> [?]):
255.255.255.0 - ok? [y|n] y
What is my gateway? (current: 172.16.148.1, default: <NONE> [?]): 172.16.148.254
172.16.148.254 - ok? [y|n] y
```

- El siguiente paso es configurar los parámetros de la red de registro.

DHCP AND DNS CONFIGURATION FOR REGISTRATION NETWORK

```
What is the REGISTRATION network prefix (ex: 192.168.1.0)? (default: <NONE> [?]): 172.16.158.0
172.16.158.0 - ok? [y|n] y
What is the REGISTRATION network mask (ex: 255.255.255.0)? (default: <NONE> [?]): 255.255.255.0
255.255.255.0 - ok? [y|n] y
What is the IP address of PacketFence in the REGISTRATION network? (default: <NONE> [?]): 172.16.158.2
172.16.158.2 - ok? [y|n] y
What is the REGISTRATION network DHCP scope starting address? (default: <NONE> [?]): 172.16.158.11
172.16.158.11 - ok? [y|n] y
What is the REGISTRATION network DHCP scope ending address? (default: <NONE> [?]): 172.16.158.253
172.16.158.253 - ok? [y|n] y
```

- Continuando se configura los parámetro de la red de cuarentena.

DHCP AND DNS CONFIGURATION FOR ISOLATION NETWORK

```
What is the ISOLATION network prefix (ex: 192.168.1.0)? (default: <NONE> [?]): 172.16.153.0
172.16.153.0 - ok? [y|n] y
What is the ISOLATION network mask (ex: 255.255.255.0)? (default: <NONE> [?]): 255.255.255.0
255.255.255.0 - ok? [y|n] y
What is the IP address of PacketFence in the ISOLATION network? (default: <NONE> [?]): 172.16.153.2
172.16.153.2 - ok? [y|n] y
What is the ISOLATION network DHCP scope starting address? (default: <NONE> [?]): 172.16.153.11
172.16.153.11 - ok? [y|n] y
What is the ISOLATION network DHCP scope ending address? (default: <NONE> [?]): 172.16.153.253
172.16.153.253 - ok? [y|n] y
```

- Por último se configura las la interfaz de para la captura de dispositivos de red y las notificaciones que envía la herramienta.

TRAPPING CONFIGURATION

```
What is my monitor interface? (default: <NONE>) [eth3|eth2|eth1|eth0|?]: eth1
eth1 - ok? [y|n] y
```

ALERTING CONFIGURATION

```
Where would you like notifications of traps, rogue DHCP servers, and other sundry goods sent? (default: pf@localhost [?]): cristina_palmay@hotmail.com
cristina_palmay@hotmail.com - ok? [y|n] y
What should I use as my SMTP relay server? (default: localhost [?]):
localhost - ok? [y|n] y
Please review conf/pf.conf and conf/networks.conf to correct any errors or change pathing to daemons
After starting PF, use bin/pfcmd or the web interface (https://pf.justiciariobamba.gov.ec:1443) to administer the system
Committing settings...
Enjoy!
[root@pf pf]# █
```

4. Configuración de los archivos de configuración

- Crear o cambiar un usuario para administrar la interfaz web:

```
htpasswd /usr/local/pf/conf/admin.conf admin
```

- Agregar la conexión de la BD al archivo de configuración:

El archivo de configuración general

```
/usr/local/pf/conf/pf.conf
```

Se agrega las líneas de Conexión a la BD:

```
[database]
pass=123456
db=pf
user=pf
port=3306
host=localhost
```

- Levantamos el servicio de packetfence y para que inicie:

```
service packetfence start
```

Selección del modo de registro:

Por defecto es local (por medio de un archivo plano), si se desea puede ser por otros métodos como se muestra en la imagen:

- Definición de Switchs:

Se puede hacer por interfaz web o configurar el archivo:

```
/usr/local/pf/conf/switches.conf
```

En este archivo se agregan los switchs con los que se desea trabajar. Así:

```
[172.16.148.57]
type=Cisco::Catalyst_2960
mode=production
vlans=2,3,4,5,6,8,70,80
normalVlan=6
registrationVlan=80
isolationVlan=70
macDetectionVlan=6
guestVlan=80
customVlan1=2
customVlan2=3
customVlan3=4
customVlan4=5
customVlan5=8
cliPwd=tulipan
cliEnablePwd=tulipan
SNMPVersionTrap=2c
SNMPCommunityTrap=nac
SNMPVersion=2c
SNMPCommunityRead=nac
```

```
SNMPCommunityWrite=nac
uplink=10018,10019,10020,10021,10022,10024,10025,10046,1
0101,10102
```

Configuración del DNS:

El servidor DNS no se configura como se debe tiene un bug por lo tanto nos toca configurar manualmente para lo cual nos ubicamos en la carpeta donde se encuentran los archivos de configuración:

```
/usr/local/pf/conf/named-isolation.ca
/usr/local/pf/conf/named-registration.ca
```

Configuramos los archivos named de acuerdo a nuestras redes:

- DNS de Cuarentena:

```
; Isolation network DNS configuration
; This file is manipulated on PacketFence's startup before
being given to named
$TTL 3600
. IN SOA %%hostname%%. %%incharge%% (
2009020901 ; serial
    10800      ; refresh
    3600       ; retry
    604800    ; expire
    86400     ; default_ttl
)
IN      NS      %%hostname%%.
*.      IN      A      172.16.153.1
IN      MX      5      %%hostname%%.

1.153.16.172.in-addr.arpa.      IN      PTR      %%hostname%%
```

- DNS de la red de Registro:

```
; Registration network DNS configuration
; This file is manipulated on PacketFence's startup before
being given to named
$TTL 3600
. IN SOA %%hostname%%. %%incharge%% (
2009020901 ; serial
    10800      ; refresh
    3600       ; retry
    604800    ; expire
    86400     ; default_ttl
)

```

```

IN      NS      %%hostname%%.
*.      IN      A      172.16.158.1
IN      MX      5      %%hostname%%.

1.158.16.172.in-addr.arpa.      IN      PTR      %%hostname%%

```

- Asignación de Vlans según la categoría en la que se encuentre el equipo:

Para esto debemos editar el archivo de configuración

`/usr/local/pf/lib/pf/vlan/custom.pm`

Este archivo modificamos de acuerdo a las VLAN's necesarias.

```

#Codigo para asignar vlans
sub getNormalVlan {my ($this, $switch, $ifIndex, $mac,
$node_info, $connection_type, $user_name, $ssid) = @_;
my $logger = Log::Log4perl->get_logger();

# Asignacion de vlans por categoria
if (defined($node_info->{'category'}) && lc($node_info->
{'category'}) eq "penales") {
return $switch->getVlanByName('customVlan1');
}
if (defined($node_info->{'category'}) && lc($node_info->
{'category'}) eq "ninez") {
return $switch->getVlanByName('customVlan2');
}
if (defined($node_info->{'category'}) && lc($node_info->
{'category'}) eq "apoyo") {
return $switch->getVlanByName('customVlan3');
}
if (defined($node_info->{'category'}) && lc($node_info->
{'category'}) eq "civiles") {
return $switch->getVlanByName('customVlan4');
}
if (defined($node_info->{'category'}) && lc($node_info->
{'category'}) eq "otrosjuzgados")
{
return $switch->getVlanByName('customVlan5');
}
return $switch->getVlanByName('normalVlan');#si la vlan no
está en una categoria especifica vlan 6
}

```

- Agregar Usuarios a un archivo plano para el registro:

Para agregar un usuario debemos ejecutar el siguiente comando

Para el primer usuario se crea así, debido a que se necesita crear el archivo.

```
htpasswd -c /usr/local/pf/conf/user.conf newuser
```

Los siguientes usuarios solamente de esta manera

```
htpasswd /usr/local/pf/conf/user.conf newuser
```

- Configurar el Idioma a español en Apache:

En el archivo de configuración `/usr/local/pf/conf/httpd.conf`

Debemos modificar la siguiente línea:

```
AddDefaultCharset ISO-8859-1
```

Por lo siguiente

```
AddDefaultCharset UTF-8
```

Y agregar la siguiente línea

```
DefaultLanguage es
```

Después de

```
DirectoryIndex index.html index.cgi index.php
```

- Registro de Sucesos

Los archivos de registros de sucesos o archivos logs de packetfence son los siguientes:

`/usr/local/pf/logs/packetfence.log` – Sucesos de el demonio pf

`/usr/local/pf/logs/access_log` – Apache – Registro de acceso al Portal captivo

`/usr/local/pf/logs/error_log` – Apache – Registros de error al portal captivo

`/usr/local/pf/logs/admin_access_log` – Apache – Web Admin/Services Access Log

`/usr/local/pf/logs/admin_error_log` – Apache – Web Admin/Services Error Log

`/usr/local/pf/logs/admin_debug_log` – Apache – Web Admin Debug Log

ANEXO D

NESSUS Y PACKETFENCE

1. Instalando Nessus

Para que la herramienta Nessus funcione correctamente necesitamos instalar Adobe Flash Player sino lo tenemos instalado.

- Instalar Adobe Flash Player

Lo descargamos de la página oficial y lo instalamos:

```
rpm -ivh flash-plugin-10.3.181.34-release.i386.rpm
```

- Descargamos el rpm de Nessus de la página

```
http://www.tenable.com/products/nessus/select-your-operating-system
```

- Instalamos Nessus

```
rpm -ivh Nessus-4.4.1-es5.x86_64.rpm
```

```
[root@pf ~]# rpm -ivh Nessus-4.4.1-es5.x86_64.rpm
Preparando... ##### [100%]
 1:Nessus ##### [100%]
nessusd (Nessus) 4.4.1 [build M15078] for Linux
(C) 1998 - 2011 Tenable Network Security, Inc.
```

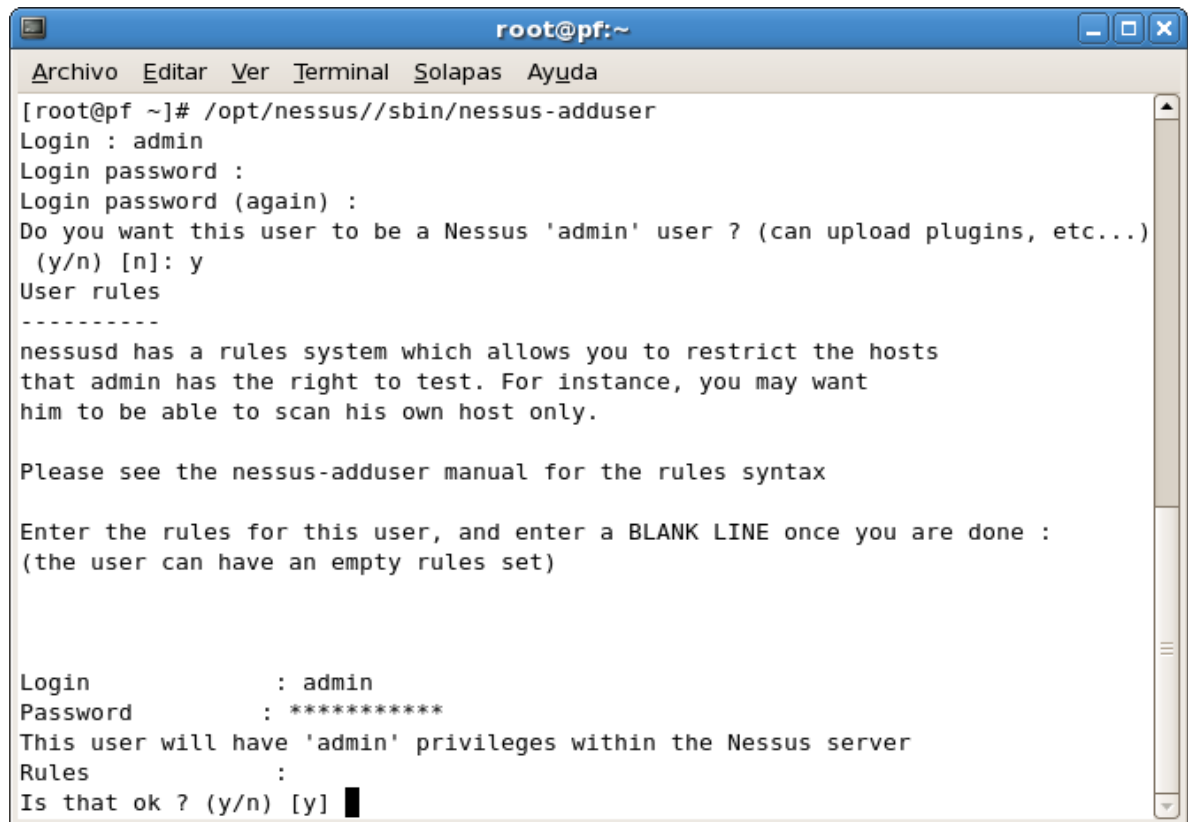
```
Processing the Nessus plugins...
[#####]
```

All plugins loaded

- Please run /opt/nessus//sbin/nessus-adduser to add a user
- Register your Nessus scanner at <http://www.nessus.org/register/> to obtain all the newest plugins
- You can start nessusd by typing /sbin/service nessusd start

- Creamos un usuario para administrar la herramienta Nessus

```
/opt/nessus//sbin/nessus-adduser
```



```
root@pf:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[root@pf ~]# /opt/nessus//sbin/nessus-adduser
Login : admin
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...)
(y/n) [n]: y
User rules
-----
nessusd has a rules system which allows you to restrict the hosts
that admin has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)

Login          : admin
Password       : *****
This user will have 'admin' privileges within the Nessus server
Rules          :
Is that ok ? (y/n) [y] █
```

- Activación de Nessus

Hay que registrarse en la página oficial de Nessus para poder usar el código de activación de la herramienta.

```
http://www.nessus.org/products/nessus/nessus-plugins/obtain-
an-activation-code
```

```
/opt/nessus/bin/nessus-fetch --register EB6C-ACEC-A989-C945-
777A
```

- Iniciamos el servicio de Nessus y configuramos para que inicie con el sistema operativo.

```
/sbin/service nessusd start
```



```
chkconfig nessusd on
```

- Ejecutamos la herramienta Nessus

En el navegador ponemos la siguiente dirección:

```
https://127.0.0.1:8834/
```



2. Integrando Nessus a PacketFence

- Archivo de Configuración

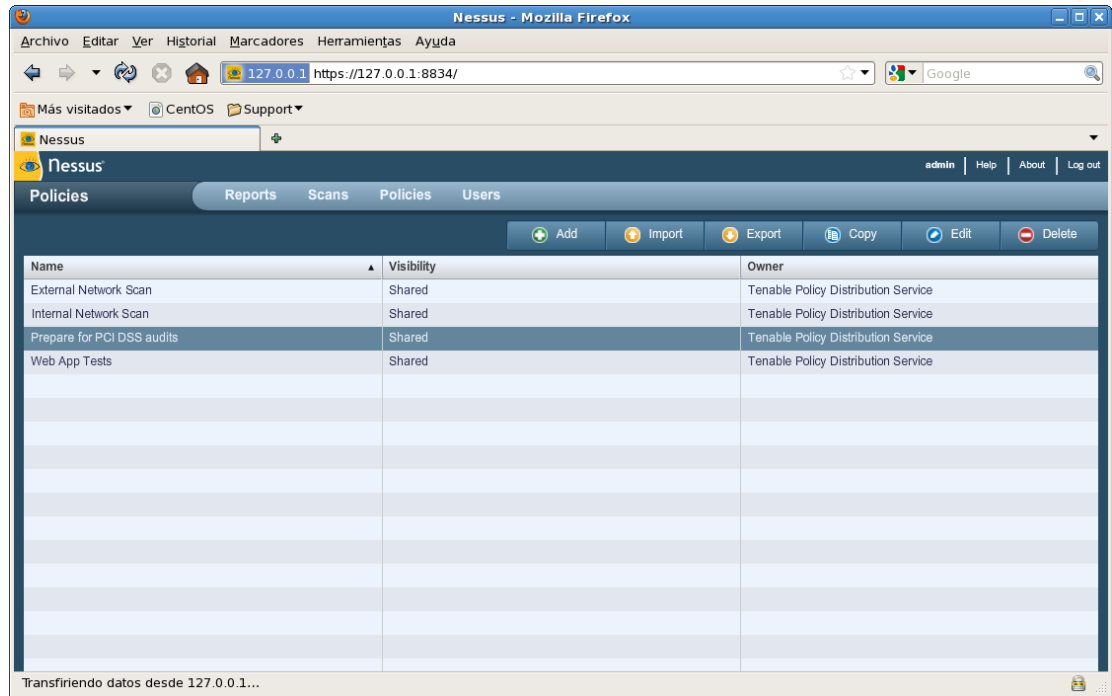
PacketFence trae consigo un archivo de configuración pre elaborado para el escaneo de vulnerabilidades en la siguiente ubicación:

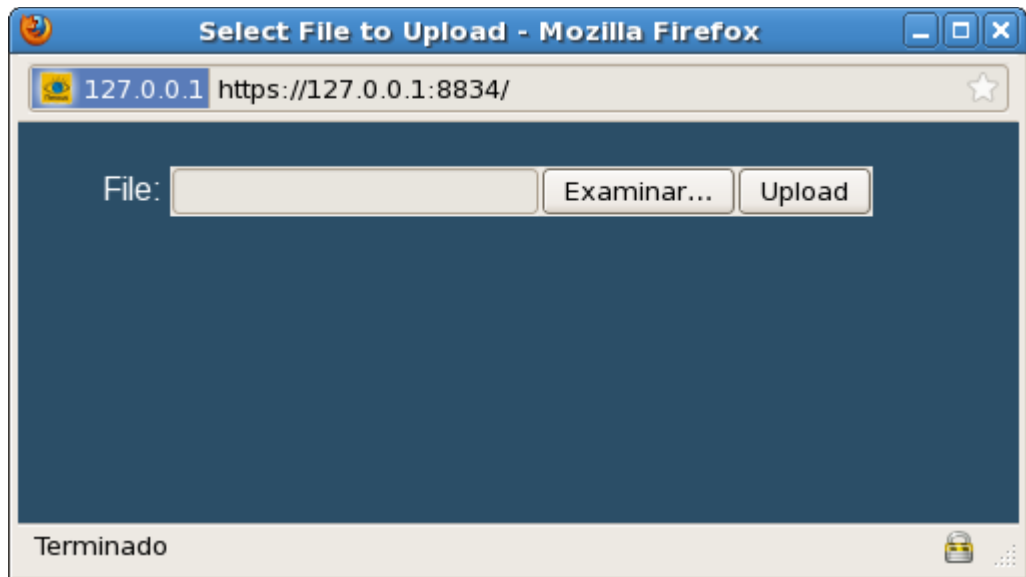
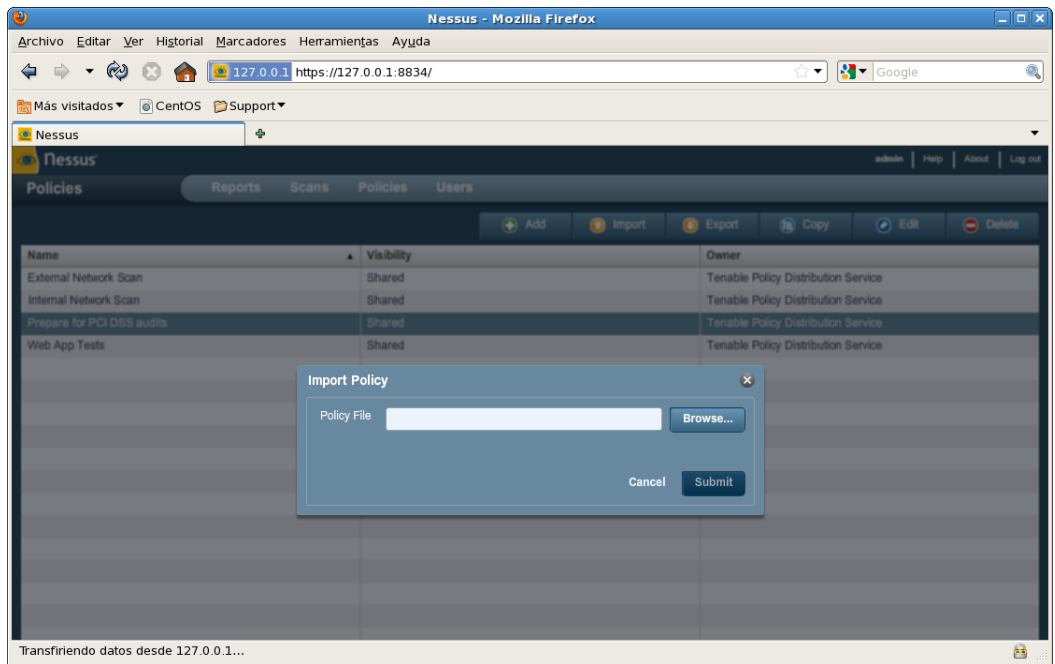
```
/usr/local/pf/conf/nessus/remotescan.nessus
```

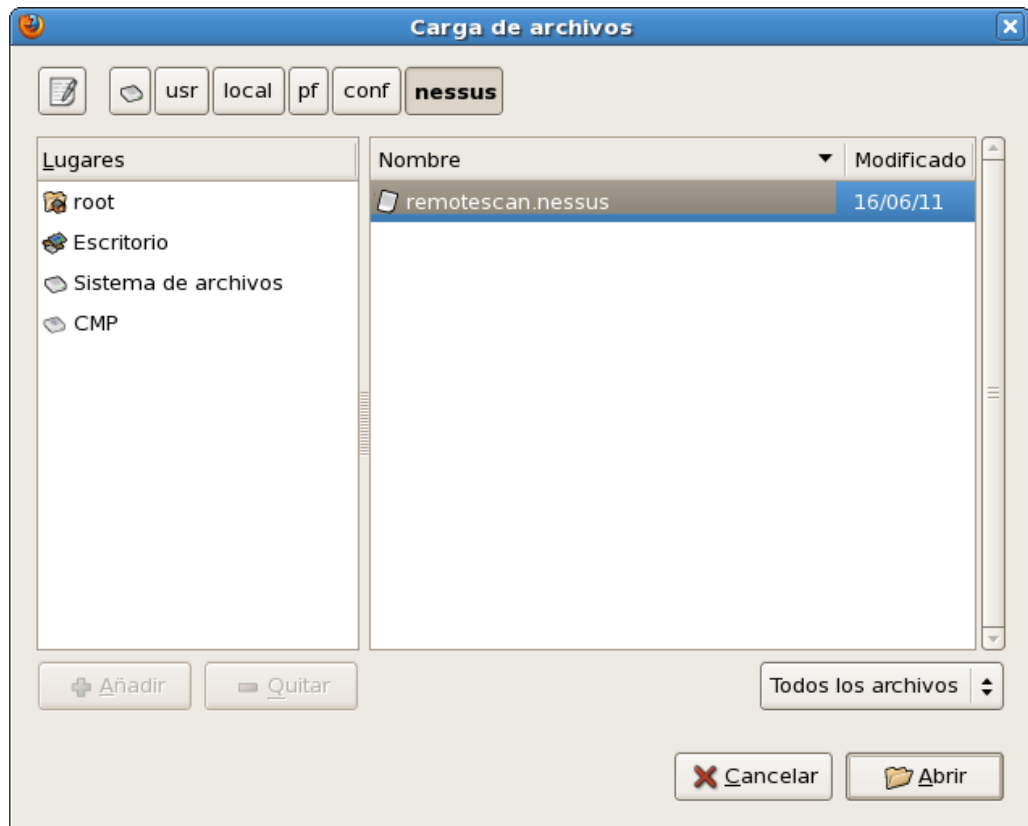
Utilizamos este archivo para configurar las políticas de pre ingreso a la red LAN.

- Configurando Nessus

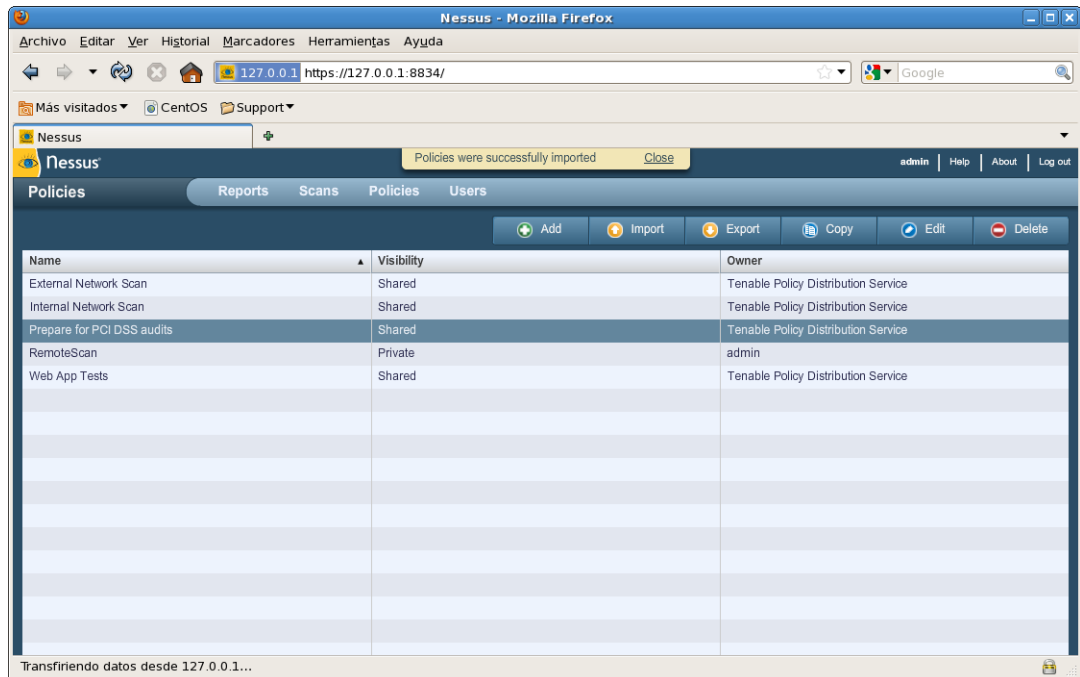
Se debe agregar a la herramienta el archivo de políticas de de PacketFence a Nessus
Para esto debemos ingresar en el menú de políticas en esta parte podemos observar políticas predefinidas en nuestro caso necesitamos agregar la política que viene por defecto en PacketFence.







Una vez agregado la política de pre ingreso en Nessus observaremos lo siguiente:



Una vez modificado podemos modificar a nuestro gusto la política de pre ingreso con la que funciona PacketFence y adaptarla a nuestras necesidades.

- Agregando Nessus a PacketFence

Luego en el servidor PacketFence configuramos el usuario, contraseña y plugins en el archivo de configuración `/usr/local/pf/pf.conf`.

```
[scan]
ssl=enabled
pass=123456
user=admin
port=1241
host=127.0.0.1
registration=enabled
nessusclient_file=remotescan.nessus
nessusclient_policy=RemoteScan
live_tids=54615
```

Para evitar problemas al escanear los clientes con la política de seguridad debemos darle permisos 755 al archivo `remotescan.nessus`

```
chmod 755 /usr/local/pf/conf/nessus/remotescan.nessus
```

ANEXO E

ENCUESTA

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

OBJETIVO: Determinar si la seguridad de la red LAN de la Dirección Provincial del Consejo de la Judicatura de Chimborazo, mejoró con la implementación de la herramienta de Network Admission Control.

CUESTIONARIO

1. ¿Cree usted que es útil controlar el acceso a la red LAN institucional?

SI___ NO___

2. ¿Cuándo se presentaba una acceso indebido de seguridad podía usted determinar donde se generaba el problema?

SI___ NO___

3. -¿Cómo calificaría usted. la manipulación y gestión de la herramienta Network Admission Control implementada para supervisar la red LAN de la institución?

FÁCIL___ NORMAL ___ DIFÍCIL___

4. ¿Con la implementación de la herramienta Network Admission Control cree usted que se ha podido controlar las vulnerabilidades y fallas de seguridad de la red Institucional, garantizando así la seguridad de la red LAN?

SI___ NO___

5. ¿Considera usted que con la implementación de la herramienta PacketFence se ha logrado mejorar el control de acceso de los recursos?

SI___

NO___

6. ¿Piensa usted que el tener la administración y monitoreo de la red para la detección de vulnerabilidades y fallas de seguridad, favorece de alguna manera la tarea del administrador de la red LAN institucional?

MUCHO___

POCO___

NADA___

7. ¿La herramienta implementada permite obtener información detallada y en tiempo real el estado actual de los dispositivos que conforman la red?

SIEMPRE _____

CASI SIEMPRE _____

NUNCA _____

8. ¿Cree usted que la implementación de esta herramienta ayudará al desarrollo de la Infraestructura de la Institución?

SI___

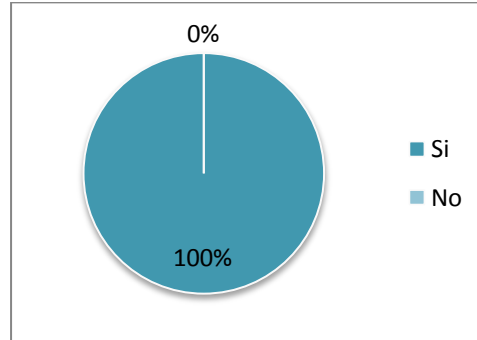
NO___

GRACIAS POR SU COLABORACIÓN

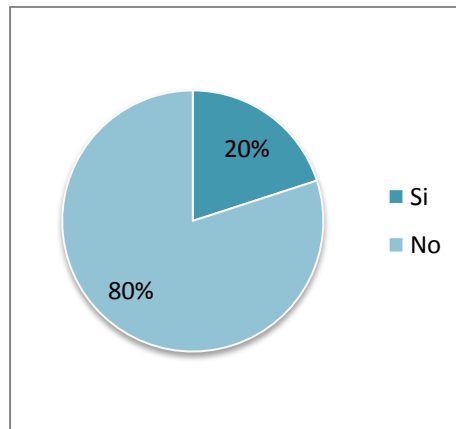
ANEXO F

Tabulación de la Encuesta

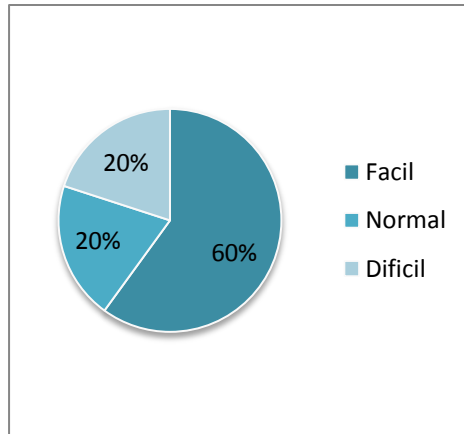
1. ¿Cree usted que es útil el controlar el acceso a la red LAN institucional?



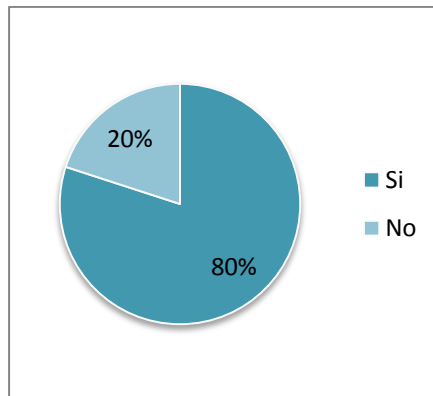
2. ¿Cuándo se presentaba un acceso indebido de seguridad podía usted determinar donde se generaba el problema?



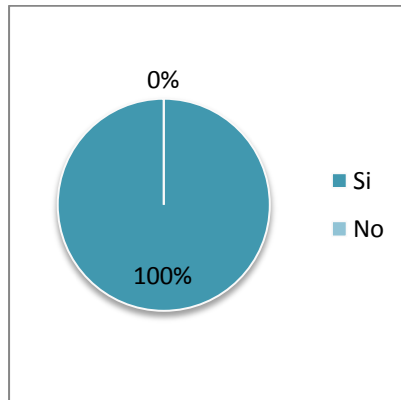
3. -¿Cómo calificaría usted la manipulación y gestión de la herramienta Network Admission Control implementada para supervisar la red LAN de la institución?



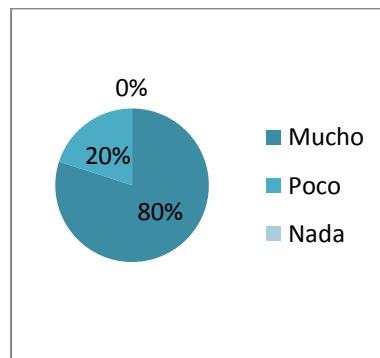
4. ¿Con la implementación de la herramienta Network Admission Control cree usted que se ha podido controlar las vulnerabilidades y fallas de seguridad de la red Institucional, garantizando así la seguridad de la red LAN?



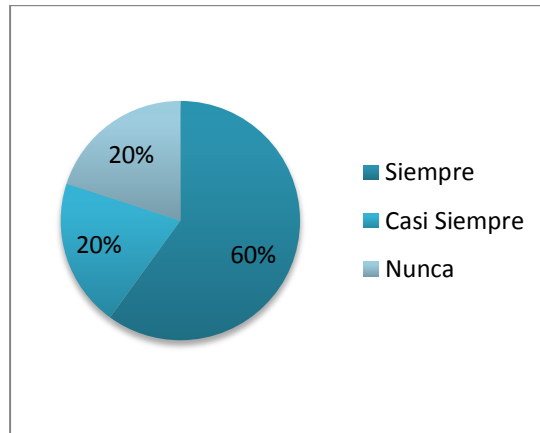
5. ¿Considera usted que con la implementación de la herramienta PacketFence se ha logrado mejorar el control de acceso de los recursos para disminuir las vulnerabilidades y fallas de seguridad en la red LAN?



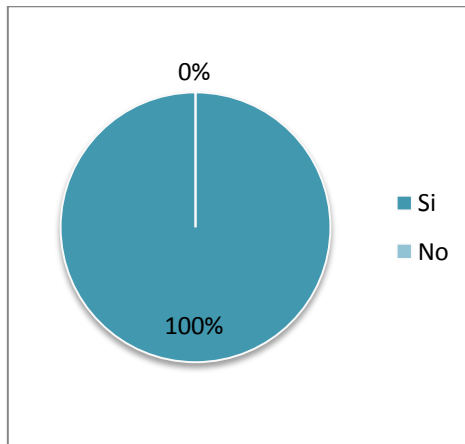
6. ¿Piensa usted que el tener la administración y monitoreo de la red para la detección de vulnerabilidades y fallas de seguridad, favorece de alguna manera la tarea del administrador de la red LAN institucional?



7. ¿La herramienta implementada permite obtener información detallada y en tiempo real el estado actual de los dispositivos que conforman la red?



8. ¿Cree usted que la implementación de esta herramienta ayudará al desarrollo de la Infraestructura de la Institución?



BIBLIOGRAFÍA DE INTERNET

[1] ARQUITECTURA DE NAC

URL: <http://www.networkcomputing.com/data-protection/tutorial-network-access-control-nac.php?p=1>

2012-01-26

[2] CLAVES PARA ELEGIR LA MEJOR SOLUCIÓN NAC

URL: <http://www.eweekeuropa.es/knowledge-center/knowledge-center-seguridad/claves-para-elegir-la-mejor-solucion-nac-83>

2012-02-09

[3] DOCUMENTACIÓN DE PACKETFENCE

URL: <http://www.packetfence.org/documentation/documentation.html>

2012-02-15

[4] DOCUMENTACIÓN FREENAC

URL: <http://freenac.net/es>

2012-02-15

[5] EL FUTURO DE NAC

URL: http://www.idg.es/cio/El_futuro_de_NAC/art186000-.htm

2012-02-09

[6] FASES DE NAC

URL: http://www.networkworld.es/NAC_Las-preguntas-mas-candentes/seccion-/articulo-187522

2012-03-04

[7] MANUAL DE SEGURIDAD EN REDES

URL: <http://www.scribd.com/doc/2926302/Manual-de-Seguridad-en-Redes>

2012-03-16

[8] NETWORK ADMISSION CONTROL

URL: http://red.gov.cl/evento-mayo-2009/pdf/Seguridad_NAC.pdf

2012-02-15

[9] POLÍTICAS DE SEGURIDAD

URL: <http://www.123innovationgroup.info/#art2>

2012-03-16

[10] QUE SALIÓ MAL

URL: <http://www.networkworld.com/reviews/2010/052410-network-access-control-test.html>

2012-01-21

[11] QUIEN NECESITA NAC

URL: [http://www.networkworld.es/NAC_Las-preguntas-mas-candentes-
/seccion-/articulo-187522](http://www.networkworld.es/NAC_Las-preguntas-mas-candentes-/seccion-/articulo-187522)

2012-01-21

[12] REDES DE AUTODEFENSA

URL: <http://dl.dropbox.com/u/2150563/Self%20Defending%20Networks%20and%20the%20Immune%20System.pdf>

2012-02-07