UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE INGENIERIA

TESIS

OPTIMIZACION DE LA SEGURIDAD DE LA RED DE DATOS DEL IBUNAM BAJO PFSENSE.

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACION:

PRESENTA :

GUADALUPE XIMENA GUTIERREZ ZEA

DIRECTOR DE TESIS: ING. JOEL VILLAVICENCIO CISNEROS

CIUDAD UNIVERSITARIA 06 DE ENERO DE 2014

Agradecimientos

A mis padres, por todo.

A la comunidad del Instituto de Biologia por el apoyo en la implementacion de este proyecto en especial al Dr. Victor Sanchez Cordero Davila, director.

Agradezco a todos mis compañeros que estuvieron conmigo a lo largo de todo el proceso:

Noemi, Jo, Alfred, George, Celi gracias por creer en mi...

Alberto, por hacerme fuerte..

Los quiero..

Mena.

Índice general

Indice de Figuras **2**

1. Introducción **6**
1.1. Red de computadoras . . . 6
1.1.1. Tipos de redes. . . . 6
1.2. Seguridad de la Información. . . . 15
1.3. Seguridad de la Red . . . 15
1.4. Seguridad Perimetral. . . . 15
1.5. Seguridad Informática. . . . 15
1.5.1. Objetivos de la Seguridad Informática. . . . 16
1.5.2. Esquema de seguridad basado en Criterios Comunes. . . . 16
1.5.3. Niveles de seguridad. . . . 17
1.5.4. Rendimiento de seguridad. . . . 18
1.6. Estándares de Seguridad Informática. . . . 19
1.6.1. Familia ISO 27000. . . . 19
1.6.2. ISO 27001 . . . 21
1.6.3. ISO 27002 . . . 21
1.6.4. ISO 27003 . . . 21
1.6.5. ISO 7498-2 . . . 22
1.6.6. NIST-Recommendations, Guidelines on Firewalls and Firewall Policy. 22
1.6.7. OSSTMM . . . 23

2. Redes de Datos. **24**
2.1. Topologías de Red. . . . 24
2.1.1. Topologías Físicas. . . . 24
2.1.2. Topologías Lógicas . . . 27
2.2. Modelo OSI . . . 28
2.2.1. Capa 7 Aplicación . . . 28
2.2.2. Capa 6 Presentación . . . 30
2.2.3. Capa 5 Sesión . . . 30
2.2.4. Capa 4 Transporte . . . 30
2.2.5. Capa 3 Red . . . 36
2.2.6. Capa 2 Enlace de datos. . . . 44
2.2.7. Capa 1 Física . . . 51
2.3. Modelo de Arquitectura TCP/IP. . . . 56

3. Servicios y Mecanismos de Seguridad. 59
3.1. Vulnerabilidades y amenazas . . . 62
3.2. Seguridad Física. . . . 64
3.2.1. Tipos de Vulnerabilidades y amenazas. . . . 64
3.3. Seguridad Lógica. . . . 66
3.3.1. Tipos de Vulnerabilidades y Amenazas Lógicas. . . . 67
3.4. Controles de Seguridad. . . . 68
3.4.1. Controles de Seguridad física. . . . 68
3.4.2. Controles de Seguridad Lógica. . . . 69
3.4.3. Integración de Políticas de Seguridad Informática. . . . 83

4. Estudio de Caso e implementación. 85
4.1. Estudio de Caso: IB. . . . 85
4.1.1. Análisis de Página WEB. . . . 88
4.1.2. Análisis de Correo Electrónico. . . . 90
4.1.3. Optimización de esquema de seguridad. . . . 92
4.2. Implementación de filtrado de contenido con PFSENSE. . . . 95
4.3. Sistema de Respaldo. . . . 96
4.4. Configuración de DHCP . . . 97
4.5. Enrutamiento InterVLAN . . . 99
4.6. Portal Cautivo para usuarios móviles. . . . 100
4.7. Firewall y control de acceso. . . . 102
4.8. NAT . . . 103
4.9. Definición de DMZ y Data Center. . . . 105
4.10. Sistema de Filtrado . . . 106
4.11. Optimización de IDS . . . 110
4.12. Reintegración de la red de datos de la Unidad de Informática para la Biodiversidad (UNIBIO). . . . 112

5. Análisis de Vulnerabilidades y Resultados 113
5.0.1. Análisis de Vulnerabilidades después de la optimización. . . . 118

Bibliografía 123

Anexo 125

Índice de figuras

1.1. Red WAN. 7
1.2. Red MAN. 7
1.3. Modelo Jerárquico LAN 9
1.4. Definición y aplicación de VLANS 11
1.5. Tipos de VLANS. 13
1.6. VPN Cliente-Servidor. 14
1.7. VPN Cliente hacia LAN. 14
1.8. VPN LAN hacia LAN. 14
1.9. Familia ISO 27000. 20

2.1. Topología tipo Estrella 24
2.2. Topología tipo Malla 25
2.3. Topología tipo Malla Completa 25
2.4. Topología tipo Bus 25
2.5. Topología tipo Anillo 26
2.6. Topología tipo Arbol 26
2.7. Modelo OSI 28
2.8. Protocolos de Aplicación 29
2.9. Cabecera UDP 32
2.10. Cabecera TCP 33
2.11. Enlace de tres vías. 35
2.12. Cabecera IPv4 37
2.13. Dispositivo de capa 3: router. 41
2.14. Tipos de Rutas. 42
2.15. Funcionamiento de router en capas del modelo OSI 43
2.16. Formato de Trama 44
2.17. La función del encabezado. 44
2.18. La función del trailer. 45
2.19. Estándares y protocolos manejados en capa de enlace. 48
2.20. Dispostivos de capa 2: Switch. 49
2.21. Registro de tabla ARP. 50
2.22. Transformación de información en el modelo OSI 51
2.23. Estándares de cableado UTP. 52
2.24. Estándares de cableado TIA. 52
2.25. Fibra optica Multimodo y Monomodo 53

2.26. Modelo de protocolo TCP/IP 56
2.27. Comparación modelo OSI y TCP/IP 57

3.1. Relación de conceptos. 63
3.2. Contramedidas asociadas a las amenazas hacia los objetivos de seguridad. . 63
3.3. Arquitectura Dual Homed. 74
3.4. Arquitectura Screening/Bastion Host 75
3.5. Proceso de DHCP. 76
3.6. Traducción NAT. 77
3.7. Pinholing. 77
3.8. Balanceo de Carga. 78
3.9. Se asigna una escala para cada conexión saliente de tráfico para distribuirlo proporcionalmente. 79
3.10. El tráfico viaja por el enlace normal. 79
3.11. El tráfico se desvía hacia el enlace funcional. 79
3.12. El tráfico fluye por el enlace con la prioridad mas alta. 80
3.13. El tráfico cambia a un enlace activo sin congestionamiento. 80
3.14. Balanceo de carga por enlace. 80
3.15. Balanceo por persistencia hasta que termine la conexión. 80
3.16. Balanceo de carga con enlace menos uso. 81
3.17. Balanceo de carga con el porcentaje mas bajo. 81
3.18. Balanceo de Carga tipo Enforced. 81
3.19. Balanceo de carga tipo Lowest Latency. 81
3.20. Firewall Transparente. 82
3.21. Estructura normativa. 83

4.1. Topologico de la red de datos en producción. 86
4.2. Porcentaje de vulnerabilidades de página web. 88
4.3. Despliegue de vulnerabilidades de pagina web 89
4.4. Escaneo a Correo electronico. 90
4.5. Escaneo a Correo electronico despliegue. 91
4.6. Captura de trafico de correo. 92
4.7. Optimización de topologico IB. 93
4.8. Logotipo Pfsense. 95
4.9. Servidor TFTP. 97
4.10. Servicio DHCP activo. 97
4.11. Configuración de interfaz DHCP. 98
4.12. Ruteo InterVLAN. 100
4.13. Operación de un Portal Cautivo. 101
4.14. Visualización de Portal Cautivo. 101
4.15. Visualización de interfaz de reglas del Firewall. 102
4.16. Visualización de la bitacora de Firewall. 103
4.17. Visualización de Interfaz de configuración NAT con port forward. 103
4.18. Visualización de configuración de NAT 1 a 1. 104
4.19. Visualización de NAT saliente. 104

4.20. Ubicación de zona desmilitarizada y Data Center. 105
4.21. Instalacion de Paquetes. 106
4.22. Configuración Proxy server. 107
4.23. Configuración de Dansduardian. 108
4.24. Verificación de servicios activos. 109
4.25. Portal de control de acceso Dansguardian. 109
4.26. Pagina inicial de Sensor Honeynet UNAM. 111
4.27. Pagina de reporte de incidentes. 111
4.28. Firewall Unibio. 112

5.1. Gráficas de Latencia. 114
5.2. Gráficas de tráfico de una semana. 115
5.3. Gráficas de tráfico de tres meses. 116
5.4. Gráficas de trafico WAN. 117
5.5. Gráficas de trafico WAN firewall 2. 117
5.6. Interfaz web de correo actualizado y seguro. 118
5.7. Despliegue de vulnerabilidades de correo seguro 119
5.8. Pagina Web nueva. 120
5.9. Porcentaje de vulnerabilidades de pagina web bajo pfsense 121
5.10. Despliegue de vulnerabilidades de pagina web bajo pfsense 121

Capítulo 1

Introducción

El Instituto de Biología es una de las instituciones con la misión del desarrollo de la investigación científica, en particular con el origen, interacción, distribución y conservación de la diversidad biológica. El conjunto de años de investigación conforman un banco de datos digitales el cual va cada día en aumento. La tecnología esta en todas partes y el IB [1] no es una excepción, por lo que la institución cuenta con servicios de red para la compartición, generación y almacenamiento de información de tipo académica. Dicho acervo es un activo esencial y el mas importante de dentro de cualquier institución, por lo tanto debe y necesita estar debidamente asegurado. Debido al incremento en la interconectividad de los dispositivos y el flujo de información entre ellos es necesario que la Unidad de Cómputo que es la encargada de proporcionar este tipo de servicio verifique la calidad del mismo. Por lo que el objeto de esta tesis con respecto a lo antes mencionado es cubrir la totalidad del servicio y sus variantes con el objetivo de iniciar una revisión de la situación actual de los servicios de TI.

1.1. Red de computadoras

Una red informática también llamada red de computadoras, es un conjunto de múltiples equipos informáticos, conectados por medio de dispositivos físicos o cualquier otro medio para el transporte de datos, compartiendo un sistema de comunicaciones. Con la finalidad de compartir información y recursos.

1.1.1. Tipos de redes.

Las redes de computadoras se diseñan y construyen en arquitecturas que pretenden servir a los objetivos de uso. Generalmente están basadas en la conmutación de paquetes[2]

[1] Instituto de Biología.

[2] Se denomina conmutación de paquetes al establecimiento de un intercambio de bloques de información con un tamaño específico entre dos puntos, un emisor y un receptor, se clasifican de acuerdo a su tamaño, distancia y arquitectura física.

WAN

Wide Área Network.

Una red de área amplia es un tipo de red de computadoras capaz de cubrir distancias geográficamente extensas desde unos 100 hasta 1000 km, proporcionando servicio a un país o continente *ver fig 1.1*

Figura 1.1: Red WAN.

En su mayoría son construidas para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet para proveer de conexión a los usuarios. Normalmente la WAN es una red de punto a punto, es decir que es utilizado en sistemas de comunicación via satélite o radio.

MAN

Metropolitan Área Network.

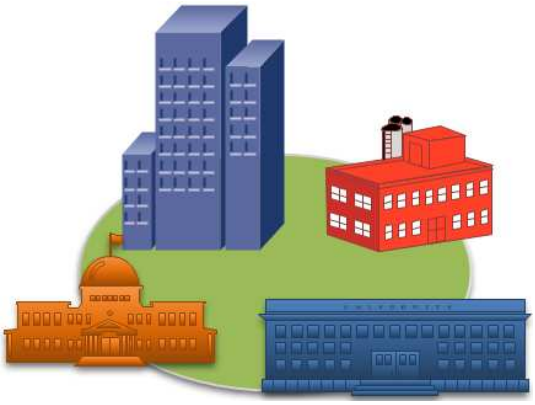


Figura 1.2: Red MAN.

La red de área metropolitan, comprende una ubicación geográfica determinada y su distancia de cobertura es mayor a 4 Km, con un diámetro en entorno de 500 km. Es una red de alta velocidad que da cobertura en un área geográfica extensa, proporciona la capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y video,sobre medios de transmisión tales como fibra óptica y par trenzado. El concepto de red de área metropolitana representa una evolución del concepto de red LAN a un ámbito mas amplio, cubriendo áreas mayores que en algunos casos no se limitan a un entorno metropolitano, sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes MAN *ver fig1.2*.

LAN

Local Área Network.
Una red de área local o un grupo de redes locales interconectadas que están bajo el mismo control. Es una red de datos de alta velocidad y bajo nivel de errores, generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región. Su extensión esta limitada físicamente a un entorno de 200 metros a 1 Km.
Características importantes:

- Tecnología broadcast con el medio de transmisión compartido.
- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Extensión máxima no superior a 3 km.
- Uso de un medio de comunicación privado.
- Múltiples medios de transmisión: cable coaxial, cable telefónico y fibra óptica.
- Facilidad con que se pueden efectuar cambios de hardware y software.
- Posibilidad de conexión con otras redes.

Modelo Jerárquico de Red LAN.

Una red jerárquica se administra y expande con facilidad, ademas de que los problemas se resuelven con mayor rapidez. Dicha arquitectura implica la división de la red en capas independientes. Cada capa cumple con funciones específicas que definen su rol dentro de la red general *ver fig1.3*. La separación de las diferentes funciones existentes en una red, hace que el diseño de la red se vuelva modular facilitando la escalabilidad y el rendimiento de la red.El modelo de diseño jerárquico típico se separa en tres capas: Núcleo, Distribución y Acceso.

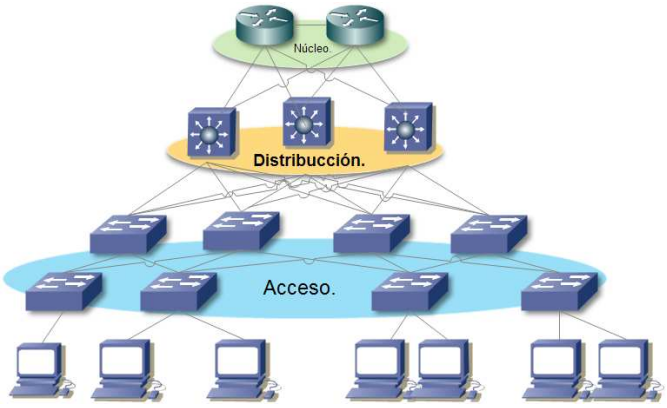


Figura 1.3: Modelo Jerárquico LAN

- Núcleo. La capa núcleo del diseño jerárquico es el backbone de alta velocidad de la internetwork. Dicha capa es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto, debe poder reenviar grandes cantidades de datos rápidamente.

- Distribución. La capa de distribución agrega los datos recibidos de los switch de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. Esta capa controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las LAN virtuales VLANS.

- Acceso. La capa de acceso interactúa con los dispositivos finales, como PCs, impresoras y teléfonos IP, para proporcionar acceso al resto de la red. La capa de acceso puede incluir routers, switch, puentes, hubs y puntos de acceso inalámbricos. El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos de red y controlar que dispositivos pueden comunicarse en la red.

Beneficios de una red jerárquica.

- **Escalabilidad:** La escalabilidad es una propiedad deseable de un sistema, red o proceso, que indica su habilidad para extender el margen de operaciones sin perder calidad, o bien manejar el crecimiento continuo de trabajo de manera fluida. Es decir es la propiedad de estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos. Las redes jerárquicas escalan muy bien debido a la consistencia de us diseño resultando fácil planificar e implementar la expansión.

- **Rendimiento:** El rendimiento de la comunicación mejora al evitar la transmisión de datos a través de un switch. Debido a que las capas núcleo y distribución realizan sus operaciones a velocidades muy altas, hay menos contención para el ancho de banda de la red. Como resultado, las redes jerárquicas con un diseño apropiado logran casi la velocidad de cable entre los dispositivos.

- **Administración y mantenimiento:** Debido a que las redes jerárquicas son modulares en naturaleza y escalan, son fáciles de mantener. La consistencia entre los switch en cada nivel hace que la administración sea mas simple.

VLANS

Virtual LAN.
El rendimiento de una red puede ser un factor en la productividad de una organización y su reputación para realizar sus transmisiones en la forma que es previsto. Una de las tecnologías que es excelente en la contribución de un rendimiento óptimo es la división de una red grande en VLANs. Una VLAN es una subred IP separada de manera lógica, las VLANs permiten que redes de IP y subredes múltiples existan en la misma red conmutada. Para que estas se comuniquen deben tener una dirección IP y una máscara de subred consistente con esa VLAN. Una VLAN permite que un administrador de red cree grupos de dispositivos conectados a la red de manera lógica, que actúa como si estuvieran en su propia red independiente, incluso si comparten infraestructura común con otras VLANs. También se pueden implementar políticas de acceso y seguridad para grupos en particular.

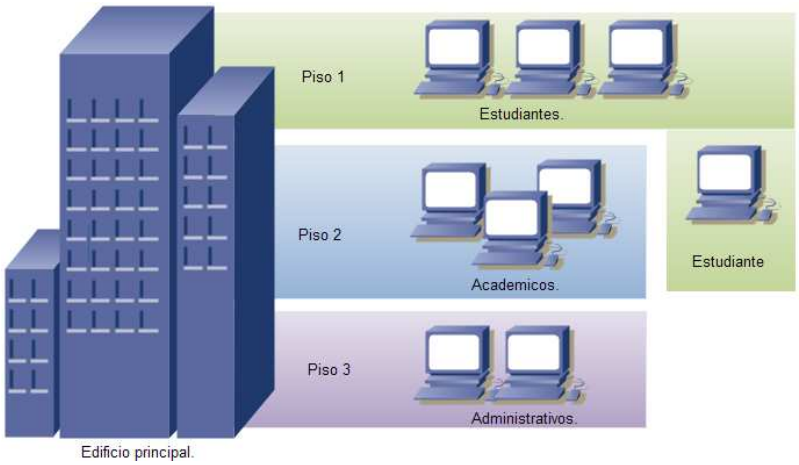


Figura 1.4: Definición y aplicación de VLANS .

La implementación de la tecnología VLAN permite que una red admita de manera flexible las metas internas, impulsando la productividad y el crecimiento de la institución. Los beneficios de utilizar VLANs son:

- **Seguridad:** Los grupos que poseen datos sensibles son aislados del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.
- **Reducción de Costos:** El ahorro en el costo deriva de la baja necesidad de actualizaciones de red, y el uso mas eficiente de enlace y ancho de banda existente.
- **Mejor rendimiento:** La división de redes planas en múltiples grupos lógicos de trabajo, reduce el tráfico innecesario en la red y potencia el rendimiento.
- **Mitigación de broadcast:** La división de una red en VLANs reduce el número de dispositivos que pueden participar en una tormenta de broadcast.
- **Mayor eficiencia del personal de TI:** Las VLANs facilitan el manejo de la red, debido a que los usuarios con requerimientos similares se agrupan en una sola entidad. También es fácil para el administrador identificar alguna falla de red si se busca por grupos muy específicos.
- **Administración de aplicaciones mas simple:** Tener funciones separadas hace que gestionar un proyecto o trabajar con una aplicación especializada sea mas fácil, lo cual hace que agregar dispositivos de red y usuarios también lo sea.

Cada VLAN debe poseer un nombre y un identificador ID. Dicho identificador las divide en dos tipos: rango normal o rango extendido.

- Rango Normal: Se utilizan en pequeños y medianos negocios o empresas. Su ID debe estar entre el 1 y 1005.

- Rango Extendido: Posibilita a los proveedores de servicio que amplíen la infraestructura a una cantidad de usuarios mayor. Su ID debe ubicarse entre el 1006 y 4094.

Actualmente existe fundamentalmente una manera de implementar las VLAN y estas son basadas en puerto, las cuales asocian el número de puerto de acceso hacia la VLAN. A continuacion se enlistan los tipos de VLAN y sus características principales ver *ver fig1.5*. Tipos de VLAN:

- VLAN de datos: Una VLAN de datos es una red virtual configurada para enviar solo tráfico de datos generado por el usuario. Una VLAN puede enviar tráfico basado en voz, o tráfico de administración de Switch. En estos casos es conveniente separar este tipo de tráfico para que las VLANS tengas propósitos definidos y específicos para un tipo de servicio. Esta VLAN puede denominarse *vlan de usuarios*.

- VLAN de voz: Una VLAN que transporta voz se denomina VLAN de voz, este tipo de tráfico debe ser separado para admitir la Voz sobre IP (VoIP), ya que este servicio requiere ancho de banda garantizado, para asegurar la calidad de la voz, prioridad en la transmisión y la capacidad de ser encaminado en áreas de congestión de la red con una demora de menos de 150ms.

- VLAN predeterminada: Todos los puertos de un switch se convierten en un miembro de la VLAN predeterminada luego de que éste arranque. Cuando esto sucede todos los puertos pertenecen al mismo dominio de broadcast, con lo cual se admite a cualquier dispositivo conectado en el switch, normalmente esta VLAN viene predeterminada como VLAN1.

- VLAN nativa: Una VLAN nativa sirve como identificador común en extremos opuestos de un enlace troncal.[3]

[3]Se le llama enlace troncal a una conexión punto a punto, que transporta el tráfico de múltiples VLANs por medio del protocolo 802.1Q.

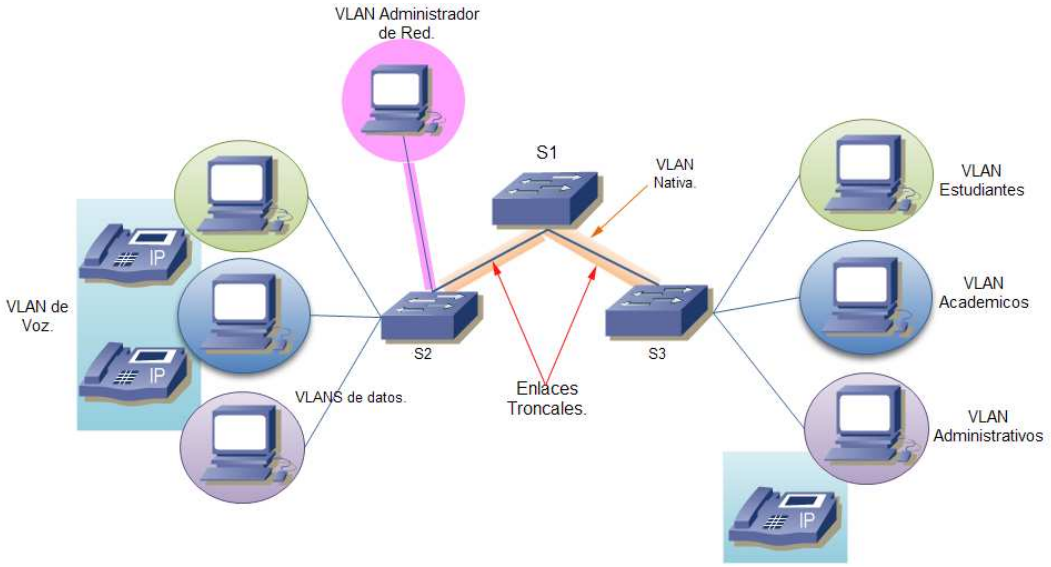


Figura 1.5: Tipos de VLANS.

VPN

Virtual Private Network.
Una red privada virtual es una tecnología de red que permite una extension de la Red de Área Local sobre una red pública o no controlada. Es decir es una conexión segura, punto a punto entre dos nodos utilizando la infraestructura de Internet. Estos dos nodos pueden ser routers, firewalls, o un servidor. Esto permite enlazar dos o mas redes simulando una única red privada permitiendo así, la comunicación entre computadoras como si fuera punto a punto. De esta manera un usuario remoto se puede conectar individualmente a una LAN utilizando una conexión VPN y de esta manera utilizar aplicaciones, enviar datos etc, de manera segura.

Las redes privadas utilizan tecnología de túnel (tunneling) para la transmisión de datos mediante un proceso de encapsulación y cifrado, lo cual se transforma en una ventaja de seguridad, ya que los datos viajan a través de Internet de manera cifrada a través del túnel, lo cual hace que sea prácticamente ilegible para quien intercepte estos paquetes. Esta tecnología es muy útil para interconectar rede que se extienden sobre áreas geográficas extensas, como ciudades diferentes o hasta países y continentes. Las ventajas principales de las VPNs comprenden: seguridad, disminución de costos, óptima administración, facilidad de uso. Existen múltiples formas de implementar una VPN, puede ser basada en Hardware o a través de software, pero lo mas importante es el protocolo que se utilice para dicha implementacion, los mas utilizados son SSL/TLS e IPsec y PPTP.

De los tipos de conexión VPN son:

- **VPN Cliente-Servidor.** El usuario remoto necesita servicios o aplicaciones que corran en el mismo servidor VPN.

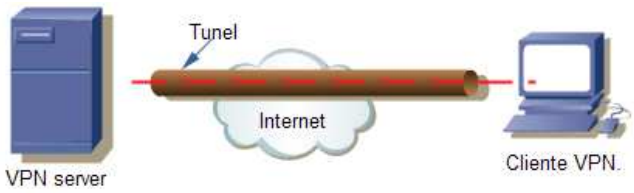


Figura 1.6: VPN Cliente-Servidor.

- **VPN Cliente hacia LAN.** El usuario remoto que utilizará servicios o aplicaciones que se encuentran en uno o mas equipos dentro de la LAN.

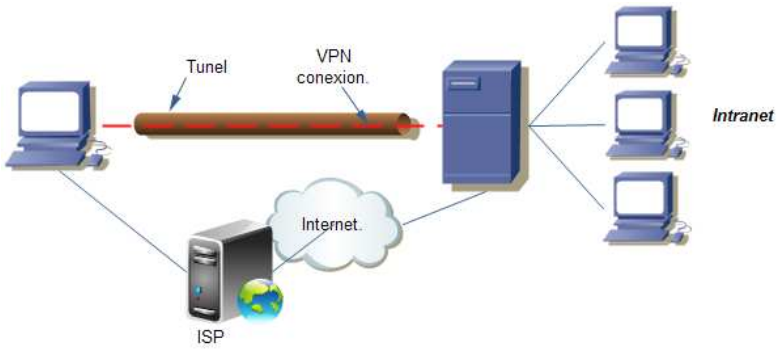


Figura 1.7: VPN Cliente hacia LAN.

- **VPN LAN hacia LAN.** Tambien llamada textLAN to LAN o L2L, esta arquitectura se unen a dos intranets a través de routers, servidores VPN en las LANs y clientes VPN.

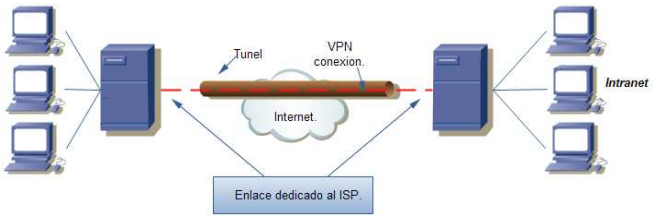


Figura 1.8: VPN LAN hacia LAN.

1.2. Seguridad de la Información.

Se llama seguridad de la Información a todas las medidas o precauciones que se adoptan para evitar cualquier acción que comprometa la información[4]. Sin importar la forma que tome la información o el medio de transmisión, siempre es necesaria la protección adecuada.

1.3. Seguridad de la Red

A medida que que los sistemas de información crecen, la seguridad de los mismos debe hacerlo, así bien debido a la interconectividad que se genera entre estos y la generación de redes mas amplias se tiene el siguiente concepto de seguridad de la red: *Conjunto de herramientas y normas de seguridad para la protección de equipo activo dentro de una red.*

1.4. Seguridad Perimetral.

Definimos perímetro como la frontera de la red de área local. Sin embargo debido a que las redes se han convertido en extremadamente dinámicas y existen dispositivos que rompen con el concepto tradicional de seguridad perimetral como dispositivos móviles y accesos directos a Internet de algunos de estos dispositivos.
Tenemos entonces que el perímetro comienza en donde la transferencia de datos. Para fines de esta tesis contemplaremos el perímetro como se explica en la definición inicial. Así entonces la seguridad relativa al perímetro son las precauciones que se tienen para la protección de éste y su interior.

1.5. Seguridad Informática.

Se define como el conjunto de herramientas automatizadas cuya función es proteger los tres objetivos de la seguridad informática. Un sistema confiable es definido como aquel que posee la combinación apropiada de Confidencialidad, Integridad y Disponibilidad a efectos de soportar los objetivos particulares fijados por la institución.

[4]La información es un conjunto organizado de datos procesados que constituyen un mensaje.

1.5.1. Objetivos de la Seguridad Informática.

- Confidencialidad.
  Su prioridad es que la información sea accedida solo por personal autorizado y de manera autorizada. Bajo los controles de Identificación, Autenticación y Autorización, se previene la divulgación no autorizada de información sensible.
  Los cuales se explican a continuación:

  - *Identificación:* Es la forma en que los usuarios comunican su identidad a un sistema.
  - *Autenticación:* Es el proceso por el cual se prueba que la información de identificación corresponde con el sujeto que la presenta.
  - *Autorización:* Son los derechos y permisos otorgados a un individuo (o proceso) que le permite acceder a un recurso del sistema.

  De este último objetivo se obtiene uno mas *Privacidad*, cuyo objetivo de seguridad busca proteger la información del individuo, empleando controles para garantizar que la misma no sea diseminada o accedida en forma no autorizada.

- Integridad.
  Se trata que toda la modificación a datos o información, es realizada por personas autorizadas de manera autorizada. Se protege la integridad de: los datos,los procesos de manipulación de datos, la consistencia de los mismos de manera interna y externa. Se previene la modificación No autorizada de los sistemas e información.

- Disponibilidad.
  La información y datos se encuentran disponibles para personal autorizado cuando sean necesarios. Así como la prevención de la interrupción del servicio y la pérdida de productividad.

1.5.2. Esquema de seguridad basado en Criterios Comunes.

Los criterios comunes surgen como resultado de la armonización de los criterios sobre seguridad software, mediante un proceso de evaluación en múltiples países. Se proporciona un conjunto común de requisitos funcionales para los productos de Tecnologías de la Información, ya sean hardware, software o firmware. De esta manera se establece un nivel de confianza en el grado en el que el producto TI satisface la funcionalidad de seguridad y ha superado las medidas de evaluación aplicadas. Así se garantizan las funciones de seguridad.

El CC permite comparar resultados de evaluaciones de seguridad independientes. Provee un set de requerimientos comunes para la seguridad y funcionalidad de los productos de TI [5]y las medidas a aplicar en estos mismo durante la evaluación. Los productos de TI pueden ser implementados en hardware, firmware o software. El Common Criteria es flexible con la intensión de habilitar un rango mas amplio de evaluación, que aplique a las propiedades de seguridad y los productos.

1.5.3. Niveles de seguridad.

Los niveles de seguridad describen diferentes tipos de seguridad y se enumeran desde el mínimo grado de seguridad al máximo. El estándar utilizado internacionalmente es el TCSEC Orange Book, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los E.U. Estos niveles han sido la base de desarrollo de estándares europeos y luego internacionales. Cada nivel requiere todos los niveles definidos anteriores.

Nivel D

Este nivel contiene solo una división y esta reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autenticación con respecto a los usuarios y derechos en el acceso a la información.

Nivel C1: Protección Discrecional.

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso. Con la actual descentralización de los sistemas de cómputo, el rol de superusuario es segregado en múltiples actividades y es difícil distinguir entre los cambios que se ejecutaron por el usuario.

El acceso de control discrecional es la distinción entre los usuarios y recursos. Se podrán definir grupos de usuarios con los mismos privilegios y grupos de objetivos sobre los cuales podrán actuar los usuarios o grupos de ellos a través de un control de identificación y autentificación.

Nivel C2: Protección de Acceso Controlado

Este subnivel fue diseñado para solucionar las debilidades del C1. Se tiene la capacidad de restringir aún mas el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitiendo o denegando datos a usuarios en concreto, con base no solo en los permisos, sino también en los niveles de autorización. Los usuarios de este nivel tiene autorización para realizar algunas tareas de administración del sistema, sin necesidad de ser administradores. De esta manera se permite llevar una mejor cuenta de las tareas

[5]Tecnologías de Información.

relacionadas con la administración del sistema, ya que cada usuario es quien ejecuta el trabajo y no el administrador del sistema.

Nivel B1: Seguridad Etiquetada.

Este subnivel, es el primero de los tres con que cuenta el nivel B. Se establece que el dueño del archivo, no puede modificar los permisos de un objeto que esta bajo control de acceso obligatorio. A cada objeto del sistema se le asigna una etiqueta, con un nivel se seguridad jerárquico y con categoría.

Nivel B2: Protección Estructurada.

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La protección estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior.

Nivel B3: Dominios de Seguridad.

Refuerza a los dominios de instalación de hardware,existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido. Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y pruebas ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura. Además cada usuario tiene asignados lugares y objetos de acceso.

Nivel A: Protección Verificada.

Es el nivel mas elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales para asegurar todos los procesos que realiza un usuario sobre el sistema. Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El software y hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

1.5.4. Rendimiento de seguridad.

El rendimiento es el cumplimiento de una tarea determinada, medida a partir de normas o estándares preestablecidos o conocidos de precisión, integridad, costo y velocidad. Aplicando este mismo concepto tenemos que el rendimiento en seguridad es, el cumplimiento de todas aquellas tareas determinadas contrapuestas a lineamientos establecidos, para obtener métricas que declaren y/o predigan si la administración del sistema de seguridad se lleva a cabo de manera óptima. Tales métricas pueden ser: cantidad de tráfico por ancho de banda y tiempo, porcentaje de paquetes perdidos y calidad de servicio.

1.6. Estándares de Seguridad Informática.

La normalización o estandarización es la redacción y aprobación de normas, que se establecen para garantizar el acoplamiento de elementos construidos independientemente, así como garantizar la calidad y seguridad del funcionamiento para trabajar con responsabilidad social. Acorde a la ISO, la estandarización tiene por objeto establecer, ante problemas reales o potenciales, disposiciones destinadas a usos comunes y repetidos, con el fin de obtener un nivel óptimo dentro del contexto de la seguridad informática. Los organismos nacionales que son miembros de la International Organization for Standarization (ISO) participan en la elaboración de normas internacionales a través de comités técnicos, para tratar con ámbitos específicos de actividad técnica. Fundamentalmente los objetivos de una normalización son:

- *Simplificación:* Se trata de reducir los modelos para quedarse únicamente con los mas necesarios.

- *Unificación:* Para permitir el intercambio a nivel internacional.

- *Especificación:* Se persigue evitar errores de identificación creando un lenguaje claro y preciso.

Cabe mencionar que dichas normas son voluntarias, dado que la organización no depende de ningún otro organismo internacional, esta no tiene autoridad para imponer sus normas. Dichos ISOS forman parte de la base y como guía para la estructuración, desarrollo e implementación del objetivo de esta tesis.

1.6.1. Familia ISO 27000.

Sistemas de Gestión de Seguridad Informática. ISMS

Los Estándares Internacionales, proveen un modelo a seguir en la operación e implementación de un sistema de administración. La familia Information Security Management System (ISMS), ofrece un marco de trabajo para la gestión de la seguridad de los activos de información y la preparación de una evaluación independiente a la seguridad del Sistema de Gestión de Seguridad Informática, aplicado a la protección de la información, tal como: información financiera, propiedad intelectual, detalles de los empleados, o información de terceros.

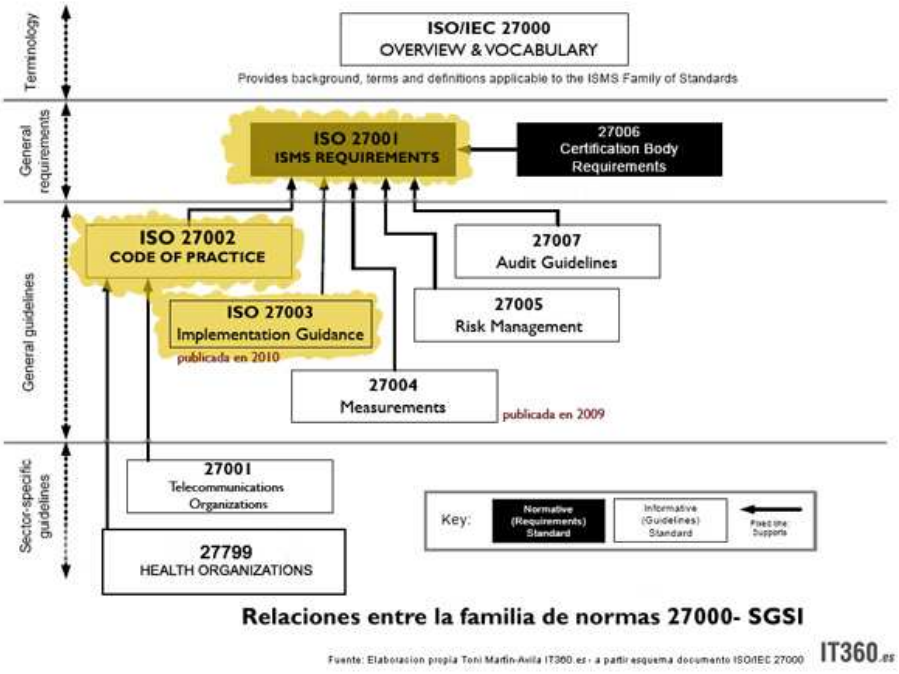


Figura 1.9: Familia ISO 27000.

Un Sistema de Gestión de Seguridad Informática proporciona un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio, basados en una evaluación de riesgos y los niveles de aceptación de riesgo diseñados para tratar y gestionar eficazmente el mismo.
Para la implementación exitosa de un ISMS es necesario tener en cuenta: la conciencia de la seguridad de la información, la asignación de responsabilidades, la incorporación de un comité, la mejora de los valores sociales, **la incorporación como elemento esencial de la seguridad de las redes y sistemas** , la prevención y detección de incidentes, para garantizar un enfoque integral en la administración, y poder evaluarla continuamente para efectuar modificaciones apropiadas. Los beneficios de la familia ISMS son principalmente la reducción del riesgo de seguridad de la información. Específicamente:

- Soporte a los procesos
- Asistencia para la administración en la estructuración del enfoque sobre ,la gestión de la seguridad de la información.
- Proporciona un lenguaje base conceptual con respecto a la seguridad de la información.
- Fomentar de los niveles aceptados a nivel mundial de las buenas practicas de seguridad de la información, proporcionando a las organizaciones la flexibilidad para adoptar y mejorar los controles pertinentes adaptándose así las circunstancias especificas para mantenerlos al frente de los cambios internos y externos.

1.6.2. ISO 27001

ISMS-Requerimientos.

Este estándar adopta el modelo PLAN-DO-CHECK-ACT el cual aplicado brinda una estructura a todos los procesos del sistema, este estándar provee un modelo solido para la aplicación de los principios en los que las normas que rigen la evaluación de riesgos, diseño e implementación de seguridad, gestión de la seguridad y la re-evaluación. Se especifican los requisitos para la implementación de controles de seguridad adaptados a las necesidades de cada organización de sus partes. Para estos controles es necesaria la identificación, el almacén, la protección, recuperación, tiempo de retención y disposición de registros documentados e implementados. Los requisitos establecidos en este estándar son genéricos y pretende que sean aplicables a todas las organizaciones, independientemente del tipo, tamaño y naturaleza. La exclusión de algún control que sea necesario para satisfacer los criterios de aceptación de riesgos, debe ser siempre y cuando los riesgos asociados han sido aceptados por la alta gerencia, a menos que tales exclusiones no afecten a la capacidad y responsabilidad de la organización para proporcionar seguridad de la información, que cumpla con los requisitos de seguridad determinados por riesgo y los requisitos reglamentarios aplicables.

1.6.3. ISO 27002

Code of practice for ISMS.

Este estándar internacional sirve como una guía práctica para el desarrollo de estándares de seguridad de la información y las practicas efectivas de gestión de la seguridad y ayuda a crear confianza sobre las actividades institucionales. Dentro de este ISO se contemplan los aspectos relacionados con la administración de un ISMS, tales como el manejo de responsabilidad, auditoría interna,revisión y mejora de la gestión del sistema. Los objetivos de control de este estándar están destinados a ser implementados para cumplir con los requisitos identificados por la evaluación de riesgos. Dichas evaluaciones de riesgo deben identificar, cuantificar y priorizar los riesgos contra los criterios de aceptación de riesgo y los objetivos relevantes para la organización.

1.6.4. ISO 27003

ISMS implementation guidance.

El proceso descrito en este estándar internacional ha sido diseñado para proporcionar apoyo a la implementación de los ISOS anteriores. Al utilizar este estándar se pretende que la institución sea capaz de desarrollar procesos de gestión de seguridad de la información, para garantizar que el riesgo de los activos de información esten continuamente dentro de lineas aceptables de seguridad, según lo definido por la institución. La implementación de un sistema de gestión de seguridad es una actividad importante y se ejecuta como un

proyecto, en una organización o institución. Este estándar explica la implementación de un SGSI en cinco fases y cada fase esta representada por una clausula independiente.

- Obtener la aprobación de la gestión para iniciar un proyecto de Seguridad de la Información.
- Definición del Sistema de Gestión de Seguridad de la Información.
- Análisis de la institución u organización
- Planificación del tratamiento y evaluación de riesgos.
- Diseño del Sistema de Gestión de Seguridad Informática.

1.6.5. ISO 7498-2

Este documento describe el Modelo de Referencia OSI, costa de una segunda parte que se refiere a la arquitectura de seguridad, la cual fue publicada en 1988 y en ella se proporciona una descripción general de lo servicios y mecanismos relacionados con la seguridad y sus interrelaciones, muestra además las correspondencias que hay entre la arquitectura de seguridad y estándar.

1.6.6. NIST-Recommendations, Guidelines on Firewalls and Firewall Policy.

Tomando como base las recomendaciones del National Institute of Standars and Technology (NIST), cuya documentación presenta una guía para la diseño e implementación de firewall y políticas de seguridad. Es una referencia para las organizaciones para comprender los alcances de la tecnología de firewall y las políticas de seguridad. Se tienen 5 fases para su implementación:

- **Plan:** Es la primera fase del proceso de implementación, el cual involucra la identificación de todos los requisitos que una institución debe contemplar, para determinar que firewall reforzara la seguridad Institucional.
- **Configure:** La segunda fase involucra todas las facetas de configuración del firewall.
- **Test:** En esta fase se implementa y prueba el prototipo que se ha designado como solución en una ambiente de laboratorio.
- **Deploy:** Una vez que se ha completado la fase de pruebas y todos los problemas han sido corregidos, esta fase se enfoca en el depliegue del firewall en la Institución.
- **Manage:** Para concluir con el ciclo, se propone un componente el cual consta de mantenimiento preventivo y correctivo. Este debe realizarse con regularidad o cuando se ejecuten cambios significativos en el firewall.

1.6.7. OSSTMM

Es un manual sobre la Metodología Abierta de Pruebas de Seguridad, es un manual estándar profesional para la ejecución de pruebas de seguridad en cualquier entorno desde el exterior al interior. Incluye lineamientos de acción, ética del **tester** profesional, la legislación sobre las pruebas de seguridad y un conjunto integral de pruebas. El objetivo del manual es crear un método aceptado para ejecutar un test de seguridad minucioso y cabal. Lo mas importante en esta metodología es que los diferentes test son evaluados y ejecutados donde sean aplicables, hasta arribar a los resultados esperados dentro de un periodo de tiempo determinado. La ISECOM (Instituto para la Seguridad y las Metodologías Abiertas), exige que una prueba de seguridad sea: Cuantificable, Consistente, Repetible y Valida mas allá del periodo de tiempo actual,exhaustivo y concordante con las leyes individuales y locales y el derecho humano a la privacidad.

Capítulo 2

Redes de Datos.

Se denominan redes de datos a aquellas infraestructuras o redes de comunicación diseñadas específicamente, para la transmisión de información mediante el intercambio de datos.

2.1. Topologías de Red.

Una topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse, es decir; es el conjunto de nodos conectados entre si y la forma en que están conectados los nodos, su conmutanción de datos es lo que dan vida a las topologías física y lógica.

2.1.1. Topologías Físicas.

Es la forma que adopta un plano esquemático del cableado o estructura física de red. A continuación se explican los diferentes tipos de topologías físicas.

Estrella.

Esta topología reduce la posibilidad de fallo, conecta los nodos de red a un nodo central. El dispositivo adecuado se llama switch este reenvía todas las transmisiones recibidas de cualquier modo periférico. La ventaja principal es que permite que todos los nodos se comuniquen entre si de manera conveniente, la desventaja es que si el nodo central falla, toda la red se desconecta.

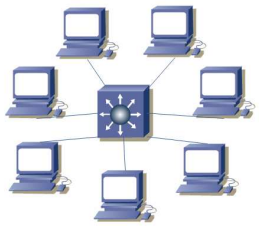


Figura 2.1: Topología tipo Estrella

Malla.

En esta topología cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo, estos enlaces garantizan que cada conexión transporta la carga de datos de los dispositivos, eliminando el problema de los enlaces compartidos por varios dispositivos. Una topología de malla es robusta lo que brinda seguridad. Para robustecer la topología también existen modificaciones de la misma tales como: Malla completa y parcial.
En las cuales los nodos se conectan físicamente con los demás nodos , la desventaja física es que solo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces y la cantidad de conexiones con los enlaces se torna abrumadora.

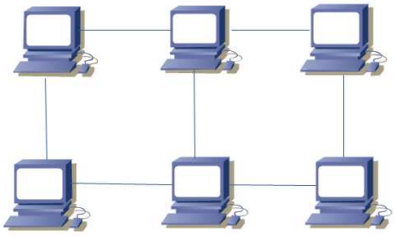


Figura 2.2: Topología tipo Malla

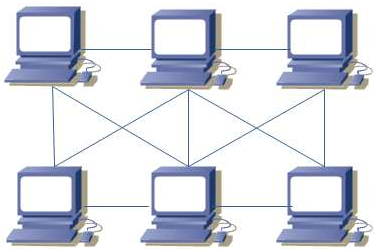


Figura 2.3: Topología tipo Malla Completa

Bus

Esta topología se caracteriza por que los nodos están conectados a un solo canal de comunicaciones. Dado que los datos comparten el mismo medio es posible compartir información, la desventaja con respecto al tráfico, ya que que se producen colisiones de datos.

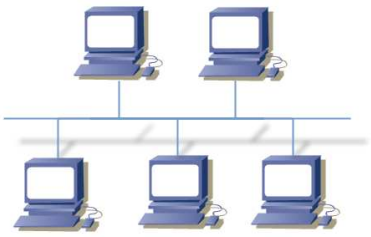


Figura 2.4: Topología tipo Bus

Anillo

En esta topología las estaciones de trabajo se conectan formando un anillo, una con otra consecutivamente, estos son capaces de recibir y transmitir datos. La desventaja de esta topología es que si un nodo falla se rompe el anillo, por ello se tiene una variante llamada *Anillo Doble* en el cual la modificación consta de agregar una conexión mas en cada nodo para que la union entre ellos sea doble y si se rompe un anillo este el otro en funcionamiento. Los anillos no están conectados entre si y se usa uno por vez, para incrementar la confiabilidad y flexibilidad de la red.

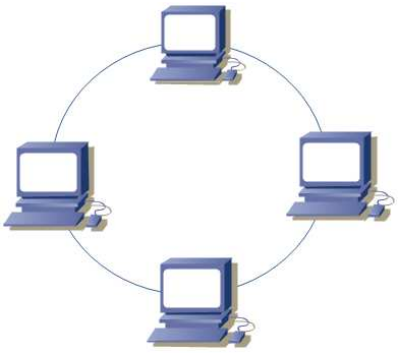


Figura 2.5: Topología tipo Anillo

Árbol

La topología de árbol es una variante de la estrella. Como en la estrella los nodos están conectados a un concentrador central que controla el tráfico. No todos los dispositivos se conectan directamente al concentrador central, el flujo es jerárquico dependiendo de la capa y ramificación, por lo tanto también hay concentradores secundarios etc.

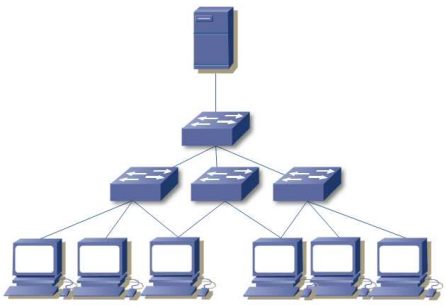


Figura 2.6: Topología tipo Arbol

2.1.2. Topologías Lógicas

Es la forma en que una red transfiere tramas de un nodo al siguiente, esta configuración consiste en conexiones virtuales entre los nodos de una red independientemente de su distribución física, poseen protocolos específicos que realizan esta acción y definen las rutas de las señales lógicas. La topología lógica influye en el tipo de trama de red y control de acceso a los medios que se utilizan *La topología física o cableado de una red probablemente no sea la misma que la topología lógica.* La topología lógica de una red esta estrechamente relacionada con el mecanismo que se utiliza para administrar el acceso a la red. Los métodos de acceso proporcionan los procedimientos para administrar dicho acceso a la red.

Bus

También llamada broadcast fue inventada en 1973, cuando la comunicación no era muy eficaz y las computadoras no podían evitar el envío de datos por el mismo canal al mismo tiempo. Como surgimiento resultó posible superar las limitaciones de las primeras redes. Por medio del estándar 802.3 CSMA/CD explicado más adelante, se genera una administración en la transmisión de datos. Esto significa que cada host [1] envía sus datos hacia todos los demás host conectados a la red. Estos no siguen ningún orden, así que el acceso se concede hacia el primero que envía información al medio. La mayor parte del tráfico en Internet se origina y termina en conexiones ethernet cuya tecnología es el bus lógico para la transmisión de datos.

Token Ring

Esta topología permite el acceso múltiple a una cantidad de nodos y comunicarse con los mismos medios compartidos. Los datos desde un solo nodo pueden colocarse en el medio en cualquier momento. Cuando muchos nodos comparten el acceso al medio , se requiere un método de enlace de datos que regule la transmisión de los mismos y que por consiguiente, reduzca las colisiones entre las distintas señales. Este tipo de transmisión controla el acceso al transmitir un token eléctrico de forma secuencial a cada host. Cuando un host recibe el token, eso significa que el host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir. Las redes que trabajan sobre token ring al contrario de las Broadcast admiten mucha presión ejercida por una LAN con un gran número de nodos.

FDDI

La tecnología de acceso es a través de lineas de fibra óptica. La redundancia se realiza mediante un doble anillo paralelo con rotación de los datos en sentidos inversos, esto último permite capturar los errores del primero, posee detección y corrección de errores. El token circula entre los equipos a velocidades muy altas. Si no llega a un equipo después

[1] Se le llama host a un sistema informático conectado a la red

de un determinado periodo de tiempo, el equipo considera que se ha producido un error en la red.

2.2. Modelo OSI

El modelo de interconexión de sistemas abiertos es una representación abstracta en capas, creada como guía para el diseño del protocolo de red *ver fig 2.7*. El modelo OSI divide el proceso de networking en diferentes capas lógicas, cada una de las cuales tiene una funcionalidad única y a la cual se le asignan protocolos y servicios específicos.
En este modelo, la información se pasa de una capa a otra, comenzando en la capa de aplicación en el host de transmisión, siguiendo por la jerarquía hacia la capa física y pasando por el canal de comunicaciones o medio al host destino, donde la información vuelve a la jerarquía y termina en la capa de aplicación.

Figura 2.7: Modelo OSI

2.2.1. Capa 7 Aplicación

La capa de aplicación es la capa superior de los modelos OSI y TCP/IP. En esta capa se proporciona la interfaz entre las aplicaciones que se utilizan y la red subyacente en la cual se transmiten los mensajes. En esta capa ocurre toda la interacción entre el usuario y su equipo de cómputo. Las responsabilidades de la capa 7 son identificar y establecer la disponibilidad de comunicación del destino, así como determinar los recursos para que exista esa comunicación. Dentro de esta capa de aplicación, existen dos formas de procesos o programas de software que proporcionan acceso a la red: aplicaciones y servicios.

- Aplicaciones reconocidas por la red.
  Las aplicaciones son los programas de software que utiliza el usuario, son reconocidas y se comunican directamente con la red tales como clientes de correo electrónico y exploradores web.

- Servicios de la capa de aplicación.
  Estos son servicios que necesitan de esta capa para utilizar algún recurso de la red como la transferencia de archivos o cola de impresión. aúnque son transparentes para el usuario estos servicios preparan los datos para su transferencia. Diferentes tipos de datos ya sea texto, gráfico o vídeo, requieren de diversos servicios de red para asegurarse de que estén bien preparados para procesar las funciones de las capas inferiores del modelo OSI. Cada servicio utiliza protocolos que definen los estándares y formatos a utilizarse.

Un protocolo es una regla o conjunto de reglas y estándares para la comunicación entre las computadoras cuando se envían datos entre ellas. Ambos, emisor y receptor deben reconocer el mismo protocolo. Al grupo de protocolos es denominado *protocolo suite o protocol stack*. Sin protocolos, la red de datos no tendría una manera común de formatear y direccionar los datos. Los protocolos de esta capa *ver fig2.8* se utilizan para intercambiar los datos entre los programas que se ejecutan en los host origen y destino. Algunos de ellos son:

Protocolos de Capa 7.	
DNS	Domain Name Service.
DHCP	Dynamic Host Configuration Protocol.
NAT	Network Address Translation.
FTP	File Transfer Protocol.
HTTP	Hypertext Transfer Protocol.
POP3	Post Office Protocol v3.
IMAP4	Internet Message Access Protocol rev 4.
NTP	Network Time Protocol.
SMTP	Simple Mail Transfer Protocol.
SNMP	Simple Network Management Protocol.
TELNET	TCP/IP Terminal Emulation Protocol.
TFTP	Trivial File Transfer Protocol.

Figura 2.8: Protocolos de Aplicación

Dentro de la capa de aplicación, existen dos formas de procesos o programas de software que proporcionan acceso a la red.

2.2.2. Capa 6 Presentación

Esta capa se encarga de la representación de la información, de manera que aúnque múltiples equipos tengan distintas representaciones de caracteres, números, sonido e imágenes, los datos lleguen de manera reconocible. En esta capa se tienen tres funciones principales.

- Codificación y conversión de datos de la capa de aplicación para garantizar que los datos del dispositivo de origen se puedan interpretar por la aplicación adecuada en el dispositivo de destino.
- Compresión de los datos de forma que los pueda descomprimir el dispositivo de destino.
- Cifrado de los datos para el recibo y transmisión.

2.2.3. Capa 5 Sesión

Como lo indica el nombre, las funciones en esta capa crean y mantienen diálogos entre las aplicaciones de origen y destino. Esta capa maneja el intercambio de información para iniciar los diálogos y mantenerlos activos y para reiniciar sesiones que se interrumpieron o desactivaron durante un periodo de tiempo prolongado. En el nivel de sesión proporciona los siguientes servicios:

- Control de Diálogo: Este puede ser simultáneo en los dos sentidos (full-duplex) o alternado (half-duplex).
- Agrupamiento: El flujo de datos se puede marcar para definir grupos de datos.
- Recuperación: La capa de sesión puede proporcionar un procedimiento de comprobación, de tal forma que si ocurre algún tipo de fallo entre los puntos de comprobación, la entidad de sesión puede transmitir todos los datos desde el último punto de comprobación y no desde el principio.
- Comprobación: La entidad de sesión puede transmitir todos los datos desde el último punto de comprobación y no desde el principio.

La capa de sesión surge como una necesidad de organizar y sincronizar el diálogo y controlar el intercambio de datos.

2.2.4. Capa 4 Transporte

La capa de transporte permite la segmentación de datos y brinda el control necesario para reemsamblar las partes dentro de los distintos streams de comunicación. Es decir que esta capa garantiza que los paquetes sean recibidos. Las principales responsabilidades de esta capa son:

- Rastreo de comunicación individual entra aplicaciones en los host de origen y destino.
  Cualquier host puede tener múltiples aplicaciones que se comunican a través de la red. Cada una de estas aplicaciones se comunicará con una o mas aplicaciones en host remotos. Esta capa mantiene los streams de comunicación múltiple entre dichas aplicaciones.

- Segmentación de datos y manejo de cada parte.
  Así como cada aplicación crea datos de stream para enviarlos estos se preparan para el envío, los protocolos de la capa de transporte describen los servicios que segmentan estos datos de la capa de aplicación. Esto incluye el encapsulado necesario en cada sección de datos. Cada sección de datos de aplicación requiere que se agreguen encabezados en la capa de transporte para indicar la comunicación a la cual esta asociada.

- Re ensamble de segmentos en streams de datos de aplicación.
  En el host de recepción, cada sección de datos se puede direccionar a la aplicación adecuada y estas secciones pueden reconstruirse para generar una secuencia completa de datos que sea útil para la capa de aplicación.

- Identificación de diferentes aplicaciones.
  Para pasar streams de datos a las aplicaciones adecuadas, la capa debe identificar la aplicación meta. Se asigna un identificador a la aplicación. Los protocolos TCP/IP denominan a este identificador número de puerto. A todos los procesos de software que requieren acceder a la red se les asigna un número de puerto exclusivo en este host. Este número de puerto se utiliza en el encabezado de la capa de transporte para indicar qué aplicación se asocia a qué parte.

Las funciones principales que especifican los protocolos de la capa de transporte son:

- Segmentación y reemsamble:
  La mayoría de las redes tienen una limitación en la cantidad de datos que se pueden incluir en una simple PDU[2]
  La capa divide los datos en bloques de datos de un tamaño adecuado. El destino re ensambla los datos antes de enviarlos a la aplicación o servicio de destino.

- Multiplexaje de conversación:
  La asignación del puerto a las aplicaciones hace que se reconozca la aplicación. Los dos protocolos más comunes de la capa de transporte del conjunto de protocolos TCP/IP son:

[2]Abreviatura de Protocol Data Unit. Término que se usa para describir datos mientras se mueven de una capa del modelo OSI a otra.

- **Protocolo de Datagramas de usuario UDP.**
  UDP es un protocolo simple, sin conexión, descrito en el RFC 768. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. Las porciones de comunicación en UDP se llaman datagramas a continuacion se explica la cabecera UDP *ver fig2.9.*

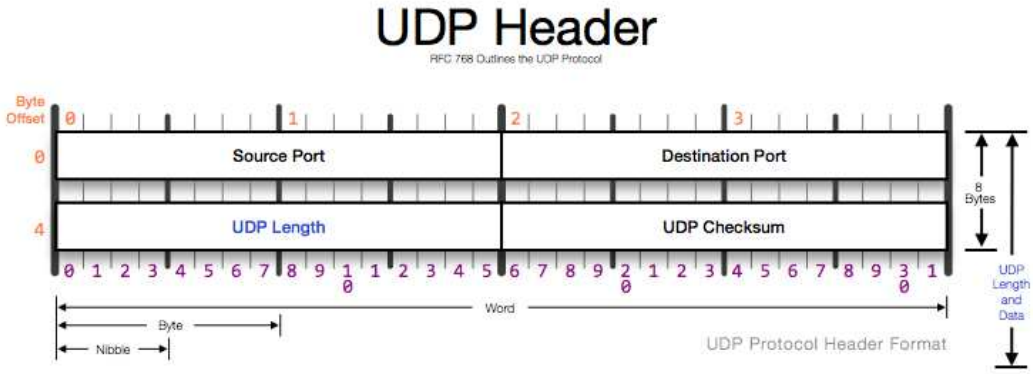


Figura 2.9: Cabecera UDP

El formato de la cabecera UDP es la siguiente:

- *Source Port:* Es el número de puerto de origen, se usan para desmultiplexar datagramas en el receptor final.

- *Destination Port:* Es el número de puerto destino del host remoto hacia el que recibirá los datagramas.

- *UDP Lenght:* Longitud del mensaje,contiene la longitud de la cabecera y la longitud de los datos del usuario. Su valor mínimo es de 8 el cual representa la longitud de la cabecera.

- *UDP Checksum:* El valor calculado no es un campo obligatorio, se utiliza cuando los mensajes deben ser encapsulados y transmitidos entre dos computadoras en una red, sin establecer ninguna entre ellas. Como no es orientado a conexión se permite que los datos sean enviados del emisor al receptor sin proveer el número de puerto. Lo cual lo hace poco confiable.

Este protocolo provee funciones básica y tiene sobrecarga menor que TCP. Las aplicaciones que utilizan UDP son: DNS,DHCP,TFTP, Stream de video, VOIP.

- **Protocolo de control de transmisión TCP**
  TCP es un protocolo orientado a conexión descrito en el RFC 793. El TCP utiliza recursos adicionales para ganar funciones. Dichas funciones adicionales son: el orden de entrega, entrega confiable y control de flujo. Cada segmento TCP contiene 20 bytes en el encabezado que encapsula los datos en la capa 7 *ver fig2.10*.

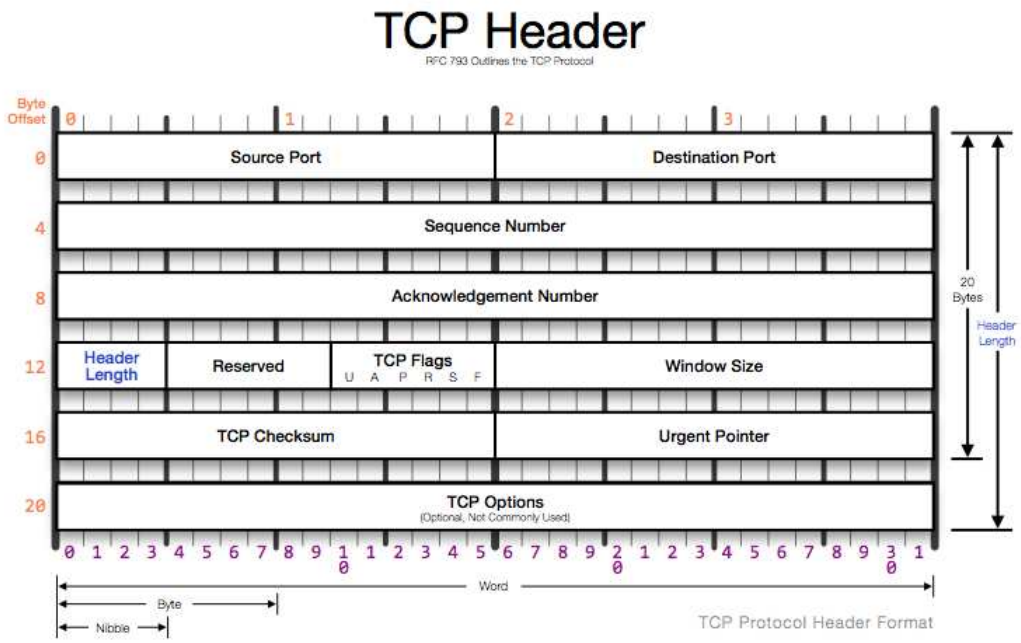


Figura 2.10: Cabecera TCP

El formato de la cabecera TCP es el siguiente:

- *Source port* : Es el puerto de origen.
- *Destination port*: Es el puerto destino.
- *Sequence number*: Es el número de secuencia es el primer byte que representa al paquete.
- *Acknowledgement number*: Este campo contiene el siguiente número se secuencia que el emisor espera recibir, este rubro se utiliza solo cuando la bandera de ACK esta prendida.
- *Header Lenght*: La longitud de la cabecera es de 32 bits necesarios ya que el campo de opciones es de longitud variable.
- *Reservado*
- *URG*: El puntero de urgente es válido.
- *ACK*: Hace que la bandera de reconocimiento sea valida.
- *PSH*: Se activa la prioridad alta para la aplicación.
- *RST*: Restablece la conexión.

- *SYN*: Esta activo cuando una conexión se establece.
- *FIN*: El remitente termina de enviar datos.
- *Window Size*: Es el máximo número de bytes que el remitente puede aceptar.
- *TCP checksum*: Calcula y verifica las cabeceras y los datos.
- *Urgent Pointer*: Solo es válido si el URG esta activo,este modo es una forma de transmitir datos de emergencia hacia el otro extremo de la conexión.
- *Options*: Longitud variable.

Se pasan los datos a la red hasta que se conoce el destino y esta listo para recibirlo. Luego TCP administra el flujo de datos y reenvía todos los segmentos de datos de los que recibió acuse a medida que se reciben en el destino. Esta confiabilidad impone una sobrecarga a la red en términos de encabezados de segmentos mucho mas grandes y mas tráfico de red. Las aplicaciones que utilizan TCP son: Exploradores Web,Correo electrónico y Transferencia de archivos.

La diferencia clave entre TCP y UDP es la confiabilidad.

En TCP antes de que un host envíe datos la capa de transporte inicia un proceso para crear una conexión con el destino. Dicha conexión permite el rastreo de una sesión o stream de comunicación entre los host. Este proceso asegura que cada host tenga conocimiento de la comunicación y se prepare. Una conversación completa de TCP necesita establecer una sesión entre los host de ambas direcciones. Por medio del 3-way handshake o enlace de tres vías el cual se explica a continuación *ver fig2.11.*

- El enlace de tres vías consta de banderas en los paquetes que se envían. El host inicial envía un mensaje con la bandera de sincronización (SYN), para iniciar la conexión, estos paquetes llevan número de secuencia en la cabecera TCP.

- El remitente reconoce la bandera y número de secuencia por lo que envía de regreso otro paquete con la bandera de reconocimiento y sincronización (ACK+SYN) junto con el número de secuencia siguiente, así mismo se inicia su propio número de secuencia.

- Por último el host inicial responde con un paquete con el siguiente número de secuencia propio y una bandera de reconocimiento (ACK) con el número de secuencia que el otro host espera. Cuando este proceso se ejecuta se establece una conexión por TCP.

Después de establecer una sesión, el destino envía un acuse de recibo al origen por los segmentos que recibe. Estos acuses de recibo forman la base de la confiabilidad dentro de la sesión TCP. Cuando el origen recibe un acuse de recibo, reconoce que los datos se han entregado con éxito y puede dejar de rastrearlos. Si el origen no recibe el acuse de recibo dentro de un tiempo predeterminado, retransmite esos datos al destino. Los servicios basados en TCP y UDP mantienen un seguimiento de las diversas aplicaciones que

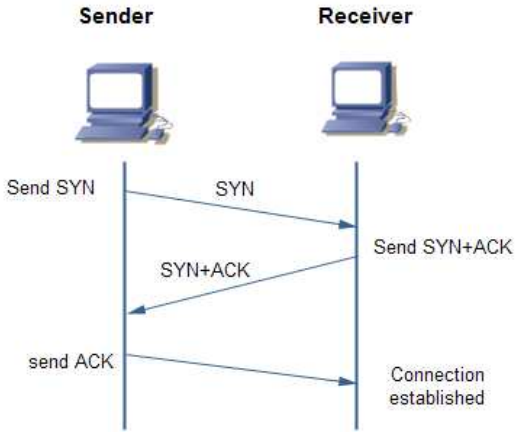


Figura 2.11: Enlace de tres vías.

se comunican. Para diferenciar los segmentos y datagramas para cada aplicación, tanto TCP como UDP cuentan con campos de encabezados que pueden identificar de manera exclusiva esta aplicaciones. Dicho encabezado contiene un puerto origen y uno destino. El número de puerto origen es el número para esta comunicación asociado con la aplicación que origina la comunicación en el host local. El número de puerto de destino es el número para esta comunicación asociado con la aplicación de destino que origina la comunicación en host.

Hay diversos tipos de puerto:

- *Puertos bien conocidos: (números del 0 al 1023)* .
  Estos números se reservan para servicios y aplicaciones, al definir estos puertos para las aplicaciones cliente se pueden programar para solicitar una conexión a dicho puerto y su servicio asociado.

- *Puertos Registrados:(números del 1024 al 49151)* .
  Estos números de puerto se asignan a procesos o aplicaciones del usuario. Dichos procesos son principalmente aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes que recibirán un puerto bien conocido. Cuando no se utilizan para un recurso del servidor, estos puertos se pueden utilizar también en forma dinámica por el cliente como puerto de origen.

- *Puertos dinámicos o privados:(números 49152 a 65535)* .
  También conocidos como puertos efímeros, están usualmente asignados de forma dinámica a las aplicaciones cliente cuando se inicia una conexión.

2.2.5. Capa 3 Red

La capa de red, provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte extremo a extremo la capa de Red emplea cuatro procesos básicos: Direccionamiento, Encapsulado, Enrutamiento y Desencapsulado.

1. **Direccionamiento.** La capa debe proporcionar un mecanismo para direccionar hacia los dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final,este debe tener una dirección única, para redes IPv4 llamaremos host a los dispositivos con una dirección.

2. **Encapsulado.** Los dispositivos no pueden ser identificados solo con una dirección; las PDU deben contener mas información como lo son host origen y destino. De esta manera se completa el proceso de encapsulado, el paquete se envía a la capa siguiente para la preparación de su transporte a través del medio.

3. **Enrutamiento.** Este servicio consiste en dirigir los paquetes a su host destino. Si el destino y origen no están dentro de la misma red. Este tendría que recorrer varias redes, a lo largo de su ruta cada paquete es guiado para que llegue a su destino. Esto por medio de dispositivos intermediarios que conectan las redes llamados routers. La función del router es seleccionar las rutas y dirigir paquetes hacia su destino.

4. **Desencapsulamiento.** Finalmente el paquete llega a su destino y el host destino examina la dirección destino para verificar que el paquete fue direccionado correctamente, de ser así el paquete es desencapsulado y se envía al servicio adecuado en la capa de transporte. Los protocolos de esta capa son: Protocol Internet version 4 y 6 , IPv4 e IPv6, Intercambio Novell de paquetes de internetwork (IPX),Servicio de red sin conexión (CLNS/DECNet) A continuación se muestra la cabecera el protocolo IP*ver fig2.12*.

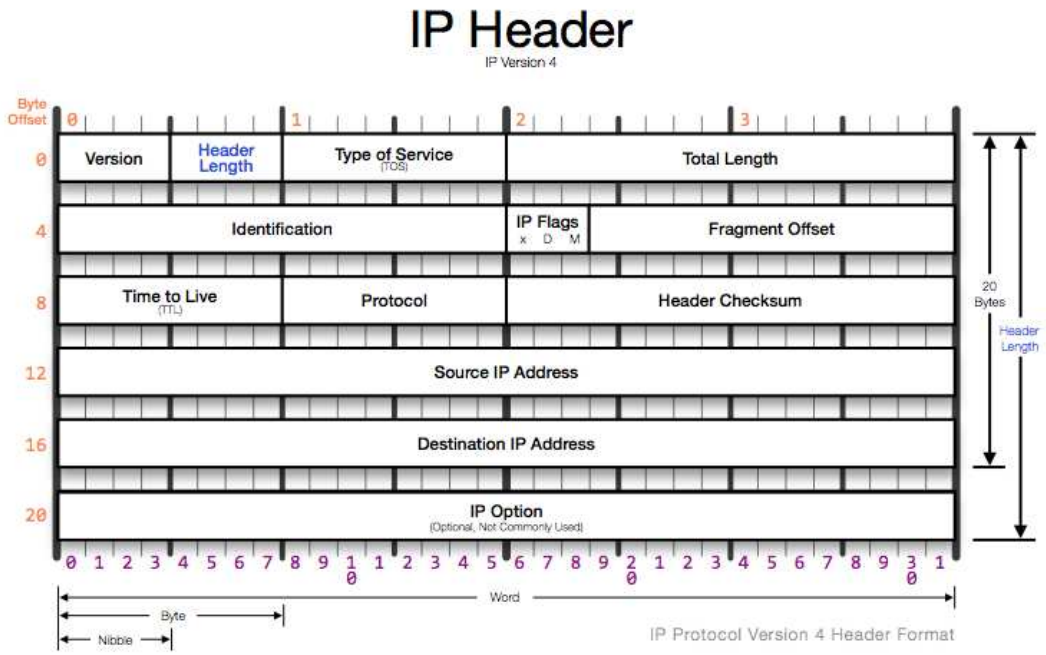


Figura 2.12: Cabecera IPv4

- *Version*: Este campo describe el formato de la cabecera a utilizar, IPv4 o IPv6.
- *Header Length*: La longitud o tamaño de cabecera en bits. Su valor mínimo es de 5 bits para una cabecera correcta y el máximo son 15.
- *Type of Service*: Este campo describe el tipo de Servicio (ToS). contiene un valor binario de 8 bits que se usa para determinar la prioridad de cada paquete. Este valor permite aplicar un mecanismo de calidad de servicio QoS a paquetes de alta prioridad, como aquellos que llevan datos de voz en telefonía. El router o dispositivo que procesa los paquetes puede ser configurado para decidir que paquete es enviado primero basado en el valor ToS.
- *Total Length*: Es el total, del datagrama, incluyendo los datos, el tamaño mínimo es de 576 bits, si hay fragmentación entonces se establece el tamaño del fragmento en esta sección.
- *Identification*: Es el identificador único del datagrama, se utiliza en caso de que el datagrama sea fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro. El remitente debe asegurar un valor único para el origen y el destino.
- *IP Flags*: Actualmente es utilizado para especificar valores relativos a la fragmentación de paquetes. Los 3 bits son:
  - X: Es el bits 0, es reservado y lleva el valor de 0.

  - D: Si su valor es 0 quiere decir que es divisible, si es 1 no es divisible su abreviación es DF.
  - M: Si su valor es 0 quiere decir que el ultimo fragmento de la secuencia, si su valor es 1 entonces pertenece a un fragmento intermedio su abreviacion es MF.

- *Fragment Offset*: Este campo indica la posición del fragmento en unidades de 64 bits, que ocupa el paquete actual dentro del datagrama, el primer paquete de datos de una secuencia de fragmentos tendra el valor de 0.

- *Time to Live*: El campo de Tiempo de vida o TTL, es un valor binario de 8 bits que indica el resto de vida del paquete. El valor TTL disminuye al menos en uno cada vez que el paquete es procesado por un *router*. Cuando el valor se vuelve cero, el *router* descarta o elimina el paquete y es eliminado del flujo de datos de red. Este mecanismo evita que los paquetes que no pueden llegar a destino sean reenviados indefinidamente entre los routers o dispositivos intermedios causando un **routing loop**. Si se permitiera que los loops de enrutamiento continúen, la red se congestionaría con paquetes de datos que nunca llegarían a su destino. La disminución del TTL garantiza que este finalmente llegue a cero y el paquete vencido se descartará.

- *Protocol*: Este valor binario de 8 bits indica el tipo de contenido que el paquete traslada. El campo protocolo permite a la capa de red pasar los datos al protocolo apropiado de la capa superior.

- *Header Checksum*: La suma del control de la cabecera, es un número que se recalcula cada vez que algun nodo cambia alguno de los campos.

- *Source IP address*: El campo de dirección IP de origen contiene un valor binario de 32 bits que representa la dirección de host de capa de red de origen del paquete. Se mantiene inalterable a lo largo de todo el recorrido, habilita al host destino para responder al origen si es necesario.

- *Destination IP address*: Este campo de dirección IP de destino con un valor binario de 32 bits contiene la dirección destino la cual es inalterable a lo largo del recorrido del paquete y esta habilita a los routers a cada salto para reenviar el paquete hacia su destino.

- *IP Option*: No es un campo obligatorio contiene un indicador de copia, verdadero o falso y cuatro clases de opcion: control, reservado, depuración y mediciones.

La función de la capa de red es la transferencia de datos desde el host que origina los datos hacia el host que los usa. Si el host de destino esta en la misma red que el host de origen el paquete se envía sin necesidad de un *router*. Sin embargo, si el host de origen no esta en la misma red, el paquete puede llevar una PDU a través de muchas redes, si es así la información que contiene no es alterada por ningún *router* cuando se toman las decisiones de envió. En cada salto, las decisiones de envío se basan en la información del encabezado del paquete. Este paquete se mantienen intacto a través de todo el proceso

desde el host de origen hasta el destino, para que esta comunicación sea exitosa, y se de entre dos redes diferentes el paquete se envía hacia su gateway, si este es enviado a un segundo router es responsabilidad del dispositivo el reenvío del paquete. En los dos tipos de protocolo se coloca la dirección IPv4 del host de origen en el encabezado del paquete como la dirección de origen. Las direcciones son de dos tipos: públicas y privadas. La amplia mayoría de las direcciones en el rango de host unicast son direcciones públicas. Estas están diseñadas para ser utilizadas en los host de acceso publico desde internet. aún dentro de estos bloques de direcciones, existen muchas direcciones designadas para otros fines específicos. El uso de las direcciones públicas es regulado por la Autoridad de números asignados de Internet (IANA) es un soporte maestro de direcciones IP, hasta mediados de los noventa la IANA asigno el resto de las direcciones IP a diversos registros para que estos realicen la administración de áreas regionales o con propósitos particulares, estas compañias de registro se llaman registros regionales de Internet (RIR).
Las principales son: AfriNIC (región Africa),APNIC (región Asia/Pacifico), ARIN (región América Norte),LACNIC (región Latinoamericana y caribe) y RIPE NCC (Europa, Medio Oriente y Asia Central). Estos bloques de direcciones Ip son suministrados por un ISP (Proveedor de Servicios de Internet). Dependiendo del nivel del servicio requerido y disponible, los clientes usan diferentes niveles de ISP. Estos niveles se designan mediante una jerarquía basada en el nivel de conectividad al backbone.

- Nivel 1.
  Parte superior de la jerarquía, son grandes proveedores a nivel nacional o internacional, ofrecen conexiones y servicios altamente confiables. Lo cual se convierte en las principales ventajas para este nivel dado que hay menos oportunidades de falla o cuellos de botella en el tráfico, la única desventaja es el costo elevado.

- Nivel 2.
  Estos ISP generalmente se centran en los clientes de la empresa o institución, suelen tener recursos de TI para ofrecer sus propios servicios de red.

- Nivel 3.
  El objetivo de estos ISP son los mercados minoristas y del hogar en una ubicación específica, su necesidad principal es la conectividad y soporte. Cabe mencionar que la disminución de velocidad en cada nivel es por la lejanía de la conexión al backbone. aunque la mayoría de las direcciones son públicas designadas para uso en redes a las que se accede desde Internet, existen bloques de direcciones que se utilizan en redes que requieren o no acceso limitado a Internet. Estas direcciones se denominan privadas.

  Los bloques de direcciones privadas son:

  - De 10.0.0.0 a 10.255.255.255
  - De 172.16.0.0 a 172.31.255.255
  - De 192.168.0.0 a 192.168.255.255

Por lo general los host que no requieren acceso a internet pueden utilizar las direcciones privadas sin restricciones. Sin embargo las redes internas aún deben diseñar esquemas de direcciones de red, para garantizar que los hosts de las redes privadas utilicen direcciones IP que sean únicas dentro de su entorno de *networking*. Históricamente la RFC1700 agrupaba rangos de unicast en tamaños específicos llamados direcciones de clase A, B y C. También definía a las direcciones de clase D y E.

- Bloques de clase A.
  Se diseño este bloque para admitir redes extremadamente grandes con mas de 16 millones de direcciones host. Estas direcciones usaban un prefijo /8 donde el primer octeto, es decir; los primeros 8 bits indican la dirección de red,el resto se usaba para las direcciones host.

- Bloques de clase B.
  Este espacio fue diseñado para satisfacer la necesidades de las redes de tamaño moderado a grande con mas de 65,000 hosts. Una dirección B usaba los dos octetos de orden superior para indicar la dirección de red. Los dos octetos restantes especificaban las direcciones host. La clase B tenía una asignación de direcciones un tanto mas eficiente que la clase A debido a que dividía equitativamente el 25 % del total del espacio total de las direcciones IPv4 entre aproximadamente 16,000 redes.

- Bloques de clase C.
  Esta clase era de las direcciones mas antiguas disponibles. Este espacio proporciona direcciones de redes pequeñas con un máximo de 254 hosts. Solo se utilizaba el ultimo octecto para las direcciones de host.

No todos los requisitos de las organizaciones se ajustaban a una de estas tres clases. La asignación con clase de espacios de direcciones a menudo desperdiciaba muchas direcciones, lo cual agotaba la disponibilidad de direcciones IPv4. Este métodos se dejo de utilizar en los 90s actualmente se utiliza el direccionamiento sin clase, en el cual se asignan los bloques de direcciones adecuados según la cantidad de host a las compañias u organizaciones sin tener en cuenta la clase unicast.
Es necesario que la asignación del espacio de direcciones de la capa de red dentro de la red institucional este bien diseñada. Los administradores de red no deben seleccionar de forma aleatoria las direcciones utilizadas en sus redes. El fin de la asignación de direcciones dentro de la red deber ser planificada y documentada a fin de:

- **Evitar duplicación de direcciones.** Cada host en una internetwork debe tener una dirección única. Sin la planificación y documentación adecuadas de estas asignaciones de red, se podría fácilmente asignar una dirección a mas de un host.

- **Proporcionar y controlar el acceso.** Algunos host proporcionan recursos para red interna y externa, como los servidores. Estos pueden ser controlados por la dirección de capa 3. Si estas direcciones no son planificadas y documentadas, no es posible controlar fácilmente la seguridad y accesibilidad de los dispositivos.

- **Controlar seguridad y rendimiento.** De igual manera es necesario controlar la seguridad y el rendimiento de los host de la red en general, con la realización de estas actividades de monitorizacion y planeación es posible identificar el dispositivo en la red que tenga problemas.

Para hacer que una red LAN se enrute correctamente se necesita una dirección IP que realice la conexión hacia el exterior esta dirección recibe el nombre de **Gateway**, conocido como default gateway, es necesaria para enviar un paquete fuera de la red local. Si la porción de red de la dirección de destino del paquete es diferente de la red del host origen, el paquete tiene que hallar la salida fuera de la red original. Este gateway es una interfaz conectada a la red local, y los host están configurados para reconocer la dirección como gateway.

Dispositivos de Red de Capa 3.

Router

En el centro de una red se encuentra un *router*, este dispositivo conecta una red con otra red; es decir que un *router* es la unión o intersección que conecta múltiples redes IP *ver fig2.13*. Un router es responsable de la entrega de paquetes en diferentes redes a su debido tiempo, ademas del reenvió de paquetes un *router* proporciona otros servicios. Tales como asegurar la disponibilidad de conexión de red, integran servicios de red, voz y datos, y disminuyen el impacto de gusanos, virus y otros ataques en la red mediante la autorización o el rechazo del reenvió de paquetes. Un *router* es una computadora,el primero fue utilizado para la Red de la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de los Estados Unidos, con un procesador de mensajes de interfaz el 30 de agosto de 1969. Como es una computadora, posee, CPU, RAM y ROM y un sistema operativo llamado IOS.

Figura 2.13: Dispositivo de capa 3: router.

Su principal función es enrutar los paquetes, esto quiere decir que el dispositivo determina el mejor camino a seguir para un paquete mediante una tabla de enrutamiento. Esta se utiliza para encontrar la mejor coincidencia entre la dirección IP de destino de un paquete y una dirección de red en la tabla, de este modo el *router* determina que interfaz de salida reenviara el paquete estas rutas pueden ser estáticas, dinámicas o los dispositivos que estén conectados directamente.

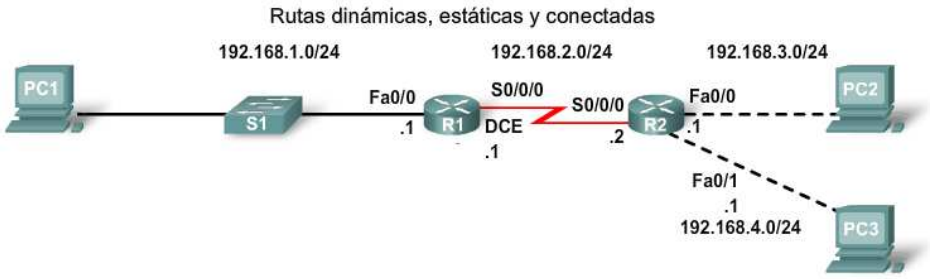


Figura 2.14: Tipos de Rutas.

Las tablas de los routers poseen los datos sobre cada red conectada directamente,*ver fig2.14* y la interfaz que la posee. Si la ruta es una red remota se tiene la métrica de enrutamiento y la distancia administrativa La distancia administrativa (AD) es una clasificación de la confiabilidad de una fuente de información de enrutamiento. Generalmente se expresa con un valor numérico entre 0 y 255. Mientras mayor sea el valor, menor será la clasificación de la confiabilidad. Si un *router* tiene diferentes protocolos en su tabla, seleccionará el que tenga la ruta más baja.
La métrica es un método por el cual un algoritmo de enrutamiento determina cuál ruta es mejor que otra. Las métricas incluyen ancho de banda, costo de comunicación, retardo, conteo de saltos, carga etc. Las cuales se explican a continuación:

- Conteo de saltos: Es una métrica simple que cuenta la cantidad de routers que un paquete tiene que atravesar.
- El ancho de banda: Influye en la selección de rutas al preferir la ruta con el ancho de banda más alto.
- Carga: Considera la utilización de tráfico de un enlace determinado.
- Retardo: Considera el tiempo que tarda un paquete en atravesar una ruta.
- Confiabilidad: Evalúa la probabilidad de una falla de enlace, calculada a partir del conteo de errores de la interfaz o las fallas de enlace previas.
- Costo: Es un valor determinado por el *router* o el administrador de red para indicar la preferencia de una ruta. El costo puede representar una métrica, o una combinación de las mismas.

Para comprender aún más el comportamiento de un *router* se tienen 3 principios sobre las tablas de enrutamiento:

- *Cada router toma sus propias decisiones de forma independiente, según la información de su tabla de enrutamiento.*
- *El hecho de que un router tenga información en su tabla de enrutamiento no significa que los otros routers tengan la misma información.*

- *La información de enrutamiento acerca de una ruta de una red a otra no proporciona información de enrutamiento acerca de la ruta inversa o de retorno.*

Dado que los routers no necesariamente tienen la misma información en sus tablas de enrutamiento, los paquetes pueden recorrer la red en un sentido, utilizando un camino y regresar por otro camino diferente. A esto se le denomina enrutamiento asimétrico. Este tipo de enrutamiento es mas común en Internet que en las redes locales.

Se considera un dispositivo de capa 3 ya que su decisión principal de reenvío se basa en la información del paquete que contiene la dirección IP. Cuando un router recibe un paquete, examina su dirección IP de destino. Si la dirección IP no pertenece a ninguna de las redes del router conectadas directamente, el router envía ese paquete hacia otro router que tenga en su tabla de enrutamiento el destino correcto. Cuando encuentra una coincidencia con la dirección de red en la tabla de otro router, este encapsula el paquete IP en trama de enlace de datos *ver fig2.15* para ser reenviado hacia su destino. Es probable que los routers reciban paquetes de tipo trama de enlace de datos, como PPP o Ethernet. Esta encapsulacion depende del tipo de interfaz del router y del tipo de medio al que se conecta. Las diferentes tecnologías de enlace pueden incluir tecnologías LAN como Frame Relay,ATM, y Punto a Punto. La imagen muestra las capas sobre el modelo OSI sobre las que se lleva acabo el proceso de enrutamiento de un punto a otro.

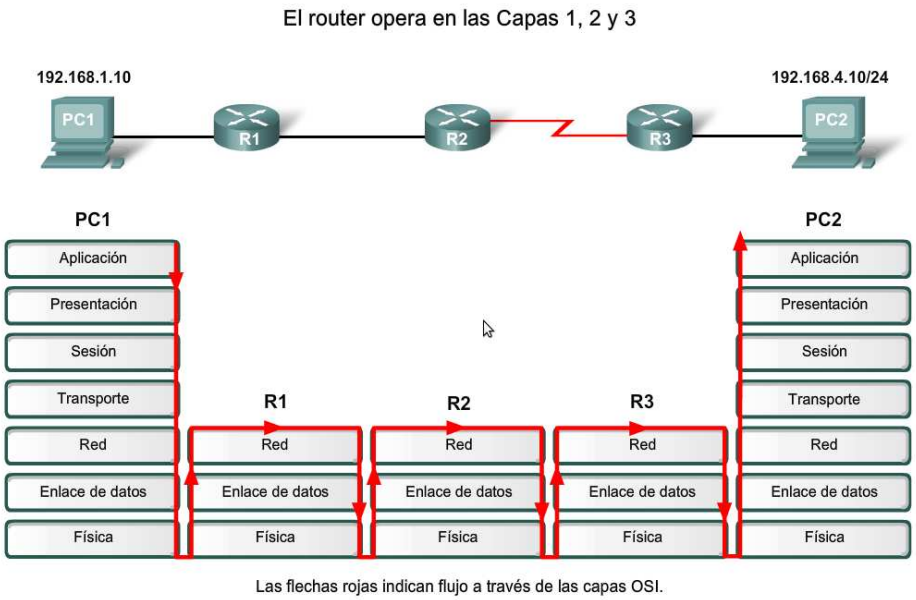


Figura 2.15: Funcionamiento de router en capas del modelo OSI

Es importante para los administradores de red, conocer la tabla de enrutamiento a profundidad cuando se resuelven problemas de red. Comprender la estructura y el proceso de búsqueda de la tabla ayuda a diagnosticar cualquier problema.

2.2.6. Capa 2 Enlace de datos.

La función de la capa de enlace de datos es preparar los paquetes de la capa de red pasa su transmisión y controlar el acceso a los medios físicos[3]. Los paquetes dejan de llamarse así y se convierten en tramas, una trama contiene tres elementos: encabezado, datos y una cola, también llamada trailer la contiene el código de detección de errores. La descripción de la trama es un elemento clave de cada protocolo *ver fig2.16*.

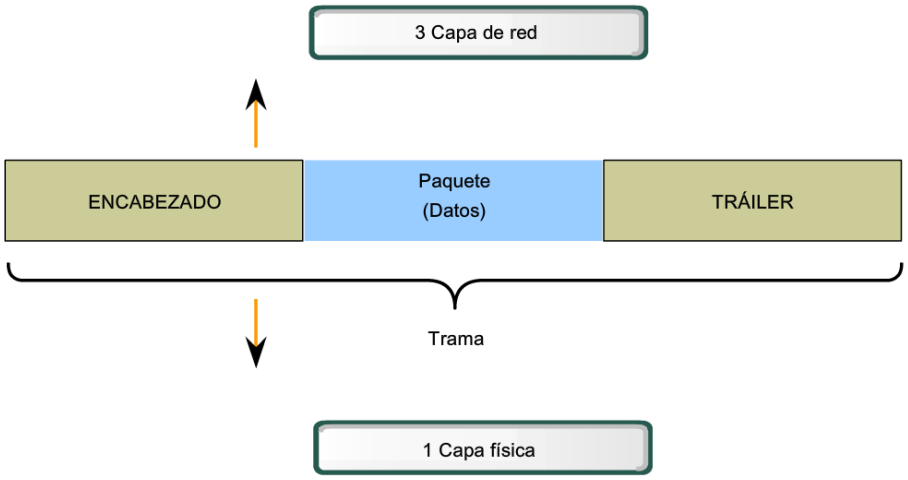


Figura 2.16: Formato de Trama

Como se ve en la *fig2.17* el encabezado de trama contiene la información de control que especifica el protocolo de capa de enlace de datos para la topología lógica específica y los medios de uso. La información de control de trama es diferente para cada tipo de protocolo y es utilizada por dicho protocolo para proporcionar las características demandadas por el entorno.

Figura 2.17: La función del encabezado.

Los campos típicos del encabezado de trama incluyen:

- *Inicio de trama:* Indica el comienzo de la trama.
- *Dirección origen y destino:* Indica los nodos de origen y destino en los medios.
- *Prioridad/calidad:* Indica un tipo particular de servicio de comunicación para el procesamiento.

[3]Los medios físicos para la transferencia de información entre nodos, es decir el material que realmente transporta las señales, cable de cobre,fibra óptica etc.

- *Tipo:* Indica el servicio de la capa superior que se incluye en la trama.
- *Control de conexión lógica:* Se utiliza para establecer la conexión lógica entre nodos.
- *Control de enlace físico:* Se utiliza para iniciar y detener el tráfico a través de los medios.
- *Control de congestión:* Indica congestión en los medios.

Los protocolos de la capa de enlace de datos agregan un trailer en el extremo de cada trama, este se utiliza para determinar si la trama llego sin errores. Este proceso se denomina detección de errores, esta se logra al colocar un resumen lógico o matemático de los bits que comprenden la trama en la cola del paquete *ver fig1.1*

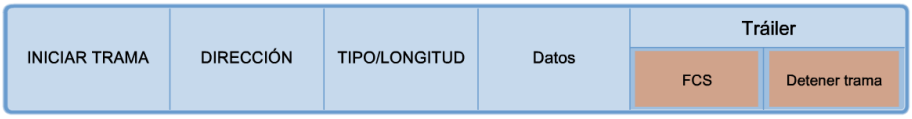


Figura 2.18: La función del trailer.

El campo de secuencia de verificación de trama (FCS) se utiliza para determinar si se produjeron errores de transmisión y recepción de la trama. La detección de errores se agrega en la capa de enlace de datos, por que es en donde se realiza la transferencia de los datos a través del medio.
Los medios son un entorno potencialmente inseguro para los datos, las señales en los medios pueden estar sujetas a interferencia, distorsión o pérdida que podría cambiar sustancialmente los valores de los bits que dichas señales presentan. Este mecanismo de verificación en el campo FSC descubre la mayoría de los errores provocados por los medios. Para asegurarse que el contenido de la trama recibida en el destino coincida con el de la trama que salió del nodo de origen, un nodo de transmisión crea un resumen lógico del contenido de la trama. Esto se conoce como valor de comprobación de redundancia cíclica (CRC). Este valor se coloca en el campo Secuencia de verificación de la trama (FCS) para representar el contenido de la trama. Cuando la trama llega al nodo de destino, el nodo receptor calcula su propio resumen lógico o CRC de la trama. El nodo receptor compara los dos valores CRC. Si los dos valores son iguales, se considera que la trama llegó como se transmitió. Si el valor CRC en el FCS difiere del CRC calculado en el nodo receptor, la trama se descarta. Existe siempre la pequeña posibilidad de que una trama con un buen resultado de CRC esté realmente dañada. Los errores en los bits se pueden cancelar entre sí cuando se calcula el CRC. Los protocolos de capa superior entonces deberían detectar y corregir esta pérdida de datos.

El protocolo que se utiliza en la capa de enlace de datos determina si se realiza la corrección del error. La FCS se utiliza para detectar el error, pero no todos los protocolos admiten su corrección.

Dos de las funciones básicas de la capa de enlace son:

- Permitir a las capas superiores acceder a los medios por medio de tramas. Para dar soporte a una gran variedad de funciones de red, la capa de enlace de datos a menudo se divide en dos subcapas: superior e inferior. La capa superior define los procesos de software que proporcionan servicios a los protocolos de capa de red. El control de enlace lógico (LCC) coloca la información en la trama que identifica que protocolo de capa esta utilizando la trama. La subcapa inferior define los procesos de acceso a los medios que realiza el hardware. El control de acceso a los medios (MAC) proporciona a la capa de enlace el direccionamiento y la delimitacion de datos de acuerdo con los requisitos de señalizacion física del medio y al tipo de protocolo de capa de enlace en uso.

  Separar la capa de enlace de datos en subcapas permite a un tipo de trama definida por la capa superior acceder a diferentes tipos de medios definidos por la capa inferior.

- Controlar la ubicación de los datos en los medios y la recepción por medio de técnicas de control de acceso y detección de errores.

  Las técnicas de control de acceso a los medios definen si los nodos comparten los medios y de que manera lo hacen. Los protocolos definen las reglas de acceso, algunos métodos de control utilizan procesos altamente controlados para asegurar que las tramas se coloquen con seguridad en los medios. Este control depende de como se comparte el medio y la topologia. Algunas topologias comparten el medio con varios nodos, en cualquier momento puede haber una cantidad de dispositivos que intentan enviar o recibir datos, para eso existen reglas que rigen como esos dispositivos comparten los medios. Dos de esos métodos básicos de control son:

  - **Controlado**: Cada nodo tiene su propio tiempo para utilizar el medio.

    Al utilizar este método, los dispositivos de red toman turnos en secuencia para acceder al medio. A este método se le conoce como acceso programado o determinista. Si un dispositivo no necesita acceder al medio, la oportunidad de utilizar el medio pasa al siguiente dispositivo. Cuando un dispositivo coloca una trama en los medios, ningún otro dispositivo puede hacerlo hasta que la trama haya llegado al destino y haya sido procesada por el destino. aúnque el acceso controlado esta bien ordenado y proporciona rendimiento predecible, los métodos deterministas pueden ser ineficientes por que un dispositivo tiene que esperar su turno antes de poder utilizar el medio.

  - **Con base en la contención:** Todos los nodos compiten por el uso del medio.

    También llamado no determinista, permite que cualquier dispositivo intente acceder al medio siempre que haya datos para enviar. Para evitar caos completo en los medios, estos métodos usan un proceso de *Acceso múltiple por detección de portadora (CSMA)* para detectar primero si los medios están transportando una señal. Si detecta una señal portadora en el medio desde otro nodo, quiere decir que otro dispositivo esta transmitiendo. Cuando un dispositivo

esta intentando transmitir y nota que el medio esta ocupado, esperara e intentará después de un periodo de tiempo corto. Si no se detecta una señal portadora, el dispositivo transmite sus datos.
Las redes Ethernet e inalámbricas utilizan control de acceso al medio por contención. Es posible que este método falle si es que dos dispositivos transmitan al mismo tiempo; a esto se le denomina colisión de datos, si esto ocurre, los datos enviados por ambos dispositivos se dañaran y deberán enviarse nuevamente.
Los métodos por contención no tienen las sobrecarga de los métodos de acceso controlado, sin embargo los sistemas por contención no escalan bien bajo un uso intensivo de los medios. A medida que el uso y el número de nodos aumenta, la probabilidad de acceder a los medios con éxitos sin una colisión disminuye. Ademas los mecanismos de recuperación que se requieren para corregir errores por esas colisiones disminuyen aún mas el rendimiento.

- **CSMA/Detección de colisión.**
  Con el método de CSMA/CD, el dispositivo controla los medios para detectar la presencia de una señal de datos. Si no hay una señal que indique que el medio esta libre, el dispositivo trasmite datos. Si luego se detectan señales que muestran que otro dispositivo estaba transmitiendo al mismo tiempo, todos los dispositivos dejan de enviar e intentan después.
- **CSMA/Prevención de colisiones.**
  Con el método CSMA/CA, el dispositivo analiza los medios para detectar la presencia de una señal de datos. Si el medio esta libre, el dispositivo envía una notificación a través del medio, sobre su intención de utilizarlo. El dispositivo luego envía los datos. Este método es utilizado por las tecnologías inalámbricas 802.11.

Los protocolos de capa dos *ver fig2.19.* trabajan con los de la capa tres, sin embargo el protocolo de enlace real en uso depende de la topología lógica de la red y de la implementación de la capa física. Esto quiere decir que el protocolo a utilizar para una topología de red en particular, es determinado por la tecnología utilizada, esta a su vez es elegida por el tamaño de red, cantidad de host, alcance geográfico etc. En la siguiente imagen se muestran los estándares y los protocolos que manejan en capa dos del modelo OSI.

ISO:	HDLC (Control de enlace de datos de alto nivel)
IEEE:	802.2 (LLC) 802.3 (Ethernet) 802.5 (Token Ring) 802.11(Wireless LAN [LAN inalámbrica])
ITU:	Q.922 (Estándar de Frame Relay) Q.921 (Estándar de enlace de datos ISDN) HDLC (Control de enlace de datos de alto nivel)
ANSI:	3T9.5 ADCCP (Protocolo de control de comunicación avanzada de datos)

Figura 2.19: Estándares y protocolos manejados en capa de enlace.

En una LAN los métodos de transmisión de datos de capa dos se dividen en tres clasificaciones: unicast, multicast y broadcast.

Unicast.

Es el proceso mediante el cual se envía un paquete de un host a un host individual. La comunicación se usa para comunicación de host a host, tanto en una red de cliente/servidor como en una red punto a punto.

Este método es uno a uno, el envío de datos se realiza desde un único emisor y un único receptor, este método envía por separado el tráfico de los datos a cada equipo que ha solicitado los datos, a su vez esto provoca la inundación de la red por la cantidad de tráfico.

Multicast.

El proceso por el cual se envía un paquete de un host a un grupo seleccionado de host.

La transmisión multicast esta diseñada para conservar el ancho de banda de la red. Esta reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts. Con ayuda de multicast el origen puede enviar un único paquete que llegue a miles de hosts de destino.

Broadcast.

El proceso por el cual se envía un paquete de host a todos los hosts de la red.

Cuando un host recibe un paquete con la dirección de broadcast como destino, este procesa el paquete como lo haría con un unicast. La transmisión de broadcast se usa para ubicar servicios o dispositivos especiales para las cuales no se conoce la dirección o cuando un host debe proporcionar información a todos los host de la red.

A diferencia de unicast donde los paquetes pueden ser enrutados por toda la internetwork, los paquetes de broadcast normalmente se restringen a la red local. Dependiendo del tipo

de dispositivo que bordea la red se tienen dos tipos de broadcast: dirigido y limitado. El método de broadcast es emitido por el *Address Resolution Protocol*, ARP protocolo que trabaja en ambas capas 2 y 3. Documentado en el RFC 826, dicho protocolo es responsable de encontrar la dirección hardware (MAC) que corresponde a determinada dirección IP. Para ello se envía un paquete de tipo *ARP request* a la dirección broadcast con MAC = *(FF:FF:FF:FF:FF:FF)*,la cual contiene la IP por la que se pregunta y se espera que esta maquina responda con un *ARP replay* con la dirección MAC que le corresponde, para realizar esta conversión se utilizan tablas ARP, en las cuales se concentra la dirección IP que le corresponde a cada dirección física. El protocolo que realiza esta operación inversa se llama RARP *(Reverse Address Resolution Protocol)*descrito en el RFC 903. Un evento de red que se asocia con el broadcast son las *Tormentas de broadcast* estas ocurren cuando se envían muchos broadcast de manera simultanea a través de todos los segmentos de red. Las tormentas hacen uso sustancial de ancho de banda y causan retraso en los limites de tiempo de transmisión.

Dispositivos de red capa 2

Switch

Un switch es un término que se aplica a un dispositivo electrónico o mecánico que permite el establecimiento de una conexión según sea necesario y que se termine cuando ya no haya ninguna sesión que se deba mantener, un switch reenvía selectivamente tramas individuales desde un puerto receptor hasta el puerto en el que esté conectado el nodo destino*ver fig2.20*. Cuando se establece la conexión se inicia la transmisión, si el nodo destino se encuentra inactivo, el switch almacena las tramas entrantes en la memoria buffer y después envía al puerto correspondiente, este proceso se conoce como almacenaje y reenvío. Con esta conmutación el switch recibe la trama y verifica si contiene errores, si la trama es correcta se reenvía a su destino, registrando en su *tabla mac* que hace coincidir una dirección MAC de destino con el puerto utilizado para conectarse a un nodo.

Figura 2.20: Dispostivos de capa 2: Switch.

Para cada trama entrante, la dirección MAC de destino en el encabezado de la trama se compara con la lista de direcciones de la tabla MAC. Si se produce una coincidencia, el número de puerto de la tabla que se asocio con la dirección MAC se utiliza como puerto de salida de la trama *ver fig2.21*.

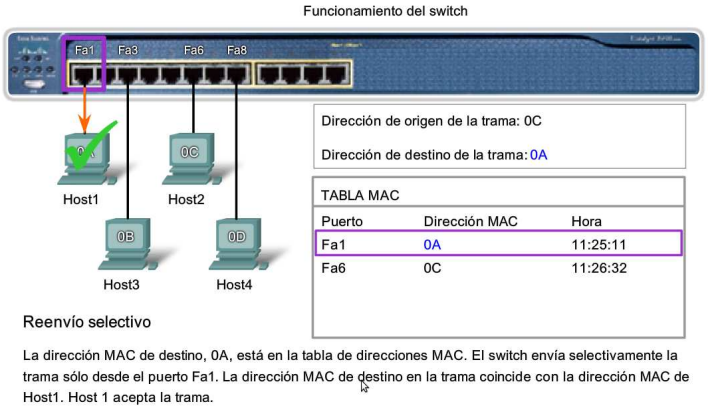


Figura 2.21: Registro de tabla ARP.

En caso contrario el switch envía la trama a todos los puertos, excepto al puerto en donde llegó la trama. El proceso que consiste en enviar una trama a todos los segmentos se denomina, *saturación*.

Debido al amplio rango de medios físicos utilizados a través de un rango de topologías en interconexión de red, hay una gran cantidad de protocolos de capa dos. Algunos de ellos son:

- Ethernet.
- Protocolo punto a punto (PPP).
- Control de enlace de datos de alto nivel (HDLC).
- Frame Relay.
- Modo de transferencia asíncrona (ATM).

Los protocolos de la capa de enlace hacen poco para controlar el acceso a medios no compartidos, un ejemplo son las conexiones punto a punto, la capa 2 tiene que considerar si la comunicación es *half-duplex o full-duplex*, la comunicación half-duplex quiere decir que los dispositivos pueden transmitir y recibir en los medios, pero no pueden hacerlo simultáneamente. En la comunicación full-duplex, los dos dispositivos pueden transmitir y recibir en los medios al mismo tiempo. La capa de enlace de datos supone que los medios están disponibles para transmitir para ambos nodos en cualquier momento. Esta capa releva a las capas superiores de la responsabilidad de colocar y recibir datos en la red, aísla de manera efectiva los procesos de comunicación en las capas superiores desde las transiciones de medios que pueden producirse entre extremos.

2.2.7. Capa 1 Física

Los protocolos de la capa superior OSI preparan los datos desde la red humana para realizar la transmisión hacia su destino. La capa física controla la manera en que se transmiten los datos en el medio de comunicación. La función de la capa física del modelo de referencia OSI es la de codificar en señales los dígitos binarios que representan las tramas de la capa de enlace de datos, además de transmitir y recibir estas señales a través de los medios físicos que conectan los dispositivos de red, proporciona los medios de transporte para los bits que conforman la trama de la capa de enlace, su objetivo es crear la señal óptica, eléctrica o de microondas que representa a los bits en cada trama. Así mismo recupera estas señales individuales desde los medios, restaurarlas para sus representaciones de bit y envío hacia la capa subsecuente. Los medios no transportan la trama como una única entidad. Los medios transportan señales, una por vez, para representar los bits que conforman la trama. La siguiente imagen muestra el proceso de la información y su transformación a lo largo de todo el modelo OSI.

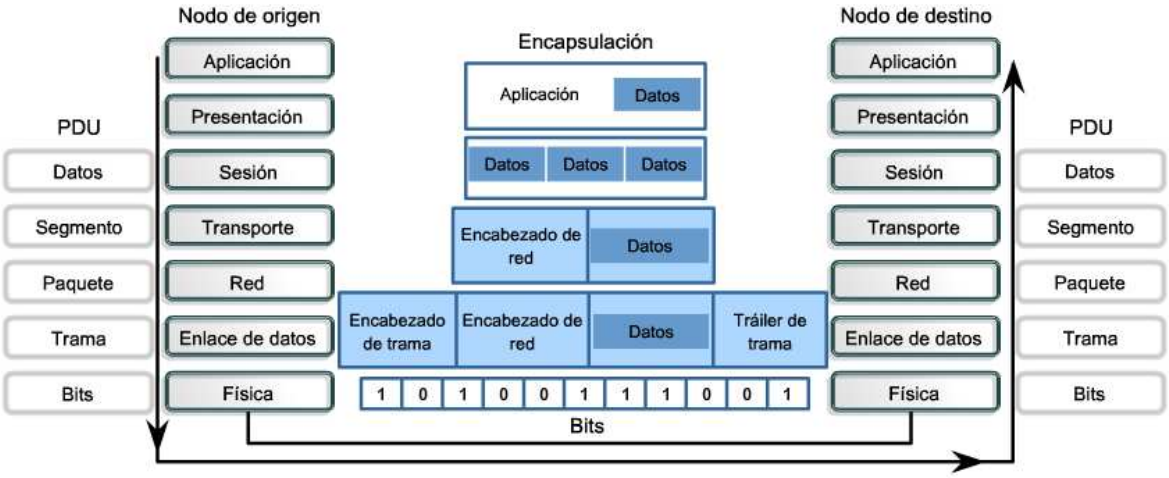


Figura 2.22: Transformación de información en el modelo OSI

Existen tres tipos básicos de medios de transmisión de datos a través de red los cuales se representan datos:

- Cable de cobre
- Fibra óptica
- Inalámbrico

Medios de Cobre.

El medio más utilizado para las comunicaciones de datos es el cableado que utiliza alambres de cobre para señalizar bits de control y de datos entre los dispositivos de red. El cableado consiste en una secuencia de alambres individuales de cobre que forman circuitos que cumplen objetivos específicos de señalización. El tipo de medio de cobre elegido se especifica mediante el estándar de la capa física necesario para enlazar las capas de enlace de datos de dos o mas dispositivos. Estos cables pueden utilizarse para conectar los nodos de una LAN a los dispositivos intermediarios, como routers o switch. Los cables también se utilizan para conectar dispositivos WAN a un proveedor de servicios de datos. Cada tipo de conexión y sus dispositivos complementarios incluyen requisitos de cableado estipulados por los estándares de la capa física. Los datos se transmiten en cables de cobre como impulsos eléctricos. Un detector en la interfaz de red de un dispositivo de destino debe recibir una señal que pueda decodificarse exitosamente para que coincida con la señal enviada. Los tipos de cable con blindaje o trenzado de pares de alambre están diseñados para minimizar la degradación de señales debido al ruido electrónico. El cableado UTP, con una terminación de conectores RJ-45, es un medio común basado en cobre para interconectar dispositivos de red, es posible que los cables necesiten armarse según las diferentes convenciones para los cableados *ver fig2.23*. Los principales tipos de cables se obtiene al utilizar convenciones específicas de cableado. Cable: directo, cruzado y consola *ver fig2.24*.

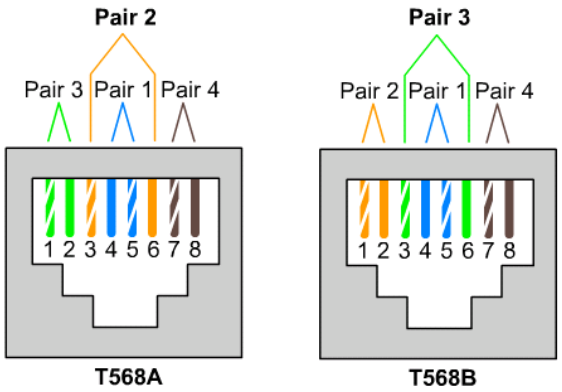


Figura 2.23: Estándares de cableado UTP.

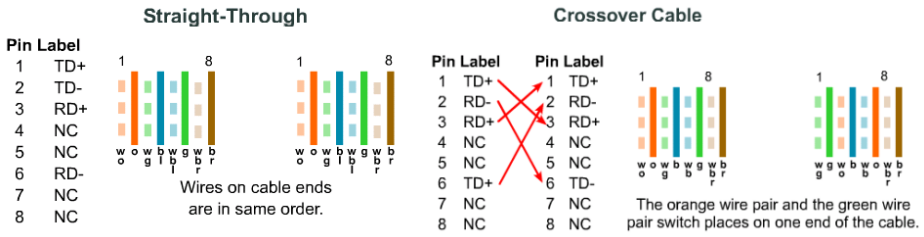


Figura 2.24: Estándares de cableado TIA.

Otros tipos de cable de cobre son: cable coaxial y par trenzado blindado (STP).

Fibra Óptica.

El cableado de fibra óptica utiliza fibras de plástico o de vidrio para guiar los impulsos de luz desde el origen hacia el destino. Los bits se codifican en la fibra como impulsos de luz. El cableado de fibra puede generar velocidades muy superiores de ancho de banda para transmitir datos sin procesar. La mayoría de los estándares actuales de transmisión aún necesitan analizar el ancho de banda potencial de este medio. Debido a que las fibras de vidrio que se utilizan en los medios de fibra óptica no son conductores eléctricos, el medio es inmune a la interferencia electromagnética y no conduce corriente eléctrica no deseada cuando existe un problema de conexión a tierra. Las fibras ópticas pueden utilizarse en longitudes mucho mayores que los medios de cobre sin la necesidad de regenerar la señal, ya que son finas y tienen una pérdida de señal relativamente baja. Algunos de los problemas de implementación de medios de fibra son: El costo,diferente habilidad de equipo para la infraestructura, manejo mas cuidadoso. En la actualidad, en la mayor parte de los entornos empresariales se utiliza principalmente la fibra óptica como cableado backbone para conexiones punto a punto con una gran cantidad de tráfico entre los servicios de distribución de datos y para la interconexión de los edificios cuando así sea el caso. Los láseres o diodos de emisión de luz generan impulsos de luz que se utilizan para representar los datos transmitidos como bits en los medios. Los dispositivos electrónicos semiconductores, denominados fotodiodos, detectan los impulsos de luz y los convierte en voltajes que pueden reconstruirse en tramas de datos.

En términos generales, los cables de fibra óptica pueden clasificarse en dos tipos:

Fibra multimodo y monomodo.

La fibra óptica monomodo transporta un solo rayo de luz, generalmente emitido desde un láser. Este tipo de fibra puede transmitir impulsos ópticos en distancias muy largas, ya que la luz del láser es unidireccional y viaja a través del centro de la fibra. La fibra multimodo normalmente utiliza emisiones LED que no generan un único haz de luz coherente *ver fig2.25*. Los tendidos extensos de fibra pueden generar impulsos poco claros al recibirlos en el extremo receptor ya que la luz ingresa a la fibra en diferentes ángulos requiere de distintos periodos de tiempo para viajar a través de la fibra. Este efecto denominado dispersión modal, limita la longitud de los segmentos de fibra.

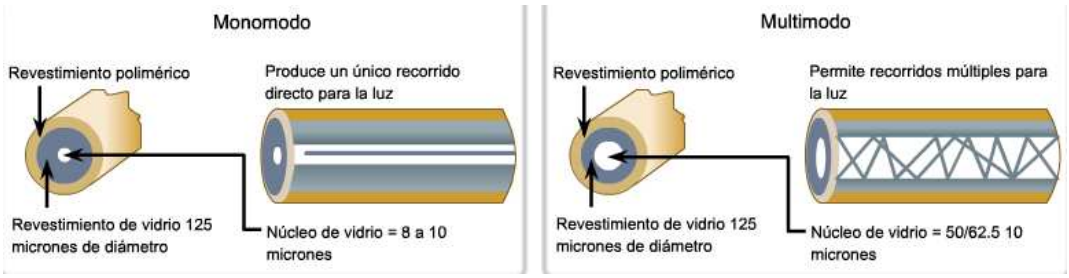


Figura 2.25: Fibra optica Multimodo y Monomodo

Inalámbricos

Estos medios transportan señales electromagnéticas mediante frecuencias de microondas y radiofrecuencias que representan los dígitos binarios de las comunicaciones de datos, funcionan bien en entornos abiertos. Es susceptible a la interferencia y puede distorsionarse por dispositivos comunes como teléfonos inalámbricos domésticos, algunos tipos de luces fluorescentes, hornos de microondas y otras comunicaciones inalámbricas. Además, los dispositivos y usuarios que no están autorizados a ingresar a la red pueden obtener acceso a la transmisión. Los estándares de la industria de telecomunicaciones sobre las comunicaciones inalámbricas de datos abarcan las capas física y de enlace de datos. Los cuatro estándares comunes de comunicación de datos que se aplican a los medios inalámbricos son:

- *IEEE estándar 802.11* Comúnmente denominada Wi-Fi,se trata de una tecnología LAN inalámbrica que utiliza una contención o sistema no determinista con un proceso CSMA/CA
- *IEEE estándar 802.15* Estándar de red de área personal inalámbrica comúnmente llamada Bluetooth, utiliza un proceso de emparejamiento de dispositivos para comunicarse a través de una distancia de 1 a 100 metros.
- *IEEE estándar 802.16* Comúnmente asociada como WiMAX (interoperabilidad mundial para el acceso por microondas), utiliza una topología punto a multipunto para proporcionar un acceso de ancho de banda inalámbrico.
- *IEEE 802.20* MBWA o Mobile broadband Wireless Access es una especificación del IEEE para las redes de acceso a Internet para redes moviles. Publicado en 2008, se esperaba crear una norma que permitiera una red siempre activa, a bajo costo, y redes de banda ancha movil tambien llamada MobileFi, este comprendia una baja latencia y anchos de banda de 5, 10 y 20 MHz.
- *Sistema global para comunicaciones móviles GSM* Incluye las especificaciones de la capa física que habilitan la implementación del protocolo de servicio general de radio por paquetes (GPRS) de capa 2 para proporcionar la transferencia de datos a través de redes de telefonía celular móvil.

La presentación de los bits dependen del tipo de medio. Para los medios de cable,las señales son patrones de pulsos eléctricos. Para los medios de fibra, las señales son patrones de luz y para las inalámbricas son transmisiones de radio. Las tres funciones esenciales de esta capa son:

- Componentes físicos.
  Los elementos físicos son los dispositivos electrónicos de hardware, medios y conectores que transmiten y transportan las señales para representar los bits.
- Codificación.
  La codificación es un método que se utiliza para convertir un stream de bits de datos

en un código predefinido. Los códigos son grupos de bits utilizados para ofrecer un patrón predecible que pueda reconocer tanto el emisor como el receptor. La utilización de patrones predecibles permite distinguir los bits de datos de los bits de control y ofrece una mejor detección de errores en los medios. Además esos códigos pueden proporcionar códigos de control, como la identificación del comienzo y el final de una trama.

- Señalización.
  Esta capa debe generar señales inalámbricas, ópticas o eléctricas binarias en los medios. Este método de representación de bits se denomina método de señalización, acorde a un estándar que define que tipo de señal representa los bits, por medio de un cambio de señal eléctrica o un impulso óptico o un método mas complejo.
  Los diferentes medios físicos admiten la transferencia de bits a distintas velocidades. La transferencia de datos puede medirse de tres formas:

  - **Ancho de banda.**
    La capacidad que posee un medio de transportar datos se describe como el ancho de banda de los datos sin procesar de los medios. El ancho de banda digital mide la cantidad de información que puede fluir desde un lugar hacia otro en un periodo de tiempo determinado. Generalmente en kilobits por segundo o megabits. El ancho de banda practico de una red se determina mediante una combinación de factores: las propiedades de las tecnologías y los medios físicos elegidos para señalizar y detectar señales de red. Las propiedades de los medios físicos, las tecnologías actuales y las leyes de la física desempeñan una función al momento de determinar el ancho de banda disponible.

  - **Rendimiento.**
    El rendimiento es la medida de transferencia de bits a través de los medios durante un periodo de tiempo determinado. Debido a diferentes factores, el rendimiento generalmente no coincide con el ancho de banda especificado en las implementaciones de la capa. Muchos factores influyen en el rendimiento, como la cantidad y el tipo de tráfico además de la cantidad de dispositivos de red que se encuentran en la red que se esta midiendo, en las topologías multiacceso los nodos compiten por el acceso, por lo tanto cada nodo se degrada a medida que aumenta el uso de los medios. Solo se necesita un segmento en la ruta con un rendimiento inferior para crear un cuello de botella en el rendimiento de toda la red.

  - **Capacidad de transferencia útil (Throughtput.)**
    Es la medida de datos utilizables transferidos durante un periodo de tiempo determinado. A diferencia del rendimiento, que mide la transferencia de bits y no la transferencia de datos utilizables, la capacidad de transferencia útil considera que los bits generan sobrecarga del protocolo. Esta capacidad representa el rendimiento sin la sobre carga de tráfico para establecer sesiones, acuses de recibo y encapsulaciones.

2.3. Modelo de Arquitectura TCP/IP.

TCP/IP es un conjunto de protocolos que hacen posible la comunicación entre dos computadoras, antes la intercomunicación entre las computadoras no era importante, ahora es indispensable. Este consta de cuatro capas de abstracción según definidas en el RFC 1122. Esta suite fue desarrollada antes de que el modelo OSI fuera publicada, por lo tanto no lo utiliza como referencia. TCP/IP fue desarrollado con base al *Department of Defense (DoD).*

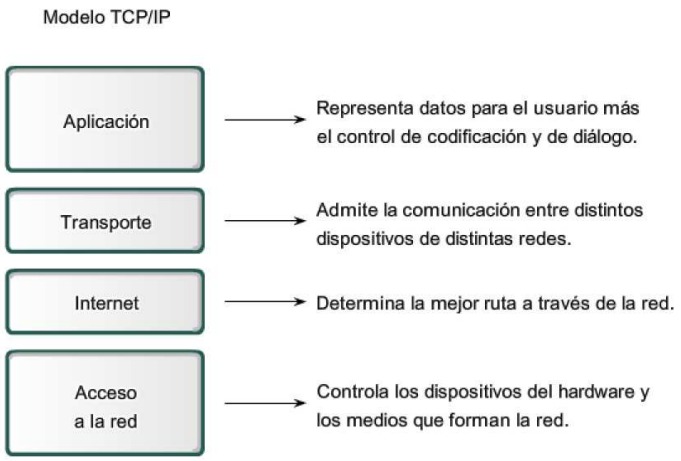


Figura 2.26: Modelo de protocolo TCP/IP

Para entender bien los origenes del Internet, se debe tener en cuenta a ARPAnet, quien fue la predecesora del internet de hoy, era una super red creada por el Advance Research Projects Agency (ARPA), fue desarrollada en respuesta a las amenazas nucleares de la unión sovietica, su objetivo era proveer el servicio tolerante a fallos para que los lideres militares tuvieran comunicación en caso de una guerra nuclear. El protocolo implementado fue *Network Control Protocol (NCP)*, sin embargo no pudo complementar las necesidades de la red. Estas necesidades fueron: No poseer mas de un punto crítico, redundancia en rutas, modificación de rutas *al vuelo* y la habilidad de conexion de diferentes host con diferentes características. Debido a que NCP tenia tantas limitantes y no era lo suficientemente robusto para la super red, la cual empezó a crecer sin control lo cual obligo a arpanet a renovar y desarrollar un nuevo lenguaje para internet. En 1974 Vint Cerf and Bob Kahn, públicaron el protocolo *A Protocol for Packet Network Interconcection* en este documento se describe el Protocolo de Control de Transmision, (TCP) cuyo protocolo en los 80's reemplazo a NCP. Los objetivos del diseño de esta suite fueron: la independencia de software y hardware para mayor compatibilidad en plataforma y arquitectura; la auto recuperación y manejo errores en los datos, la habilidad de incluir redes a la internetwork sin necesidad de afectar el servicio y enrutaminento. Esta suite de protocolos ha sido utilizada por mas de 20 años, con el tiempo y pruebas se ha comprobado su estabilidad. TCP/IP tiene muchas características y beneficios, tales como:

- Soporte. Desde su comienzo, TCP/IP recibe soporte de varios proovedores de software y hardware. Esto significa que la suite de protocolos no recae en el desarrollo de un solo proovedor.
- Interoperabilidad. Una de las razones por las que TCP/IP ha ganado popularidad y aceptación a nivel universal es por que puede ser instalado en cualquier plataforma.
- Flexibilidad. La suite de protocolos es extremadamente flexible, esto hace la tarea del administrador de red mas eficiente.
- Enrutamiento. Una limitación de muchos protocolos es la dificultad de mover los datos de un segmento a otro. TCP/IP es excepcional a la adaptación del proceso de enrutamiento. TCP/IP es el protocolo estándar de comunicaciones en internet. No se puede conectar a Internet sin utilizar TCP/IP. Sin importar si la red es de dos host o miles, esta suite funciona a la perfección, es escalable y robusta para interconectar diferentes tipos de LANs.

Los protocolos que forman parte de la suite de protocolos TCP/IP pueden describirse análogamente con el modelo OSI *ver fig2.27.*

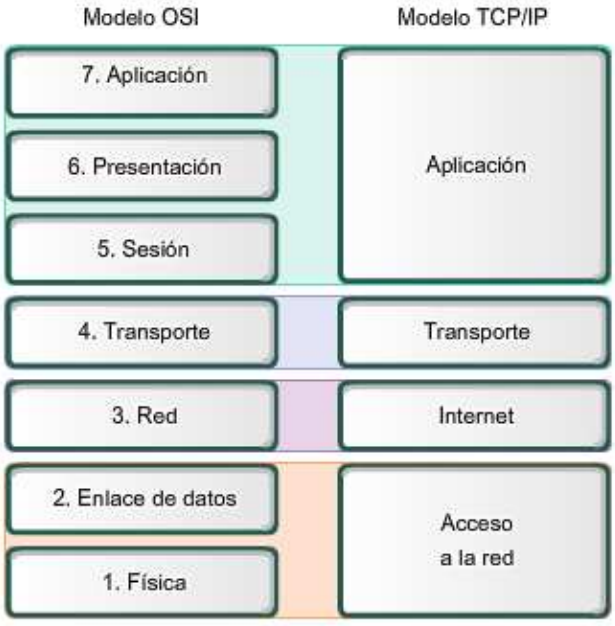


Figura 2.27: Comparación modelo OSI y TCP/IP

Como se puede ver en la imagen las tres primeras capas del modelo OSI son equivalentes a la capa de Aplicación. Seguido de la capa de transporte que conserva su nombre, la capa de red cambia de nombre por Internet y las ultimas dos capas de Enlace de Datos y Física equivalen a la capa de Acceso a la Red.

Para comprender la diferencia entre estos dos modelos es necesario saber que existen dos tipos básicos de modelos de networking: **modelos de protocolo y modelos de referencia.**

Un modelo de protocolo proporciona un modelo que coincide fielmente con la estructura de una suite de protocolo en particular. El conjunto jerárquico de protocolos relacionados en una suite representa típicamente toda la funcionalidad requerida para interconectar la red humana con la red de datos, como TCP/IP. El modelo TCP/IP es un modelo de protocolo porque describe las funciones que se producen en cada capa de los protocolos dentro del conjunto TCP/IP. Un modelo de referencia proporciona una guia común para mantener consistencia en todos los tipos de protocolos y servicios de red. Un modelo de referencia no está pensado para ser una especificación de implementación ni para proporcionar un nivel de detalle suficiente para definir de forma precisa los servicios de la arquitectura de red. El propósito principal de un modelo de referencia es asistir en la comprensión más clara de las funciones y los procesos involucrados. El modelo de interconexión de sistema abierto (OSI) es el modelo de referencia de internetwork más ampliamente conocido. Se utiliza para el diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas. Este fue propuesto como una aproximación teórica y también como una primera fase en la evolución de las redes de computadoras. Por ello el modelo OSI es mas fácil de entender, aúnque el modelo utilizado sea TCP/IP, es de gran ayuda comprender ambos modelos ya que aplican los mismos principios.

Capítulo 3

Servicios y Mecanismos de Seguridad.

Para proteger las comunicaciones de los usuarios en las redes, es necesario dotar a las mismas con cinco clases de servicios de seguridad.

- **Autenticación.**
  Este servicio corrobora la veracidad de la fuente de una unidad de datos. La autenticación de entidad par, sirve para verificar que la entidad pareja o de una asociación es quien dice ser. La autenticación del origen de los datos permite reclamar el origen de las fuentes de los datos recibidos, sin embargo, este servicio no proporciona protección contra la duplicación o la modificación de unidades de datos.

- **Control de Acceso.**
  Este servicio se utiliza para evitar el uso no autorizado de los recursos.

- **Confidencialidad de Datos.**

  Este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación. Este servicio puede ser orientado o no a conexión, a campo selectivo y flujo de tráfico.

- **Integridad de Datos.**

  Este servicio garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor. Los servicios de integridad de datos orientados a conexión con recuperación de datos proporcionan integridad durante una sesión, a diferencia de los servicios no orientados a conexión en los cuales no se recuperan los fallos de integridad.

- **No Repudio.**

  Este servicio proporciona la prueba ante una tercera parte de cada una de las entidades comunicantes, que han participado en una comunicación. Dicha prueba puede ser cuando el destinatario tiene prueba del origen de los datos, o bien, cuando el origen tiene prueba de entrega integra de los datos al destinatario deseado.

Para proporcionar estos servicios de seguridad es necesario incorporar mecanismos de seguridad en los niveles del modelo OSI, para lo cual la arquitectura distingue mecanismos de seguridad específicos y generalizados.

Mecanismos de Seguridad Específicos.

Se enumeran ocho mecanismos específicos de seguridad.

- **Cifrado.**

  Se utiliza para proteger la confidencialidad de los datos ya sea en reposo o en flujo, así como para dar soporte o complementar otros mecanismos de seguridad. El cifrado puede hacerse utilizando sistemas criptográficos simétricos o asimétricos y se puede aplicar extremo a extremo o individualmente a cada enlace del sistema de comunicaciones.

- **Firma Digital.**

  Se emplean para proporcionar una analogía electrónica a la firma manuscrita en documentos electrónicos, no deben ser falsificables. Los receptores deben ser capaces de verificar la integridad y no debe poder rechazarla.

- **Control de Acceso.**

  Este mecanismo se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio y se encarga de asegurar si el emisor esta autorizado a comunicarse con el receptor, así como a hacer uso de los recursos de comunicación requeridos. Si una entidad intenta acceder a un recurso no autorizado o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazara el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y/o registrarlo.

- **Integridad de Datos.**

  Se encarga de proteger la integridad de los datos, de los paquetes de datos, de las secuencias de los paquetes de datos, así como de los campos correspondientes a dichas secuencias.

- **Intercambio de Autenticación.**

  Su finalidad es verificar la identidad de las entidades en comunicación, antes de iniciar el intercambio de información. Puede ser autenticación simple o fuerte. En la autenticación simple el emisor envía sus credenciales como usuario y password al receptor. En la autenticación fuerte se utilizan técnicas criptográficas para proteger los mensajes que se van a intercambiar.

- **Relleno de tráfico.**

  Se utiliza para brindar protección contra ataques de análisis de tráfico, generando datos espurios dentro de los paquetes, con el objetivo de no revelar si los datos que se están transmitiendo representan y codifican realmente información.

- **Control de encaminamiento.** Este mecanismo permite la selección dinámica o preestablecida de rutas especificas para la transmisión de los datos. Los sistemas de comunicaciones detectan de forma persistente ataques activos o pasivos, con lo cual pueden indicar al proveedor del servicio el cambio de ruta.

- **Mecanismo de certificación.**

  Mecanismos cuya función es asegurarse de ciertas propiedades de los datos que se comunican entre dos o mas entidades, entre los que destacan su integridad, origen, tiempo o destino. La certificación la realiza una tercera entidad de confianza, que es la que da testimonio de la autenticidad.

Mecanismos de seguridad generalizados.

Los mecanismos de seguridad generalizados no son específicos de un servicio en particular, en algunos casos se contemplan en aspectos de gestión de la seguridad. La importancia de estos mecanismos esta en general relacionada directamente con el nivel de seguridad requerido.

- Funcionalidad de confianza.

  Se trata de poner en práctica el concepto que se utiliza para ampliar o extender otros mecanismos de seguridad para establecer su efectividad.

- Etiquetas de Seguridad.

  Mecanismo asociado directamente con los recursos del sistema, ya que un nivel de seguridad puede implicar datos adicionales que se asocian a los datos transmitidos o puede ser implícito.

- Detección de eventos.

  Se trata de un mecanismo relevante para la seguridad, ya que su función es detectar violaciones aparentes de la seguridad.

- Recuperación de Seguridad.

  Se relaciona directamente con mecanismos gestores de eventos y funciones de gestión y se encarga de realizar acciones de recuperación con base en las políticas de seguridad establecidas.

- Rastreo de auditoría de seguridad.

  Este mecanismo se encarga de la revisión y examen independiente de los registros y las actividades del sistema para probar la operatividad de los controles, asegurar el cumplimiento de las políticas y procedimientos operacionales establecidos y recomendar los cambios adecuados en el control, política y procedimientos. Este mecanismo se refiere a la adquisición de datos que potencialmente facilitan las auditorías de seguridad.

El principal objetivo del establecimiento de controles de seguridad de la información, es el de reducir los efectos producidos por las amenazas de seguridad y vulnerabilidades a un nivel tolerable por la institución. Dichos controles a implementar pueden ser preventivos, detectivos y correctivos, mediante mecanismos físicos, lógicos e inclusive administrativos los cuales llevan a la institución a generar toda una política de seguridad informática cuya definición se explica mas adelante.

3.1. Vulnerabilidades y amenazas

Una amenaza es un evento cuya ocurrencia podría impactar de forma negativa en la organización o institución. Las amenazas explotan vulnerabilidades, la entidad que toma ventaja de una vulnerabilidad, suele referirse como agente de la amenaza. Una vulnerabilidad se define como la condición que podría permitir que una amenaza se materialice con mayor frecuencia, impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos o físicos. Lo cual genera un riesgo el cual se define como la probabilidad de que un agente de amenaza explote una vulnerabilidad, en combinación con el impacto que esto ocasiona *ver fig3.1.* Dicho riesgo puede dañar los activos informáticos que estén expuestos.

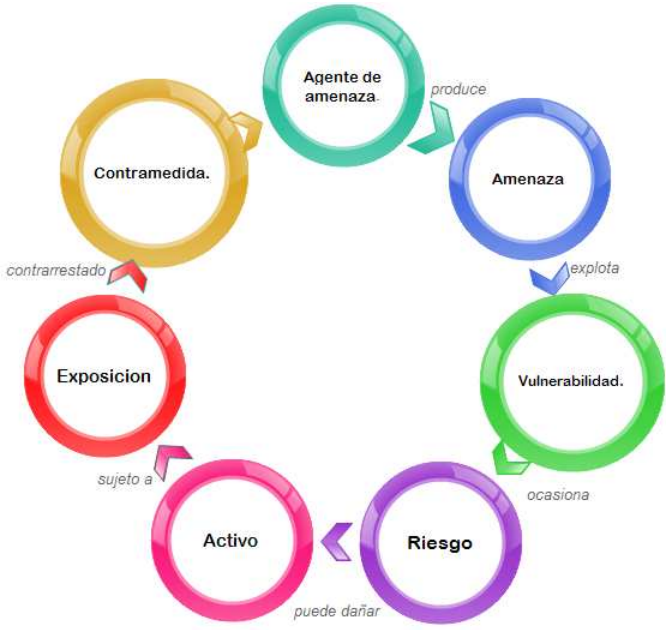


Figura 3.1: Relación de conceptos.

Esto se controla mediante contramedidas, las cuales se aplicaran para tratar de evitar lo opuesto a los objetivos de seguridad: **revelación, modificación y destrucción**, cuya relación se muestra *ver fig3.2*.

Objetivo	Amenaza	Contramedida
Confidencialidad e Integridad	• Shoulder surfing • Ingeniería Social • Usuarios descuidados • Hacker/Cracker • Masquerades/Spoofing • Descarga de archivos sin protección. • Actividad de usuario no autorizado. • Troyanos • Sniffing • Trashing	o Menor privilegio o Separación de tareas o Procedimientos para control de cambios o Cifrado de datos. o Estricto mecanismos de control de acceso. o Clasificación de la información. o Capacitación de personal.
Disponibilidad	• Denegación de servicio • Desastres Naturales • Acciones Humanas	o Seguridad Física o Mecanismos de tolerancia a fallos. o Plan de recuperación de desastres. o Procedimientos operativos.

Figura 3.2: Contramedidas asociadas a las amenazas hacia los objetivos de seguridad.

3.2. Seguridad Física.

El principal objetivo de la seguridad física, es proveer de un entorno seguro para todos y cada uno de los activos e intereses de la organización, incluyendo la actividad en los sistemas de información. La seguridad física provee protección para los edificios, estructuras, vehículos, conteniendo sistemas de información y cualquier otro componente de red. De acuerdo a sus características pueden ser referidos o estáticos, móviles o portátiles. Una característica distintiva de la seguridad física, es que esta representa el tipo mas obvio de seguridad, esto es por que en la mayoría de los casos esta es visible. Las personas pueden ver cerraduras, paneles de alarma, cámaras, guardias. La seguridad física sigue siendo un componente básico y fundamental en el plan de seguridad de una institución.

3.2.1. Tipos de Vulnerabilidades y amenazas.

Un posible intruso, que obtiene una primera impresión a partir de los dispositivos de seguridad que puede ver, probablemente sospeche que sera necesario trabajar arduamente a fin de saltear tales protecciones. Si bien es cierto que los controles lógicos ayudan a proteger los recursos de la organización, mientras la seguridad en cómputo involucra hackers, la seguridad física involucra intrusos, vándalos y ladrones.

Físicas.

Los componentes para la seguridad física contemplan elementos involucrados en la selección de un sitio seguro, diseño. La implementación de métodos para asegurar una instalación contra el acceso no autorizado, para evitar robos dirigidos a las personas o a su información. Se trata tomar de las medidas necesarias de seguridad y ambientales para proteger el personal, las instalaciones y los recursos asociados. Mediante alarmas, monitorización, sistemas de ventilación, detección y supresión de incendios.

Los objetivos de un programa de seguridad física son:

- Prevenir y disuadir el crimen.
- Reducir el daño implementando un mecanismo de retardo.
- Detectar crímenes o interrupciones.
- Evaluar el incidente.
- Establecer procedimientos de respuesta.

La consideración de la seguridad física, es de suma importancia no causar conflictos con el objetivo conocido como "Life Safety", dicho objetivo se encuentra relacionado con la provisión de una salida segura del edificio potencialmente en peligro. Para ello tenemos el concepto de CPTED= Crime Prevention Through Enviromental Design.

Este concepto, lleva como premisa básica, la cual establece que el entorno físico de un edificio, puede ser cambiado o manipulado de modo tal que sea posible producir cambios en el comportamiento de las personas, a fin de lograr que sea posible reducir la incidencia

y el miedo al crimen. Este objetivo se logra por medio de la combinación de hardware de seguridad, psicología y diseño del site, a modo de de lograr un entorno que por si mismo desaliente el crimen. El CPTED se encuentra construido sobre estrategias clave: territorialidad, vigilancia y control de acceso. La seguridad siempre es mejor cuando es pensada desde el inicio y la seguridad física no es la excepción a la regla.

La construcción de facilidades involucra entre otros aspectos la selección y ubicación de muros, puertas, ventanas así como también aquellos elementos que darán soporte a la infraestructura tal como agua, gas y electricidad. Las vulnerabilidades físicas pueden provocar una interrupción de comunicaciones, problemas en la distribución de energía debido al ruido, el cual causa fluctuaciones originando interferencia electromagnética o de radio frecuencia, así como la ausencia o mal funcionamiento de una tierra física. Con respecto al servicio de agua y gas las amenazas pueden ser cañerias rotas, fugas de agua o gas.

Naturales.

Las amenazas naturales o ambientales son aquellas ajenas al ser humano, tales como: terremotos, inundaciones, tormentas, tornados, huracanes, erupciones volcánicas, incendios, temperaturas extremas, humedad alta, o derrumbes. Los terremotos pueden ser poco intensos por lo que solamente algunos instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que estos fenómenos sísmicos esta ocurriendo en lugares donde no se los asociaba. Una inundación se define como la invasión de agua por exceso de escurrimientos superficiales o acumulación de la misma, esta es ocasionada por falta de drenaje ya sea natural o artificial.
Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones etc. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran se calcula por medio se sensores atmosféricos. La comprobación de los informes climatológicos permite la toma de precauciones para este tipo de amenazas. Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y al inadecuado almacenamiento y traslado de sustancias peligrosas y por ultimo el fuego, es una de las principales amenazas contra la seguridad, es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Hardware.

La amenaza por fallas físicas que presente cualquiera de los elementos de hardware que conforman al sistema de cómputo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño en el hardware, pero también pueden ser el resultado de un mal uso y descuido en el mantenimiento. La vulnerabilidad reside en el mal diseño por lo general se presenta cuando los componentes del sistema no son apropiados y no cumplen con los requerimientos necesarios, en decir el diseño de la pieza no fue correcto para trabajar con el sistema. Los errores de fabricación suceden cuando las piezas son adquiridas con desperfectos de fabricación y posteriormente fallan al momento de intentar utilizarse. aúnque la

calidad de los componentes de hardware es responsabilidad del fabricante, la organización que los requiere es la mas afectada por este tipo de amenaza. El suministro de energía es también una amenaza dado que las variaciones de voltaje dañan a los dispositivos, por ello es necesario verificar que las instalaciones funcionen dentro de los parámetros requeridos así mismo los tiempos de uso, periodos y procedimientos de mantenimiento y almacenamiento.

Factor Humano.

Los elementos humanos de un sistema son los mas difíciles de controlar, lo que los convierte en constantes amenazas y al mismo tiempo, es una de las partes mas vulnerables del sistema. Las vulnerabilidades de origen humano mas comunes son la falta de capacitación y concientizacion, lo que puede dar lugar a la negligencia en el seguimiento de las políticas de seguridad y mal uso de equipo de cómputo. Los actos contra la seguridad realizados a conciencia por un elemento humano pueden ser el resultado de una vulnerabilidad humana, como un usuario descuidado.

3.3. Seguridad Lógica.

La seguridad lógica se refiere a la seguridad en el uso del software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios. La seguridad lógica involucra todas aquellas medidas establecidas por la administración para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información.

Los principales objetivos de la seguridad lógica:

- Restringir el acceso a los programas y archivos.
- Asegurar que estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.

3.3.1. Tipos de Vulnerabilidades y Amenazas Lógicas.

Las amenazas lógicas son todo tipo de programas que de una forma u otra pueden dañar a los sistemas, estos han sido creados para eso (malware), o a veces es un error de programación (bug).

Software.

Las amenazas mas habituales provienen de errores cometidos de forma involuntaria por los programadores de sistemas o aplicaciones. Una situación no contemplada a la hora de diseñar el sistema de red, o un error de acceso a la memoria puede comprometer local o remotamente a un sistema operativo. Estos bugs o errores de programación pueden ser aprovechados y por programas llamados exploits, que utilizan estos fallos para atacar un sistema.

Red.

Para ello hay herramientas de seguridad las cuales representan un arma de doble filo, así como un administrador puede utilizarla para detectar y solucionar fallos en sus sistemas, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar. Es claro que no se puede basar la seguridad de un sistema en el supuesto desconocimiento de sus problemas por parte de los atacantes, por tanto es necesaria la utilización de dichas herramientas. Así también dentro del desarrollo de las aplicaciones o sistemas operativos los programadores dejan atajos llamados backdoor's o puertas traseras, algunos se dejan por mantenimiento posterior o por descuido; la cuestión es que si un atacante descubre una de estas puertas va a tener acceso a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad de sistema o red. Las bombas lógicas son partes de código de ciertos programas los cuales permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial, los activadores pueden ser algún fichero, una fecha, etc.
Los canales cubiertos son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad, dicho de otra forma, un proceso transmite información a otros que no están autorizados a leer dicha información.
Los virus son secuencias de código que se inserta en un fichero ejecutable, de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a si mismo en otros programas. Los gusanos, son programas capaces de ejecutarse y propagarse por si mismos a través de la red, en ocasiones portando virus o aprovechando bugs de los sistemas a los que se conecta para dañarlos.
Los caballos de Troya son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera de él, pero tiene funciones ocultas sin el conocimiento del usuario, como el caballo de Troya de la mitología griega, al que debe su nombre, oculta su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

3.4. Controles de Seguridad.

Dependiendo del entorno de la organización o institución, se pueden tener diferentes amenazas que comprometan a los objetivos de la seguridad, ante un riesgo concreto, la institución tiene tres alternativas: aceptar el riesgo, hacer algo para disminuir la posibilidad de ocurrencia del riesgo o transferir e riesgo. Un control de seguridad es la medida o salvaguarda que se toman para disminuir un riesgo.

3.4.1. Controles de Seguridad física.

El objetivo de los controles de seguridad física, es el de prevenir o disuadir eventos ilegales o no autorizados y si ellos ocurren detectar los mismos y eventualmente retardar la actividad a fin de ganar tiempo de respuesta.Por medio de la instalación de cercas, puertas, llaves, cerraduras, iluminación, barreras.

Sistemas de energía eléctrica ininterrumpible.

Un SAI por sus siglas en inglés, Uninterruptible Power Supply, UPS es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de las funciones de los UPS es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red eléctrica en caso de usar corriente alterna. Estos equipos dan energía a equipos llamados cargas criticas, como pueden ser aparatos médicos, industriales o informáticos que como se menciona, requieren tener siempre alimentación y que esta sea de calidad, debido a la necesidad de estar operativos en todo momento y sin fallos.

Control de acceso.

El control de acceso contempla la implementacion de una estructura de seguridad apropiada para prevenir o detener el acceso no autorizado a material confidencial. Tales como: cámaras de circuito cerrado, sistemas de alarma térmico, guardias de seguridad, identificación con fotografía, puertas de acero con seguro especial o algo mas sofisticado como acceso biométrico por medio de huellas digitales, voz, rostro etc.

3.4.2. Controles de Seguridad Lógica.

Luego de ver como los sistemas se pueden ver afectados por la falta se seguridad física, es importante mencionar que la mayoría de los daños que puede sufrir un equipo de cómputo no sea sobre sus medios físicos, sino contra la información almacenada y procesada en el. Para evitar eso, es necesario aplicar barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas a hacerlo. Estos controles pueden ser de implementados a nivel de sistema operativo, base de datos, o por medio de un sistema de aplicación. Son importantes por que ayudan a proteger de acceso o modificaciones no autorizadas.

La mayoría de las empresas y/o instituciones sufren la problemática de seguridad debido a sus necesidades de acceso y conectividad con: Redes públicas, Internet, accesos remotos, proveedores, partners, red corporativas e institucionales.

Controles de Acceso internos.

Llamamos controles internos por que se aplican dentro de la red local, tales como:

- Passwords.

  Las palabras clave se utilizan para autenticar a los usuarios, sirven para proteger los datos y aplicaciones, estos son a bajo costo, la desventaja esta en la robustez de la clave, dado que si se utilizan palabras de diccionario es fácil para un intruso adivinarlas. Para evitar esto existen algunas alternativas para con los passwords tales como: la sincronizacion de los mismo, lo cual consiste en permitir que el usuario acceda a múltiples sistemas con una sola clave, siempre que esta clave sea de alto nivel de seguridad, así como también es necesario un mecanismo que defina el periodo mínimo que debe pasar para que los usuarios cambien sus claves y un máximo para que estas caduquen.

- Cifrado.

  El cifrado es un método potente como medida de control de acceso. La ciencia que se encarga de transformar la información de manera tal que estas quede encubierta y sea incomprensible para todo aquel que no tenga la autorización de acceso se llama criptografía. La contraparte es el criptoanálisis es la disciplina encargada del estudio de los métodos para romper los mecanismos de cifrado, sin necesidad de conocer ninguna clave y así obtener o interpretar ilícitamente la información cifrada. Así bien son disciplinas opuestas y en conjunto forman la criptología. La información cifrada puede ser vista por quienes posean la clave apropiada.

- Listas de Control de Acceso ACL's.

  Las listas de control de acceso son registros en los que se encuentran los datos de los usuarios que obtuvieron permiso de acceso a un recurso del sistema, así como la modalidad del acceso.

Control de Acceso externo.

Definimos acceso externo como mecanismos que gestionan la entrada física y lógica. Algunos de los mecanismos de control son:

- Dispositivos de control de puertos.

  Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otros dispositivos de comunicaciones.

- Firewalls o puertas de seguridad.

  Estos dispositivos permiten bloquear o filtrar el acceso entre dos redes, estos permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Este tema sera explicado ampliamente mas adelante.

- Acceso de personal externo.

  Debido a que existe la contratación de personal externo que presta servicios temporarios, debe ponerse a consideración la política y administración de los perfiles de acceso.

- Accesos públicos.

  Para los sistemas de información que son de consulta pública en general, deben tenerse en cuenta medidas de seguridad especiales, dado que el riesgo se incrementa y la administración también.

Firewall.

Un firewall es un o grupo de dispositivos, que aplica una política de control de acceso, restringe el acceso entre una red protegida e internet, o entre redes.

Un requerimiento para los firewalls, es la revisión de los clientes con conexiones entrantes, para permitir o denegar el acceso. A esta verificación se le denomina *network access control (NAC) o network access protección (NAP)* este permite el acceso basado en credenciales del usuario lo cual lleva a una revisión de rutina para el acceso a la red. Existe una variedad de modelos de seguridad, o enfoques que van desde la ausencia de seguridad, "security through obscurity"(seguridad por oscuridad), a la seguridad de host y la seguridad de la red.

- *Security through Obscurity* Es un principio que consta de asegurar las cosas escondiéndolas. En términos de cómputo quiere decir que es similar a conectar un equipo de cómputo a la red y creer que nada le pasará, por que nadie sabe que esta allí, o configurar un firewall para que los outsiders [1] no puedan obtener información interna de la red. Así bien no publicar algo no es lo mismo que esconderlo.

[1]Para propósitos especifico de esta tesis, se denota a un outsider como intruso potencial externo a la red institucional y/o corporativa.

> Entre menos información puede obtener el atacante mejor, la ignorancia no los detendrá, pero se gana tiempo, para que algún sensor de tráfico lo detecte a tiempo e impida la infiltración.

A medida de que los entornos se hacen mas grandes y diversos, la seguridad de host ya no es suficiente.
La mayoría de las instituciones están recurriendo a un modelo de seguridad de la red. Es por demás mencionar que ningún modelo de seguridad provee protección perfecta, la seguridad no puede prevenir todos los incidentes, pero si puede prevenir que un incidente cause un grave daño o la negación de algún servicio.

En la construcción de edificios un firewall esta diseñado para detener el fuego y evitar que este se propague hacia otras áreas. En teoría un firewall de red tiene un propósito muy similar; este previene que las amenazas en internet se propaguen hacia la red interna.

- Restringe el acceso a puntos controlados.
- Protege el perímetro de la red.
- Protege a los usuarios de situaciones de riesgo.

Lógicamente un firewall separa, restringe y analiza.

Por lo general un firewall es implementado en el punto en donde la red interna se conecta con Internet. Todo el tráfico proveniente de Internet pasa a través de él, de esta manera el filtro tiene la oportunidad de saber si el tráfico es aceptable; cuando se implementa un firewall, se encuentran dos perímetros bien definidos.

- Perímetro interno: Donde se sitúan todos los recursos sensibles a un posible ataque.
- Perímetro externo: Donde se sitúan los recursos menos sensibles que necesitan ser accesibles desde la red externa por motivos funcionales.

Ambos deben estar aislados entre sí, por medio de un dispositivo donde se implementarán las reglas de acceso, es decir un firewall. Un firewall puede hacer mucho por la seguridad de la red, dado que: el dispositivo es el centro de las decisiones sobre seguridad y hace cumplir las políticas de seguridad este puede registrar la actividad hacia Internet eficientemente y limita la exposición de la red interna hacia Internet. Existe una variedad de tecnologías de firewall, un modo de comparación de sus capacidades es la verificación de las capas del modelo TCP/IP en que opera dispositivo, típicamente son las mas bajas como Internet y Acceso a la red.

Tipos de Firewall.

La función primaria de un firewall es filtrar, además de los servicios y otras capacidades que el firewall posea. Un firewall puede soportar diferentes tipos de filtrado, adicionalmente a los términos de uso.

Packet Filter También llamado *Stateless inspection firewall*, este filtrado se basa en permitir o denegar el tráfico de red basado en el encabezado de cada paquete acorde a las reglas de filtrado, este encabezado es revisado por el packet filter una vez hecho esto el firewall tiene tres opciones:

- *Send:* Envía el paquete a su destino.
- *Drop:* Descarta el paquete sin notificar al remitente.
- *Reject:* Rechaza el paquete, no lo reenvía y manda una notificación al remitente.
- *Log:* Registra la información acerca del paquete.

Como el filtrado tiene la capacidad de revisar cada uno de los paquetes de entrada y salida, este puede identificar fácilmente si existe alguna insistencia de una dirección ip de origen hacia destino en particular. El tráfico entrante es conocido como filtrado entrante *(ingress filtering)* , y el saliente como filtrado de egreso, *(egress filtering).*
Packet filter no lleva un registro del estado de las conexiones que atraviesan el firewall,es decir que no es posible crear una asociación entre múltiples peticiones de una sesión activa. Las ventajas de emplear este tipo de filtrado son: dado que es un filtro simple y la información que se revisa en los encabezados es poca el filtrado es de bajo costo operativo. Sin embargo entre mas procesamiento de paquetes mas lento sera el filtro y este tipo de filtros es ampliamente disponible para casi cualquier software y hardware, aúnque no es una herramienta perfecta ciertamente contempla algunas limitaciones: las reglas son difíciles de configurar, una vez configuradas son difíciles de probar, sin contar con que la mayoría del software tiene bugs lo cual causa problemas de seguridad sobre el mismo servicio, lo cual puede causar un mal funcionamiento por parte del filtro y que este valide paquetes erróneos.
El static packet filter puede ser problemático si el set de reglas es muy largo, si las reglas no están en orden o el orden no existe, el set puede crear *loopholes*. Packet filter reduce el rendimiento del dispositivo dado que aporta una carga mas al procesador,entre mas complejo el filtrado mas procesamiento requiere, la complejidad del filtrado puede aumentar si se filtra, puerto, protocolo o banderas de estado.

Stateful Application Inspection Es el proceso de envío o rechazo de tráfico basado en el contenido de la tabla de estado del firewall. Es una forma de packet filter pero dinámico, el cual crea filtros temporales de entrada, salida y tiempos de espera limitados, por lo que *dynamic packet filter* y *stateful inspection* pueden ser términos intercambiables. Stateful intercepta los paquetes en la capa de red e inspecciona si es permitido con base a una regla declarada en el set del firewall, a diferencia del tipo packet filter, este tipo de

filtrado rastrea las conexiones en una tabla de estado, esta tabla de estado por lo general contiene datos como: IP de origen, IP de destino, puerto y el estado de la conexión. Permite abrir sesiones a cierto tipo de tráfico basado en conexión, al cerrar la sesión la conexión termina. Posee registro de las conexiones, sesiones y contexto, para conexiones TCP. Para UDP que no tiene un proceso formal de conexión y el estado no puede ser determinado, por lo que se rastrear el puerto y la dirección IP, para permitir el tráfico de paquetes el firewall espera una respuesta del DNS del exterior, de esta manera entonces verifica que hubo una petición interna hacia el DNS, como el firewall no puede determinar cuando la conexión ha terminado entonces el estado de borra de la tabla después de un tiempo pre-configurado en el firewall.

Full Application Inspection Es un tipo de filtrado capaz de inspeccionar hasta nivel de aplicación, se revisa el contenido de la trama y soporta autenticación. Un filtrado de aplicación es una versión especifica de filtrado, este tipo de filtrado es capaz de inspeccionar el tráfico a cualquier nivel del modelo OSI, incluyendo así la capa de aplicación, lo cual incluye direcciones IP, nombres de domino, URL's, palabras clave etc. Este ultimo es denominado filtrado de contenido, el firewall intercepta contenido especifico de los paquetes antes de abandonar la red interna, de manera que puede bloquear, descartar o reemplazarlo, estos filtros son de ayuda cuando se enfocan en nombres y extensión de los archivos. También conocido como *deep packet inspection* este tipo de filtrado añade tecnología de detección de intrusos, mediante un motor de inspección que analiza los protocolos en la capa de aplicación, genera un perfil sobre la actividad de aplicación en la red. Los firewalls de aplicación pueden identificar secuencias de comando fuera de lo común que tengan comportamientos de tipo ataque, como la longitud de nombre de usuario extremadamente largo, peticiones hacia una base de datos o hacia un web. Una variación de los firewalls de aplicación son los *application-proxy gateway* el cual combina las funcionalidades de control de acceso de capas altas y bajas, este tipo de firewall no permite la creación de conexiones directas y el resultado es el establecimiento de dos conexiones separadas teniendo como intermediario el proxy. Este proxy trabaja en la capa de aplicación por lo cual es capas de verificar el contenido del tráfico, cifrar, decifrar y realizar verificaciones de TCP handshake lo cual lo genera una protección extra. La diferencia entre estos dos firewall consta en que los proxys proveen un mayor nivel de seguridad para algunas aplicaciones por que previenen las conexiones directas entre dos host y de esa manera puede inspeccionar el contenido del tráfico e identificar violaciones en las políticas de seguridad.

Arquitecturas de Firewall

Dual Homed Gateway Esta arquitectura es sobre un host *dual-homed*, este host contempla por lo menos dos interfaces de red *ver fig3.3*. Una de entrada y otra de salida, esto forza la separación de las redes, y posee la habilidad de obtener doble filtrado, uno en cada tarjeta. Esta arquitectura es bastante simple dado que el firewall se sitúa justo en medio de la red local y el acceso a internet, este tipo de filtros poseen un alto nivel de control. La seguridad del mismo debe ser impecable dado que es un solo punto de fallo, si un intruso compromete un dual-homed obtiene acceso completo a la red y tiene la habilidad de desconectar el firewall de internet, provocado un DoS. Esta arquitectura es apropiada cuando el tráfico a internet es poco, no es crítico y el contenido de los datos no es extremadamente valioso.

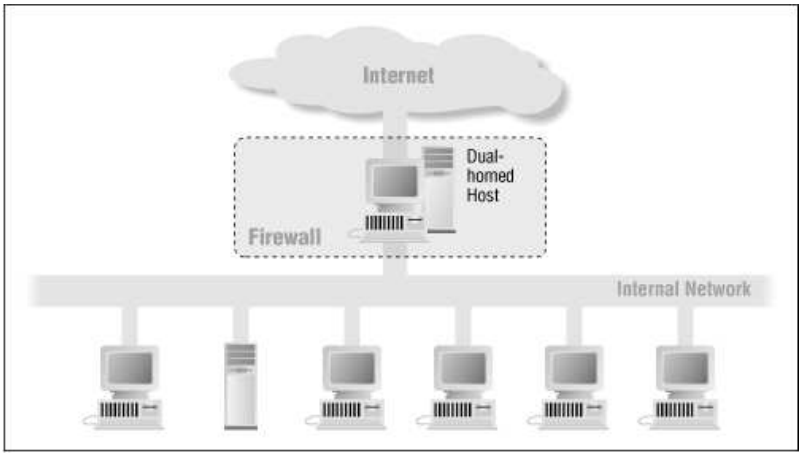


Figura 3.3: Arquitectura Dual Homed.

Screened/ Bastion Host Es posible tener un sistema de filtrado como firewall, por medio de un screened router *ver fig3.4* que proteja la red. Es de bajo costo dado que es casi necesario tener un router para la conexión a internet, de esta manera se puede configurar el dispositivo para filtrar protocolos y puertos. Y esto no ofrece una seguridad profunda. Si el firewall es comprometido, no existe seguridad. Por ello este tipo de filtros se utilizan en redes que ya tienen buena seguridad a nivel de host y el número de protocolos entrantes es limitado. Un Bastion host es aquel que esta directamente hacia la conexión de Internet en este host se puede configura un filtrado independiente o un servidor proxy, en cualquier caso este sera quien gestione las conexiones entrantes y salientes.

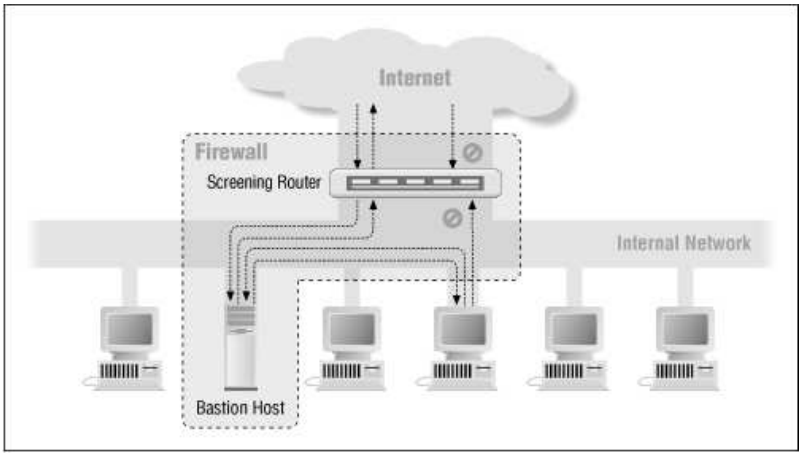


Figura 3.4: Arquitectura Screening/Bastion Host .

DMZ Del RFC *2647 firewall performance terminology* se tiene la definición siguiente: *."Es un segmento o segmentos de red ubicadas en medio de la red protegida y desprotegida."* Cuando hablamos de firewalls es inevitable determinar los perímetros mencionados anteriormente, por lo que surge el concepto de *DMZ*, la traducción de este termino es zona desmilitarizada y se trata de una red local que se ubica entre la red interna y externa, el objetivo de una DMZ es que las conexiones desde la red interna y externa estén permitidas, mientras que las conexiones de la DMZ solo sean hacia el exterior. Para cualquiera que trate de conectarse hacia la red interna, la zona desmilitarizada se convierte en una trampa. Dentro de la DMZ por lo general se ubican los servidores hacia el exterior.

Servicios de red de un firewall

DHCP El protocolo por sus siglas en ingles Dynamic Host Configuration Protocol, es un protocolo de red que permite a los host de red obtener una dirección IP junto son sus parámetros de configuración . Es un protocolo de tipo cliente/servidor [2] este servidor posee una lista de direcciones también llamado *pool* y este va asignándolas conforme estén libres, esta asignación es dinámica dado que si una dirección ha sido ocupada solo unos minutos, al ser liberada regresa al pool para ser reasignada este protocolo documentado en el RFC 2131 fue publicado en el año de 1993.

Los modos de asignación del DHCP pueden ser:

- **Manual o Estática:** Se asignan direcciones IP a un host determinado, esto ocurre en casos en los que es necesario el control de la asignación hacia los clientes y evitar así la conexión de equipos no identificados.
- **Automática:** Se asigna la dirección de manera permanente al host, esto cuando el número de clientes no varia demasiado.

[2]La arquitectura cliente-servidor es un modelo de aplicación distribuida en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados servidores, y los demandantes, llamados clientes.

- **Dinámica:** Es el método que permite reutilizar las direcciones, el administrador determina un rango de IPs y cada dispositivo puede solicitar una dirección en cuanto inicie la tarjeta de red. Esto facilita la instalación de nuevos host en la red.

  El método que emplea este protocolo para la negociación de la dirección IP, *ver fig3.5* se le conoce como DORA por las iniciales de las banderas activas y se realiza de la siguiente manera:

  - *DHCP Discovery* Esta solicitud DHCP es realizada por el cliente, hacia el servidor dentro de la red,para la asignación de la IP.
  - *DHCP Offer* Este es un paquete de respuesta del servidor DHCP al cliente, ante la petición anterior, en este punto la dirección física se involucra.
  - *DHCP Request* El cliente selecciona la configuración de los paquetes recibidos en la oferta, una vez mas el cliente solicita una dirección IP.
  - *DHCP Acknowledge* El servidor recibe la petición del cliente,para iniciar la fase final. En esta fase se inicia el reconocimiento DHCPACK en el envío del paquete al cliente. Este paquete incluye la duración e información necesaria para el cliente. En este punto el servidor reconoce la solicitud y envía un acuse de recibo al cliente.

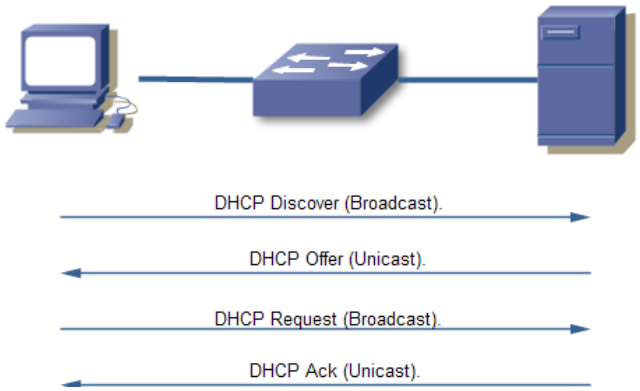


Figura 3.5: Proceso de DHCP.

Servicios de enrutamiento.

NAT Network Address Traslation es el proceso de modificación de la información en las cabeceras del paquete de una dirección IP mientras este atraviesa un dispositivo de enrutamiento. Esto permite que una red utilice un set de direcciones IP internas, y otro diferente externo.
A veces se piensa que el servicio NAT es una tecnologia de firewall, sin embargo es tecnología de enrutamiento no exclusiva de un firewall.

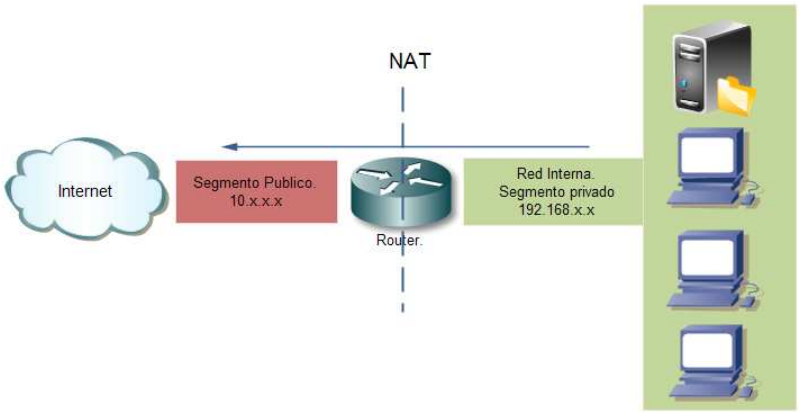


Figura 3.6: Traducción NAT.

Existen varios tipos de NAT, tales como one-to-one NAT, NAPT (network address and port translation) , PAT (port address translation) estos dos últimos tienen la opción de hacer la traducción a nivel de puerto. Tipicamente NAT actua como un *router* el cual posee direcciones privadas adentro y una sola dirección pública hacia Internet. La traducción del NAPT en donde se mapea un puerto destino en particular en el NAT y un solo host dentro de la red LAN se llama *Pinholing*.

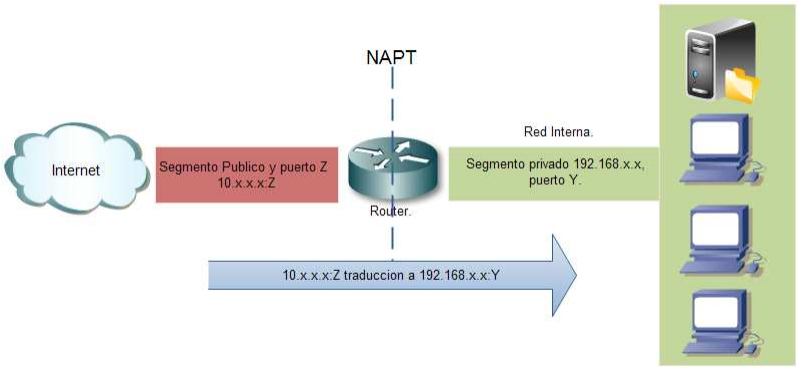


Figura 3.7: Pinholing.

Las ventajas de utilizar NAT, son: El servicio ayuda y fortalece el control del firewall sobre las conexiones entrantes y salientes, ayuda a esconder la información acerca del número de host, tipo, etc, dado que la red interna queda bajo una sola IP.

Modos de un Firewall Con referencia al modelo OSI y la capa en la que el firewall opera, se tienen 3 tipos o modos de firewall.

Modo Load Balancing El balanceo de carga es un concepto informático que refiere una técnica la cual consiste en compartir la carga de trabajo entre varios recursos tales como, procesos, discos, tarjetas de red, etc con el fin de optimizar los recursos, maximizar el rendimiento, minimizar el tiempo de respuesta y evitar la sobre carga. Esto se logra mediante el uso de varios dispositivos, en lugar de uno solo, esto incrementa la disponibilidad a través de la redundancia, usualmente es un servicio dedicado en software o hardware, como un switch o un servidor.

Figura 3.8: Balanceo de Carga.

El balanceo es útil en los enlaces de comunicaciones redundantes, por que se tiene mas de una opción para la conexión a Internet, el firewall que balancea cargas posee dos o mas interfaces de red , y entre ellas distribuye el tráfico uniformemente o también es utilizado para proveer HA (High Availability)en el caso en el que el enlace principal no funcione, hay otro mas activo; o ambos enlaces están activos y un dispositivo independiente, supervisa la disponibilidad de los mismos, entonces se reparte el tráfico y se previene la congestión. Existen 3 tipos de balanceo de carga.

1. Random Allocation (Asignación al Azar). En este tipo las peticiones son asignadas al azar, el servidor de balanceo se elige dentro de un grupo, es el mas simple de implementar.

2. Round-Robin. En este tipo de balanceo, el servidor asigna las peticiones a una lista de los servidores, en forma rotativa.

3. Weighted Round-Robin. Este tipo de asignación rotativa, asigna un peso a cada servidor de manera que el servidor es capaz de manejar carga doble, entonces se asigna hacia ese servidor con capacidades mas grandes. Lo bueno de este tipo de balanceo es que es acorde a las capacidades del equipo.

Algoritmos de Balanceo de Carga. Algunos de los Algoritmos que se emplean para la distribución del tráfico, y realizar el balanceo de carga del mismo son:

- **Weighted Balance** *(Contrapeso).* Este algoritmo asigna el tráfico al enlace mas rápido y disminuye en los mas lentos, es decir que el tráfico se envía por el enlace que tenga mayor ancho de banda, a medida que los enlaces tengan disponibilidad el trafico cambiara en cada uno de ellos.

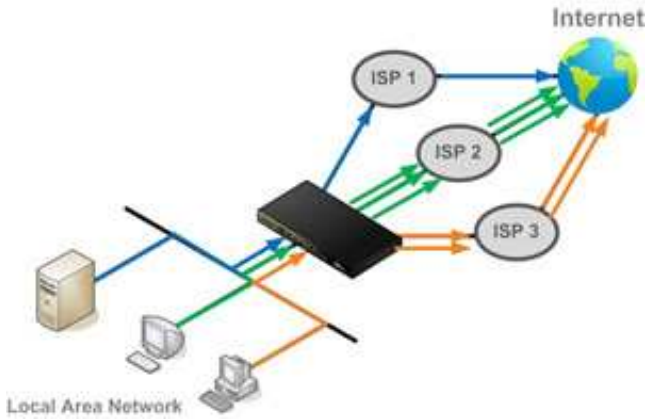


Figura 3.9: Se asigna una escala para cada conexión saliente de tráfico para distribuirlo proporcionalmente.

- **Priority** *(Prioridad).* En este algoritmo el trafico es enviado hacia el enlace que este activo, el tráfico es enrutado hacia la conexión que este disponible y tenga la prioridad siguiente con respecto a la escala, el enlace con la prioridad mas baja sera utilizada solo si los demás enlaces fallan *ver fig3.10 y 3.11.*

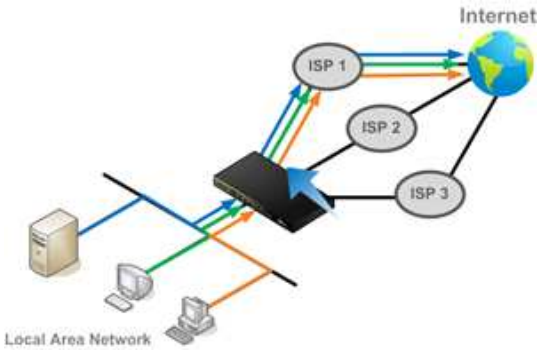


Figura 3.10: El tráfico viaja por el enlace normal.

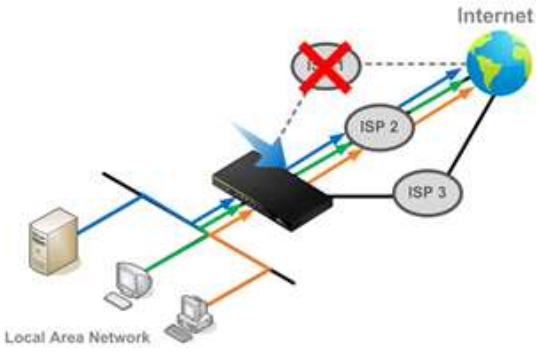


Figura 3.11: El tráfico se desvía hacia el enlace funcional.

- **Overflow** *(Sobreflujo).* Previene el tráfico lento cuando la conexión ya no tiene ancho de banda disponible, si el firewall se percata de que existe pérdida de paquetes durante la transmisión de la información, entonces comenzara a enviar parte del trafico por otro enlace activo *ver fig3.12*, es importante mencionar que no es todo el trafico, solo parte de este, para aliviar la congestión que se genera en el primer enlace *ver fig3.13*.

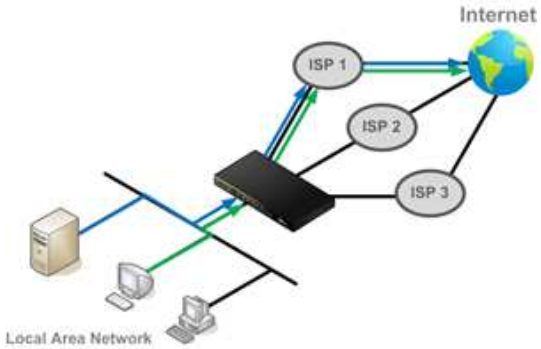


Figura 3.12: El tráfico fluye por el enlace con la prioridad mas alta.

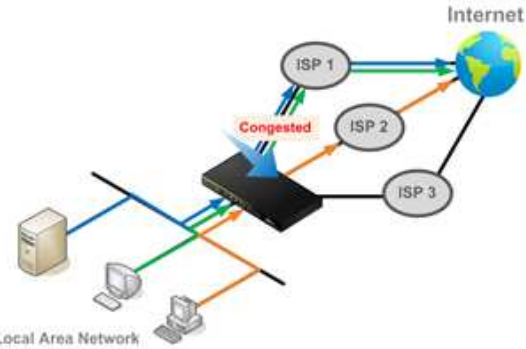


Figura 3.13: El tráfico cambia a un enlace activo sin congestionamiento.

- **Persistence** *(Persistente.)* Elimina los problemas de termino de sesión para algunos protocolos como HTTPS, por que la sesión durara activa por el mismo enlace *ver fig 3.14 y 3.15*.

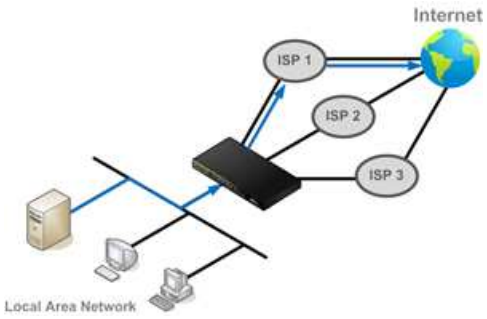


Figura 3.14: Balanceo de carga por enlace.

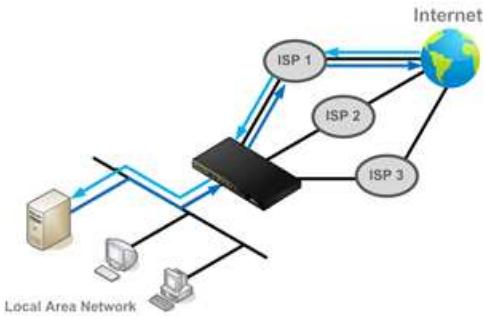


Figura 3.15: Balanceo por persistencia hasta que termine la conexión.

- **Last Used** *(Ultimo Utilizado.)*

  El tráfico sera enrutado hacia el enlace que tenga menos uso *ver fig 3.16 y 3.17.*

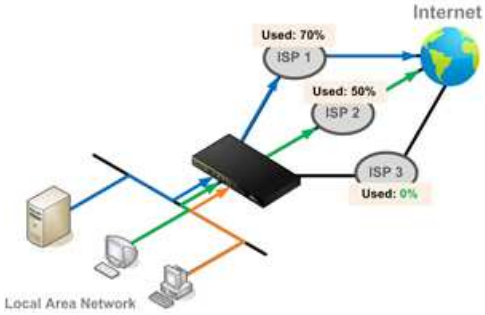


Figura 3.16: Balanceo de carga con enlace menos uso.

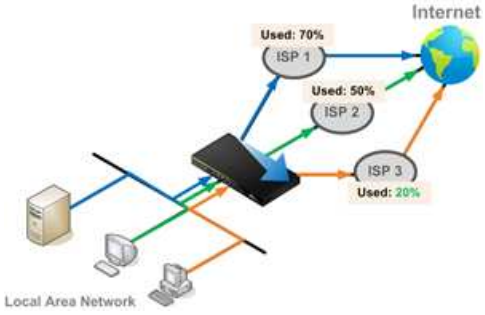


Figura 3.17: Balanceo de carga con el porcentaje mas bajo.

- **Enforced** *(Cumplimiento.)* El tráfico es restrigido a conexiones particulares, es decir que se elige el tipo de tráfico para ser enrutado todo el tiempo aún si el enlace esta activo o no. Este tipo de accesos son empleados en arquitecturas cliente servidor que permite el acceso solo de direcciones IP exclusivas.

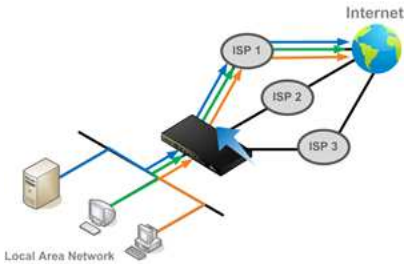


Figura 3.18: Balanceo de Carga tipo Enforced.

- **Lowest Latency** *(Menor latencia.)*

  El tráfico se asigna al enlace que posea en parámetro de menor tiempo de latencia, de los enlaces activos.

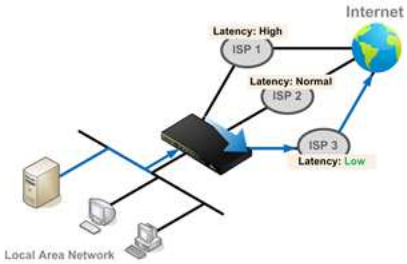


Figura 3.19: Balanceo de carga tipo Lowest Latency.

Modo Bridge Un bridge es aquel dispositivo de red que reenvía el tráfico de una interfaz a otra, por lo tanto los mismos datos fluyen a través de las dos interfaces; para que un firewall posea un comportamiento de tipo bridge, este debe poseer mínimo dos interfaces de red, una de entrada y otra de salida, en el caso del bridge ambas interfaces deben contar con una dirección IP para funcionar como gateway y así enviar todo el tráfico de la red LAN a través de este puente entre tarjetas de red justo en medio de ese proceso se ejecuta la tarea principal de un firewall: filtrar. El punto débil de este filtrado tradicional es que los paquetes una vez que han atravesado el filtro, y el firewall los ha permitido, este debe enrutarlos hacia su destino. Por ello la necesidad de que el filtro sea visible.

Modo Transparente La manera de simplificar el comportamiento de bridge radica en cambiar de capa con respecto al modelo OSI, esto significa que el filtrado de paquetes se hará en la capa de enlace: a este tipo de firewall se le denomina: **firewall transparente**. Los frames fluyen de una tarjeta a otra, este tipo de dispositivos es mucho mas sencillo, con mejor desempeño y menos procesamiento; una ventaja del mismo es que prácticamente no hay configuración sobre la red LAN, esto quiere decir que no es necesaria la configuración sobre algún otro dispositivo de red,para su implementación lo único que se hace es conectar este filtro en medio de los dispositivos a filtrar, como el firewall no posee dirección IP esta cualidad lo hace inalcanzable o invisible para Internet, lo que genera una ventaja dado que si no es visible, entonces puede alguien atacarlo?. Otra ventaja del firewall transparente es que así como no es necesario ningún tipo de configuración para su implementación tampoco lo es para sacarlo de producción, simplemente se le desconecta.

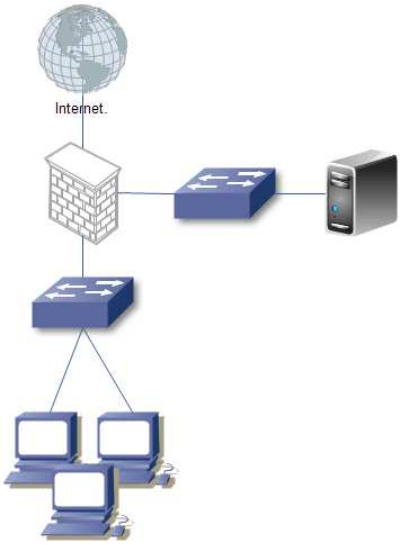


Figura 3.20: Firewall Transparente.

3.4.3. Integración de Políticas de Seguridad Informática.

Las politicas de Segurida Informatica (PSI) se suelen definir como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema, la cuales indican en términos generales que está y que no está permitido en el área de seguridad durante la operación general de dicho sistema. Dichas políticas son desplegadas y soportadas por estándares, mejores practicas, procedimientos y guías. Son de carácter obligatorio y la incapacidad o imposibilidad de su cumplimiento exige la aprobación de una excepción.

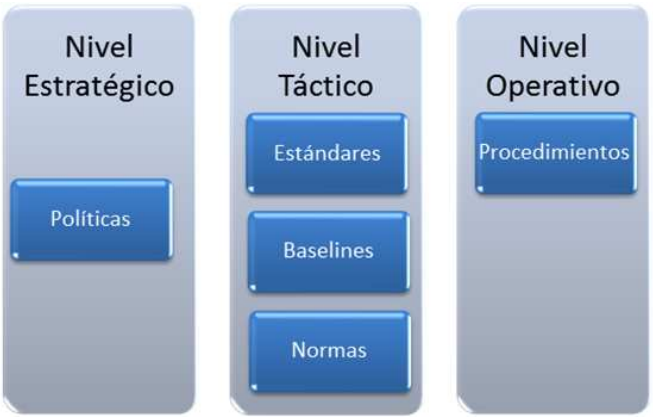


Figura 3.21: Estructura normativa.

Una política de seguridad puede ser prohibitiva, si todo lo que no esta expresamente permitido esta denegado, o permisiva, si todo lo que no esta expresamente prohibido esta permitido. Para cubrir los objetivos de la seguridad informática e institucionales, una política se suele dividir en puntos mas concretos a veces llamados normativas. Las políticas definen la organización de seguridad de la información, es independiente de la tecnología y las soluciones, define responsabilidades y autoridades para la implantación de la seguridad informática. Es importante resaltar que una política de seguridad tiene un ciclo de vida completo, este ciclo contempla, el diseño, aprobación, complementación, monitorización y actualización; de lo contrario pueden generarse políticas incompletas, redundantes,o inútiles.

Un estándar es una regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Un estándar es una regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares sirven como especificaciones para la implementación de políticas: son diseñados para promover la implementación de las políticas de alto nivel de la institución antes de crear nuevas políticas.Las mejores practicas son reglas de seguridad especificas para proporcionar un enfoque mas efectivo a una implementación de seguridad concreta. Son establecidas para asegurar que las características de seguridad de sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la institución. Una Política de Seguridad Informática es una herramienta organizacional para concientizar a los usuarios sobre la importancia y sensibilidad de la información. Con base a las mejores

practicas, estándares y análisis de riesgos es posible la creación de Políticas de Seguridad, sin esto es posible que existan fallas de seguridad indeseadas.

En resumen se tienen las siguientes definiciones:

- **Estandares:** Especifican la forma de poner en práctica un objetivo de la Política, define actividades, acciones, reglas o regulaciones obligatorias,una determinada tecnología o la aplicación de una solución de manera uniforme.
- **Lineas base***(Baselines)*: Determinan como deben ser configurados los aspectos de seguridad de las diferentes tecnologías.
- **Normas***(Guidelines)*: Son definiciones generales establecidas para colaborar con el cumplimiento de los objetivos de las Políticas proporcionando un marco en el cual implementar controles adicionales.
- **Procedimientos:** Son una descripción detallada de tareas a realizar para complementar los estándares y lineas base.

Las PSI dan vida a las políticas de firewall las cuales se definen en como el firewall debe manejar el tráfico de red para protocolos, aplicaciones, contenido y rangos o direcciones IP en particular.

Para tener un panorama mas amplio de lo que debe ser permitido y lo que debe ser bloqueado existen diferentes tipos de politicas las cuales se explican a continuación:

- **Políticas de firewall basadas en Protocolos y dirección IP.**

  Estas políticas deben permitir solo rangos de direcciones IP apropiadas, el tráfico de direcciones invalidas debe ser bloqueado, tales como direcciones de loopback, localhost, broadcast y link-local. El tráfico entrante de direcciones privadas (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16), tráfico saliente con direcciones de broadcast debe ser bloqueado; así como el tráfico entrante ICMP debe ser bloqueado exceptuando algunos tipos de código necesarios.

- **Políticas basadas en aplicación.** La base en aplicación provee una capa mas de seguridad para el tráfico entrante, tras validar el tráfico antes de que llegue a su destino. En teoría el tráfico saliente debe ser depurado para proteger al servidor mucho más de lo que el mismo pudiera protegerse.

- **Políticas basadas en Identidad del Usuario.** Varias tecnologías de firewall pueden establecer políticas basadas en autenticacion, cuyo modo es uno de los más comunes para acceder a la red, por medio de contraseñas, certificados etc. Los firewalls que emplean este método deben registrar la actividad en sus bitacoras del sistema.

- **Políticas basadas en Actividad de red.** Estas políticas consisten en las conexiones establecidas y su inactividad, es decir que el firewall verifica el tiempo que la conexión lleva establecida y si no registra actividad cierra la conexión automáticamente.

Capítulo 4

Estudio de Caso e implementación.

4.1. Estudio de Caso: IB.

El estudio de caso del Instituto de Biología abarca toda la red de datos y la seguridad de dicha red en producción.
Como primer punto se realizó un análisis del perímetro, para identificar los mecanismos y dispositivos de seguridad en producción de la red. Se encontraron los siguientes servicios de seguridad: un firewall de arquitectura *dual-homed* que cuenta con un filtrado de tipo *packet filter* mediante el motor de filtrado *IPtables* con un set de 748 reglas, sobre el sistema operativo Linux Fedora Core 8, el servicio de red inalámbrica se provee con 20 antenas inalambricas las cuales gestionan el control de acceso mediante el filtrado local de tipo MAC address. El filtrado de contenido se realiza con un dispositivo marca 3COM ®Tipping Point modelo x506 con características de firewall capa 7 e IDS. No hay administración centralizada ni sistema de monitorización. La problemática más común en la conexion a Internet era la pérdida repentina del servicio y la calidad del mismo, lo cual se traduce en una red inestable y con problemas de ancho de banda, generando incomodidad en la comunidad e inclusive la pérdida de datos. Por lo que se realiza un segundo análisis enfocado a la arquitectura de la red de datos, para identificar el origen de este tipo de inconvenientes ocurridos en la transmisión de la información. Dicha arquitectura de red contempla una red LAN en producción con topología física de árbol y lógica FDDI, subdividida en 10 VLANs gestionadas por un dispositivo multicapa central, el cual genera la interconexión de capa de distribución y realiza la tarea de enrutamiento interVLAN y DMZ a lo largo de 6 edificios, incluyendo el Jardín Botánico y el Invernadero Faustino Miranda.

De dicho análisis de red se obtuvo el siguiente esquema de red de datos en producción *ver fig 4.1* .

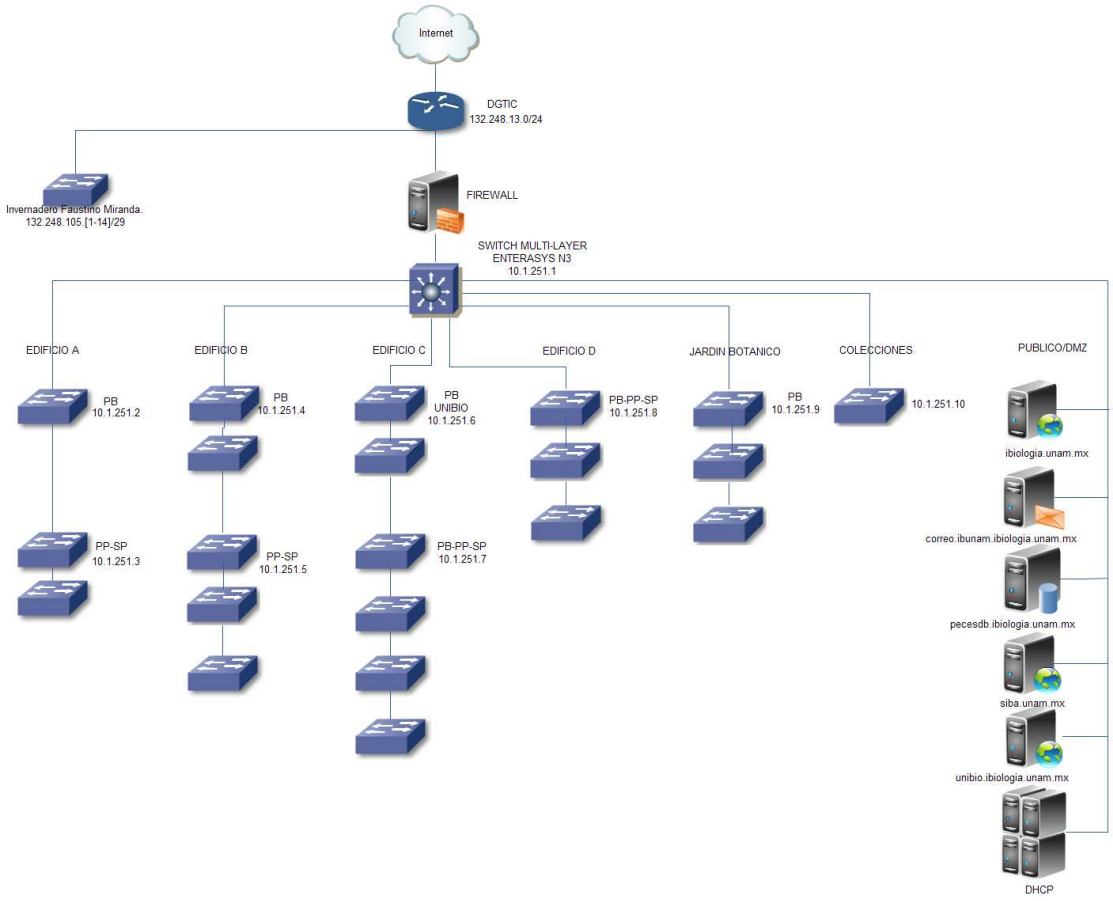


Figura 4.1: Topologico de la red de datos en producción.

El análisis arrojo varios puntos de fallo en la arquitectura de red física y lógica del Instituto de Biología, un número considerable de vulnerabilidades en diferentes servicios de red.

Iniciando por la topología física, la cual contiene dos puntos de fallo críticos, el primero reside en el firewall el cual posee múltiples vulnerabilidades sobre el sistema operativo y su ubicación lógica no era completamente estratégica dentro del esquema de seguridad; el segundo se trataba del switch de *core* en fibra óptica el cual realizaba la conexión tipo estrella, este switch era público. Lo cual generaba un hueco de seguridad,en la única capa de seguridad existente, generando una vulnerabilidad de alto impacto en el servicio, comprometiendo los objetivos de la seguridad informática. Dicha configuración no es viable, para equipos de telecomunicaciones y seguridad de tal envergadura, por lo cual no es recomendable que tanto un firewall como un switch de *core* deban intercomunicarse por medio de IPs públicas, dado que si alguno de los dispositivos es comprometido el impacto seria crítico, generando una pérdida de datos y la denegación de Internet. Uno de los objetivos de la optimización, fue privatizar la comunicación entre estos dispositivos por medio de IPs privadas para eficientar la comunicación y que su medio fuese vía intranet. Los servidores que proveían diferentes servicios hacia la comunidad, poseían vulnerabilidades lógicas por falta de actualizaciones y parches de seguridad de sistema operativo. No existían respaldos automatizados de las configuraciones de la capa de acceso, por lo que si algún dispositivo de telecomunicaciones fallaba y era necesario su reemplazo, las configuraciones debían de generarse al vuelo.

Por otro lado la administración del control de acceso inalámbrico era individual en cada unos de los puntos de acceso, esto aumentaba el tiempo de administración del control de cambios en las antenas ya que si se requerían cambios en la configuración, era necesario realizar la operación en cada uno de los 20 APs. No existía una DMZ como tal, dado que los servicios públicos convivían con la red interna y el tráfico se mezclaba en uno o más dispositivos, esto representaba otra falla en la capa de distribución de la red LAN, la vulnerabilidad reside en la exposición del switch multicapa el cual poseía una dirección pública para su administración y operación, por lo que su funcionamiento en red se veía comprometido si se llegase a explotar por cualquier método el acceso al equipo, y este fuese exitoso, el atacante tendría el control total de la red de datos y de los servicios críticos comprometidos, tales como el correo electrónico, página web, repositorio de archivos, etc.

Por otra parte dentro de la red en producción del Instituto se aloja una VLAN con servicios públicos,plataformas y bases de datos los cuales necesitaban ancho de banda especifico y una correcta colocación dentro de la topología física y lógica del Instituto de Biología. La vulnerabilidad de esta Unidad representa el riesgo de pérdida de datos, y el bajo desempeño que esta red llegaba a tener, por ser una red anidada dentro de otra red, lo cual generaba lentitud en el servicio y su administración era como cualquier otra VLAN, lo cual no era lo más apropiado ya que esta red necesitaba parámetros de red específicos tales como enrutamiento, ancho de banda y seguridad en todos los aspectos. Esta red llamada Unidad Informática de la Biodiversidad (UNIBIO),conserva y aloja bases de datos con información sensible, por lo que se aisló de la red completa de la LAN del IB, situándola con sus propio segmento de red, y con infraestructura independiente, se diseñó un esquema de seguridad a la medida de las necesidades de la Unidad, con ello se independizó y protegieron las valiosas actividades de esta Unidad. La ventaja de esto es la tolerancia a fallos, en redes mutuamente excluyentes, por lo cual esta unidad no se vera afectada en absoluto por fallas ocurridas dentro de la infraestructura de red del IB.

La duplicidad del segmento provee doble enlace, dado que el dispositivo posee la habilidad de intercambiar gateways, con prioridades preconfiguradas previamente, para el desvío de tráfico y/o balanceo de carga, esto representa un enlace parcialmente doble, dado que el enlace proveniente de la Dirección General de Tecnologías de la Información y Cómputo, proporciona dos segmentos de red en este enlace de fibra óptica. Con esta dualidad de segmento el tráfico puede cambiar de gateway en situación de contingencia. A continuación se explican los resultados obtenidos de el análisis sobre dos de los servicios más importantes que ofrece la Unidad de Cómputo hacia la comunidad del Instituto de Biología.

4.1.1. Análisis de Página WEB.

La página web tiene como objetivo ser el primer contacto que tenga el usuario en el ciber espacio con el IB, esta provee la información necesaria para dar a conocer al Instituto de Biología a nivel internacional y en ella se compila toda la información, misión, visión y los objetivos de la institución, de los servicios y los académicos que conforman la comunidad. Por ello es necesario que dicho portal este debidamente asegurado, ya que uno de los ataques informáticos más común, es hacia las páginas web de sitios conocidos, dentro de estos es común ver la modificación de la página para romper con la reputación del sitio, otro tipo de ataque se centra en la clonación del sitio para fines de phishing [1] esta técnica hace una copia fiel de la página de tal manera que se obtiene un portal falso e idéntico el cual se publica en Internet y por medio de artimañas se obtiene información de tipo confidencial.

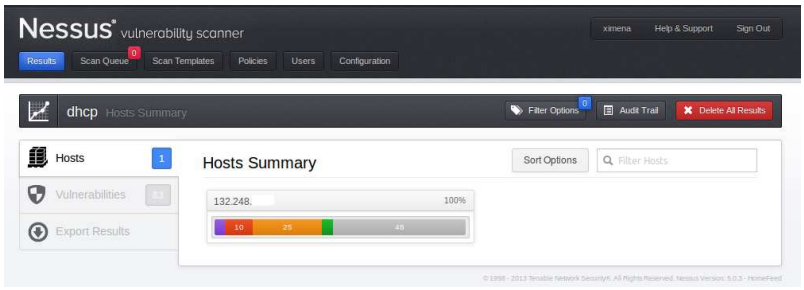


Figura 4.2: Porcentaje de vulnerabilidades de página web.

Se realizó un análisis de vulnerabilidades hacia la página web de la institución y se obtuvieron resultados con vulnerabilidades de tipo crítico hacia el servicio de *Apache* el cual soporta la página Web. Esta vulnerabilidad representa el riesgo de denegación del servicio incluso hasta atentar en contra de la integridad de la información de contenida en el portal. En la imagen siguiente se muestra el resultado del escaneo de vulnerabilidades hacia un equipo público el cual soportaba el servicio página Web y adicionalmente el DHCP *ver fig4.2.*

[1] Término informático que denomina un tipo de abuso informático y que se comete mediante el uso de engaños para adquirir información confidencial de forma fraudulenta.

En la imagen siguiente se tiene un desplegado de todas las vulnerabilidades que posee en servidor analizado, cada una posee un valor en impacto, por lo que es necesario poner suma atencion en las que son de tipo crítico y alto, dado que pueden existir muchas vulnerabilidades bajas en el servidor, pero con que haya una critica es más que suficiente para considerar que el servicio es potencialmente vulnerable. Por ello es necesario analizar cada una de las vulnerabilidades y sus características, en algunos casos la misma herramienta proporciona el detalle de lo que esta mal dentro de la configuración o instalación de la aplicación, y en la mayoría de los casos los huecos de seguridad se generan por falta de mantenimiento en software *ver fig4.3*. En el caso exclusivo del servidor que contenía la página Web y el DHCP, se consideró que no era una buena práctica, incluir en un servicio público como la página web, otro de red que debería ser exclusivo y privado. Por lo que era necesaria la segregación de servicios con respecto al perímetro de seguridad. Ya que con base en la imagen mostrada era más que evidente el riesgo con respecto a este servidor era doble por que no solo afectaba a la página web, sino también a toda la red de datos ya que si el servicio de DHCP fuese desactivado, se denegaría el Internet a toda la Institución.

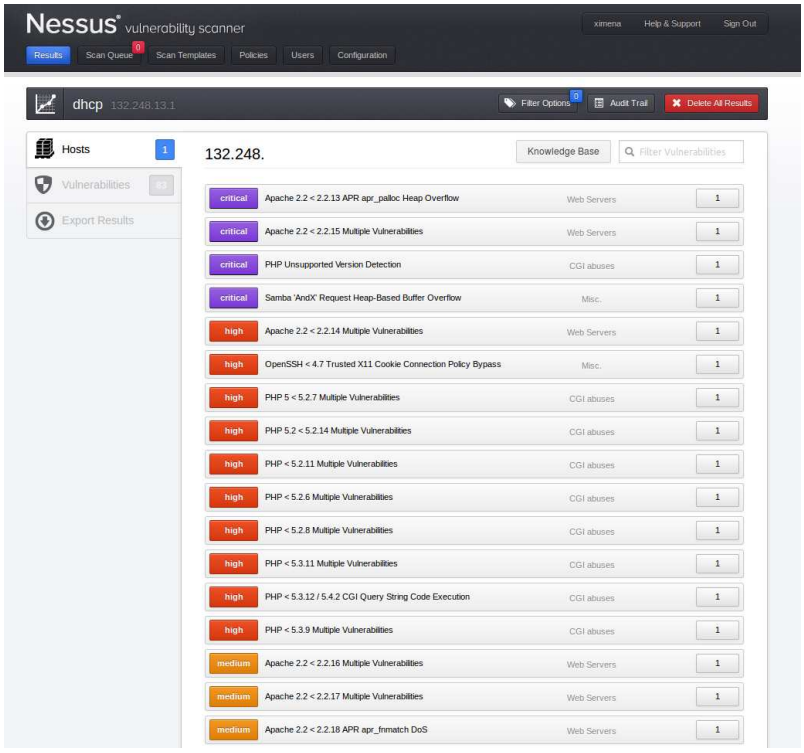


Figura 4.3: Despliegue de vulnerabilidades de pagina web

4.1.2. Análisis de Correo Electrónico.

El servicio de correo electrónico es de suma importancia por que proporciona a los usuarios de Internet la facilidad de comunicación a larga distancia, así bien se convierte en una herramienta integral auxiliar para las comunicaciones del Instituto de Biología. Por ello es imperativo que este servicio cuente con variables como la integridad y la disponibilidad 24/7. Las pruebas iniciales sobre el servicio existente arrojaron 5 vulnerabilidades con impacto crítico las cuales se deben a diversos factores de configuración y de las mismas aplicaciones que corren dentro del sistema. En la siguiente lamina se muestra la correspondencia del análisis con el servicio de correo electrónico, dicho análisis muestra las posibles vulnerabilidades del host al que se le esta aplicando el escaneo *ver fig4.4*.

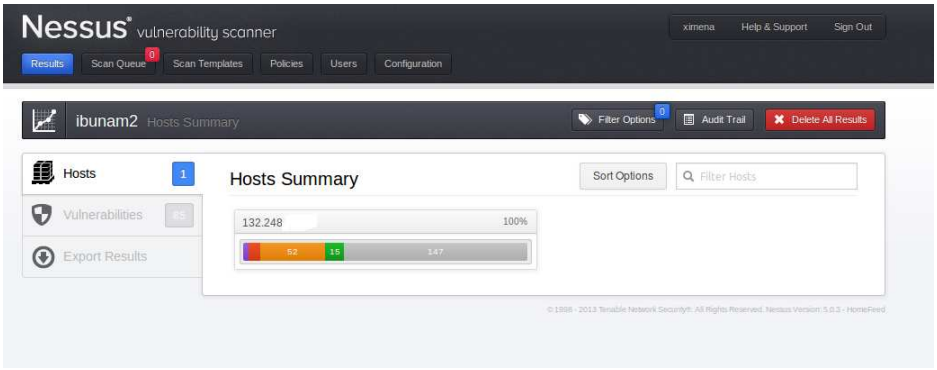


Figura 4.4: Escaneo a Correo electronico.

Una vez realizado el escaneo con la herramienta se puede visualizar el desglose de las vulnerabilidades encontradas en el sistema. Este cuenta con un código de colores que va desde el morado en estado crítico, alto en rojo, amarillo en mediano etc. Estas métricas se dan con respecto al riesgo e impacto que la vulnerabilidad puede causar sobre el servicio. En este caso el servidor que proporciona correo electrónico no posee buenos resultados. Apareciendo en sus vulnerabilidades de tipo *critical*, varios fallos de seguridad,algunos completamente explotables. Estas vulnerabilidades se refieren al riesgo que posee el servidor de ser penetrado o comprometido, es decir que algún intruso acceda al sistema *ver fig 4.5*.

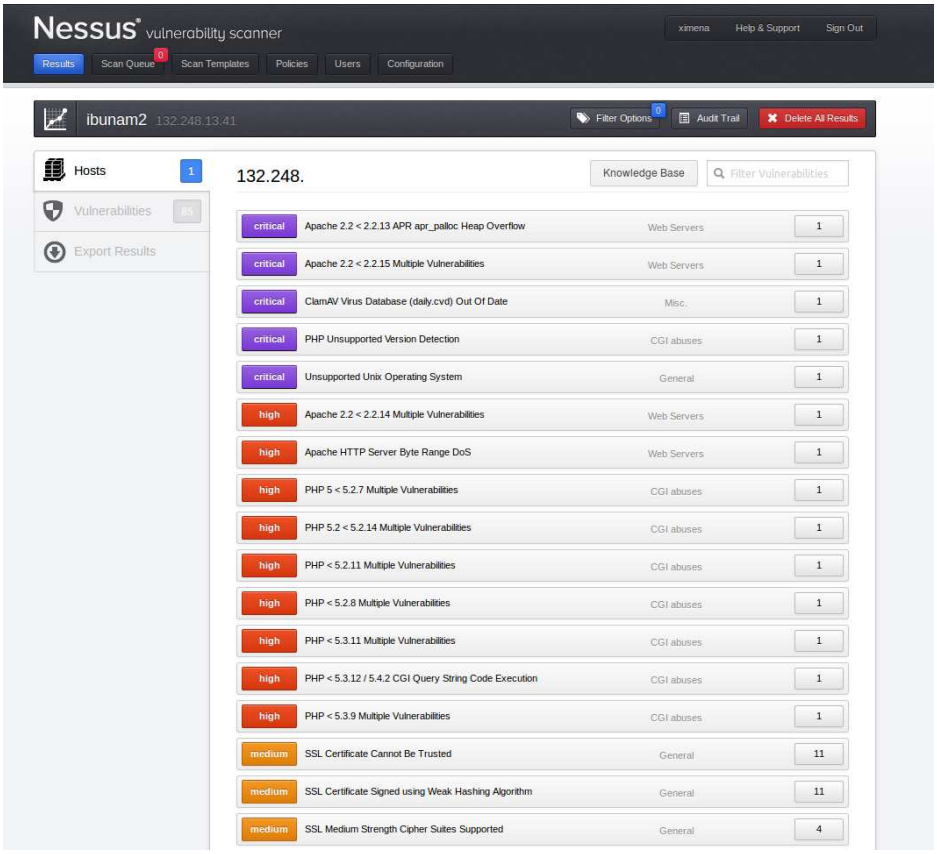


Figura 4.5: Escaneo a Correo electronico despliegue.

Sin embargo estos no son los únicos riesgos a los que esta expuesto el servicio de correo electrónico. Mediante una captura simple de tráfico se obtuvo un resultado un poco más perturbador. La prueba consistió básicamente en capturar el tráfico durante el acceso vía web al correo, el envío de un mensaje y desconexion del mismo. Dicha captura mostró la falta de seguridad en la transmisión de los datos hacia Internet. Es decir que los datos que se le proporcionan al servidor *zimbra*, para la autenticación de usuario y password viajan a través de Internet, en texto plano. Es decir que si un atacante capturara tráfico saliente del servidor tiene la posibilidad de obtener usuario y contraseña de cuentas institucionales, lo cual representa un riesgo elevado. En este escaneo se muestra de nuevo los valores que corresponden a vulnerabilidades de tipo *medium* y *low*. Por lo que se nota la ausencia de vulnerabilidades que realmente afecten al servidor o lo comprometan seriamente. En la lamina siguiente se muestra el desplegado de dichas vulnerabilidades *ver fig 4.6*

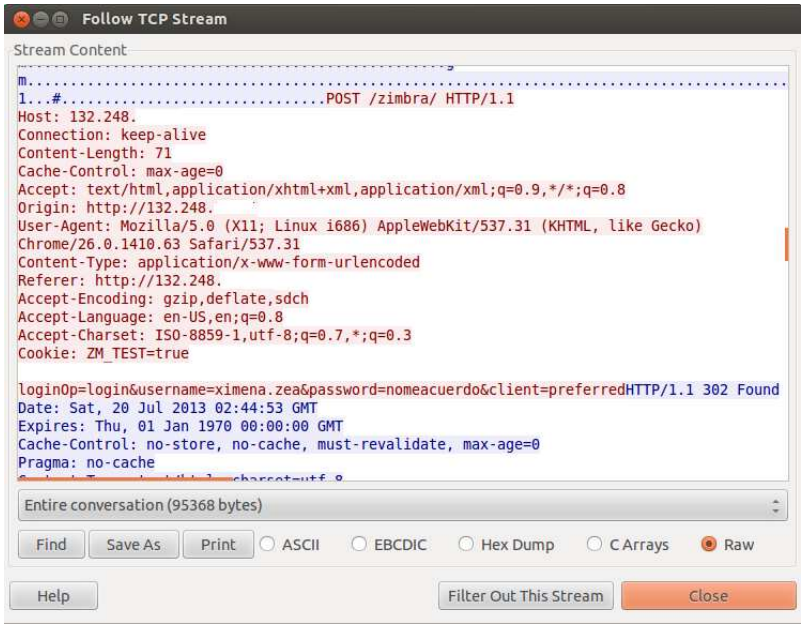


Figura 4.6: Captura de trafico de correo.

4.1.3. Optimización de esquema de seguridad.

Para mitigar los puntos de fallo y reducir los riesgos considerablemente, se generó un nuevo esquema de seguridad informática, con cambios en topología física y lógica *ver fig 4.7.*
Comenzando con la implementación de nueva tecnología de filtrado, la cual reemplaza el firewall en producción, por un arreglo de dos firewalls con capacidad superior en hardware y software, al ingresar esta dupla, se segregan servicios y se elimina un punto de fallo, dado que los servicios de seguridad, red y enrutamiento, tales como: NAT, DHCP y control de acceso se dividen en dos dispositivos para optimizar la carga y procesamiento del tráfico entrante y saliente. El set de reglas se reduce a una tercera parte, lo cual beneficia la calidad del servicio y al esquema de seguridad; se asignó ancho de banda de manera uniforme para eficientar el tiempo de respuesta de la red, y se aseguraron los servicios públicos mediante un firewall transparente con tecnología en OpenBSD, con este tipo de firewall se elimina la necesidad de realizar cambios en la configuración de los servidores, sin afectarlos y sacarlos de linea, dado que el filtro se implementa de manera simple y protege a los servidores los cuales no pertencen a la red LAN, con ello se aísla el tráfico entrante hacia ellos, evitando ataques hacia los mismos.

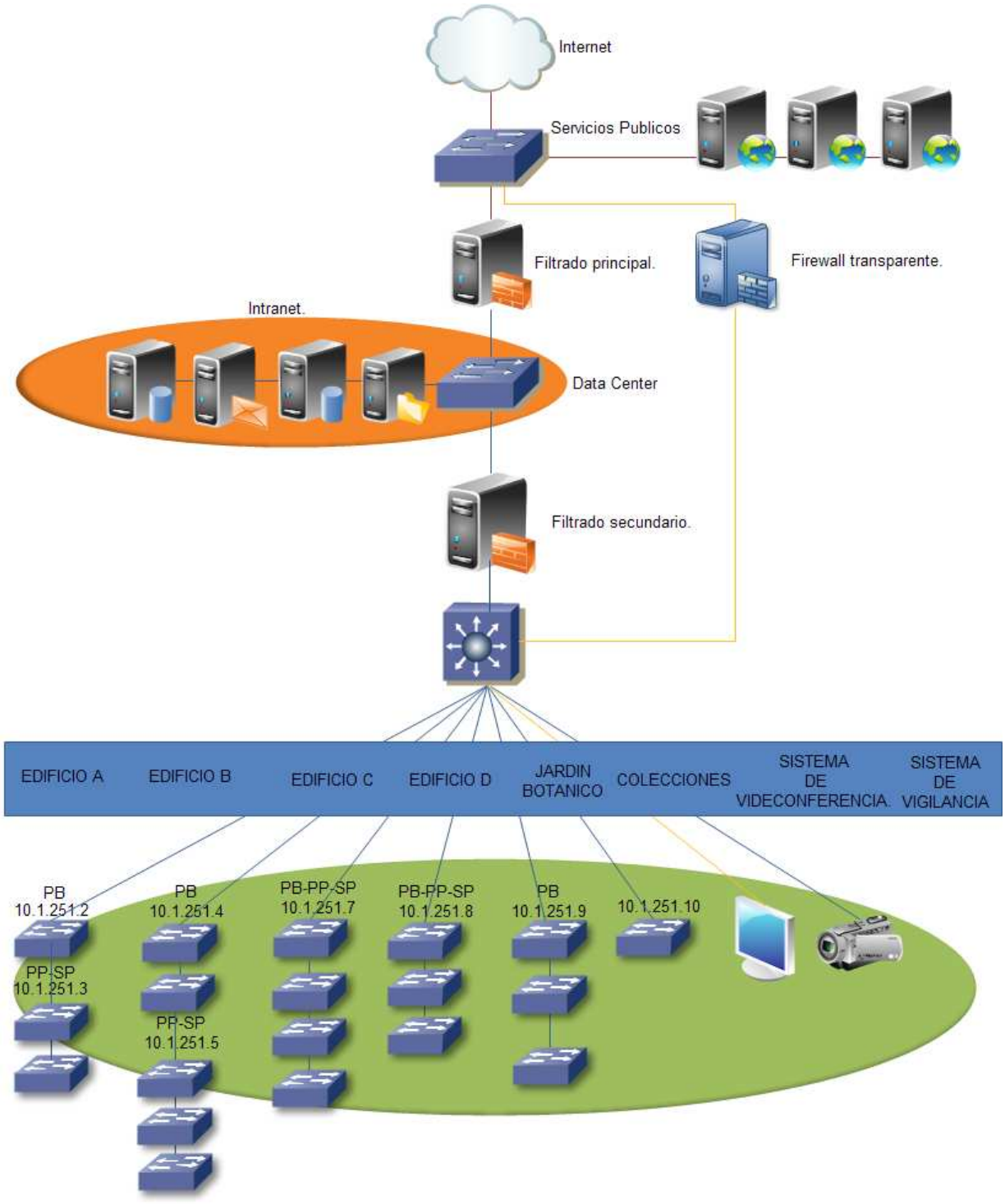


Figura 4.7: Optimización de topologico IB.

Por otra parte se optimizó la carga de tráfico en el switch de *core* de fibra óptica, liberándolo del enrutamiento inter VLAN, por lo que se hizo más liviano en procesamiento de capa dos y se aumentó su productividad y vida útil. Se genero un portal cautivo para el control de acceso inalambrico, con ello se centraliza la administración de los APs, y se genera un sistema de registro que alimenta una base de datos con usuarios permitidos para control estadístico, de investigadores, estancias, intercambios de la comunidad móvil del Instituto. Con ello se elimina la necesidad de administrar 20 dispositivos individualmente y se puede informar al usuario vía correo electrónico de sus derechos,obligaciones y políticas de uso del servicio. Para la automatización de las configuraciones de los dispositivos de telecomunicaciones,se implementa un servidor TFTP, que genere las copias con regularidad y las almacene en su interior, a fin de contar con un servidor de respaldo para todos los equipos que integran la red, servidores, routers, switch etc.

Toda esta infraestructura protege, conserva y administra el flujo de datos que se genera en la red del IB,cabe mencionar que el costo-beneficio es grande dado que la tecnología implementada no tiene costo. No es necesaria la adquisición de licencias, actualizaciones y mantenimiento. La inversión en la renovación de la seguridad del Instituto, se vio reflejada en la implementación de dos servidores robustos,el intercambio de otros servidores en producción, con los cuales se genero toda la infraestructura necesaria para la optimización. Es decir que con poco equipo y unos cambios ligeros en arquitectura y configuración, el esquema de seguridad sufrió cambios importantes y de sumo beneficio hacia los datos y la comunidad del IB. Con esto se cumple el objetivo principal de un ingeniero en redes y seguridad, se optimizan procesos y se reducen costos.

Los firewalls son empleados para separar redes con niveles de seguridad distintos, para ello es necesario comprender el diseño de red.
Los diferentes dispositivos de red que proporcionan conectividad y servicios; la arquitectura y topología de red, los cuales que proporcionara los fundamentos necesarios para diseñar un esquema de seguridad eficaz, el diseño del firewall es considerado un componente esencial para cumplir con los requisitos de acceso a la red, los procesos de diseño tienen en cuenta la seguridad y la ubicación de los puntos de acceso, de esta manera se puede aplicar la seguridad de manera apropiada.
Al implementar la seguridad en los perímetros de red, la arquitectura y las directivas que se aplican a cada dispositivo pueden tener efecto negativo tanto en el rendimiento como en la latencia.

Algunos puntos de evaluación para el diseño e implementación de un firewall son:

- *El rendimiento*: el cual es un delicado equilibrio entre suficiente seguridad, firewall y el acceso a los datos.
- *El número de capas de seguridad* que se apliquen, como listas de acceso u otras decisiones de filtrado,entre más capas más lento sera el rendimiento.

Los filtros pueden ser eficaces al evaluar el acceso mediante direcciones IP. Sin embargo, para muchos dispositivos, cuanto más largo sea el listado de reglas de acceso, más tiempo se necesitará para examinar cada paquete; el rendimiento variará en función del número de filtros que se empleen y la capa en la que sea necesario la revisión de datos y el tipo de tráfico. Para la optimización de la seguridad de la red de datos del Instituto de Biología

se realizó una reestructuración de los dispositivos de la capas núcleo y distribución, a fin de renovar el esquema de seguridad. La planeación de la implementación de la nueva tecnología de filtrado contemplo la identificación de los requerimientos institucionales el cual definirá el tipo de arquitectura y diseño del esquema de seguridad informática. Y el diseño de las Políticas de Seguridad Informática, las cuales dan vida a la implementación de esta tesis.

4.2. Implementación de filtrado de contenido con PFSENSE.

Pfsense es una distribución libre del sistema operativo FreeBSD modificada para ofrecer el servicio de firewall y router. Posee una interfaz para su administración vía web, llamada WebGUI, es una plataforma poderosa y flexible de enrutamiento y filtrado. Las razones por las que se escogió que naciera de FreeBSD fue por el soporte en drivers inalámbricos, el rendimiento de red, el soporte hacia el sistema y el desarrollo de nuevas versiones. Pfsense posee aplicaciones con propósitos específicos,tales como para servicios de VPN, DNS, Sniffers y DHCP a estos se les llama módulos, lo cuales están diseñados exclusivamente para PFsense. Posee varias funcionalidades,aparte de firewall, balancea cargas, puede ser servidor PPPoE para la autenticacion de usuarios, puede implementar enlaces redundantes por medio del protocolo CARP,realiza reportes y monitorizacion. El mecanismo de filtrado utilizado por PFsense se llama **packet filter PF** , es un filtrado de paquetes a nivel de kernel y utilidades de entorno de usuario para el control de las funcionalidades del mismo.

Figura 4.8: Logotipo Pfsense.

La implementacion se llevo a cabo en un par de servidores cuyas características técnicas principales son:

- Doble procesador Intel Xeon X5660 a 2.86 MHz.
- Memoria RAM de 48 GB.
- Discos Duros de 500 GB.
- Dos tarjetas de red Intel.

  El motivo de las tarjetas de dicha marca es para ejercer la compatibilidad de hardware con PFsense, dado que existe una lista de hardware, marcas modelos etc, los

cuales son ideales para la operación del mismo, mínimo debe poseer dos interfaces de red. En este caso se realizó la instalación con tarjetas a 10Gb, cuyo driver no existe aún en la version actual de PFsense RC2, por lo que fue necesario la compilación de los drivers y el modulo para el kernel del mismo, dado que el sistema operativo nativo es FreeBSD, se obtiene que para la version 8.1 de FreeBSD este driver aún no había sido desarrollado y por lo tanto no fue integrado. En la version 8.2 ya esta contemplado, el *release* actual de PFsense esta basado en la version 8.1 FreeBSD.

Para cualquier puesta a punto es necesario revisar el tipo de hardware a implementar y la configuración del mismo, memorias RAM, discos duros, interfaces de red etc.. de lo contrario la instalación no sera exitosa.

La suite PFsense posee múltiples paquetes disponibles dentro de una lista del mismo sistema operativo, su instalación es simple y rápida, posee herramientas de monitorización, protocolos de ruteo, paquetes de filtrado y más.

4.3. Sistema de Respaldo.

El protocolo de transferencia de archivos trivial (Trivial file Transfer Protocol) TFTP, es un protocolo simple semejante a FTP, el cual se utiliza para la transferencia de archivos pequeños a través de una red. Explicado en el RFC 783 originalmente , en su segunda revisión fue el 1350 en el año del 1992, creado por Noel Chiappa.
TFTP utiliza UDP en el puerto 69 como protocolo de transporte, no enlista el contenido, ni asegura la transferencia, es usualmente utilizado para la transferencia vía interna de información. No se tiene una definición de sesión, se realiza un intercambio informal de los paquetes, posee una arquitectura cliente-servidor, se considera servidor a aquel que abre el puerto 69 en UDP y el cliente al que se conecta.
Cualquier transferencia comienza con una petición de lectura o escritura de un archivo. Si el servidor concede la petición se abre y el archivo se envía en bloques de 512 bytes (longitud fija). Los bloques del archivo están numerados consecutivamente comenzando en 1. Un paquete de reconocimiento debe verificar cada paquete de datos antes de que próximo pueda enviar. Se asume la terminación de la transferencia cuando un paquete de datos tiene menos de 512 bytes. Casi todos los errores causaran la terminación de la conexión. Si un paquete se pierde en la red, ocurrirá un *timeout*, después de que la retransmisión del ultimo paquete haya sido ejecutada.
Existen 5 tipos de paquetes: Petición de lectura (RRQ), petición de escritura (WRQ), Datos (DATA), Reconocimiento (ACK),Error (ERROR).

Los cuales tienen 3 modos de transferencia:

- NetASCII: US-ASCII es como de define en el código estándar USA para el intercambio de información con modificaciones especificas, es decir utiliza un conjunto de caracteres de 8 bits.
- Octet: Bytes de 8 bits, también llamado binario.
- Mail: Este modo se definió originalmente en el RFC 783 y se declaro obsoleto en el RFC 1350. Este modo se india en la petición inicial de (RRQ/WRQ).

Se utiliza para leer o escribir archivos de un servidor o cliente remoto. En el caso de esta tesis el servicio de TFTP se implemento como parte de la recuperación de información sensible *verfig4.9*. El servidor con TFTP realizara la tarea de respaldo y repositorio de configuraciones de la capa *core*, distribución y acceso de la red local de datos. Este deberá estar disponible en todo momento para la copia de los archivos de configuración. El mecanismo que empleara sera una conexión simple hacia el dispositivo de red, ejecutara las instrucciones pertinentes para encontrar el archivo necesario y realizara la copia dentro de si , mismo que tendrá un mecanismo de compactacion para el almacenamiento de la información.

Figura 4.9: Servidor TFTP.

4.4. Configuración de DHCP

Como se vio en el capítulo anterior, el servicio de red de DHCP es vital para la conexión a gran escala de una red local, este servicio se implementó dentro de la red local seguido de un direccionamiento lógico de la red, el cual divide por medio de VLANs la red local, creando diferentes segmentos de red mutuamente excluyentes los cuales deberán encapsular el tráfico de manera eficiente, con esto el servidor DHCP deberá contar con diversos números de pool de direcciones Ip privadas para la asignación temporal de los host de red *ver fig4.10*.

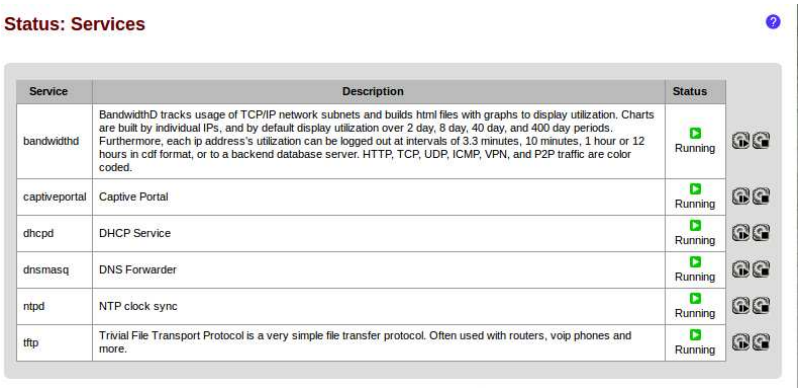


Figura 4.10: Servicio DHCP activo.

El direccionamiento de red comienza con un segmento privado clase A con máscara de 16 bits, cuyos últimos octetos contienen la capacidad de expansión a futuro. Se contemplaron las VLANs,por piso en edificio, así como por tipo de servicio. Es decir que cada piso de los edificios centrales del Instituto se encuentra en diferente VLAN por lo que la administración de las vlans debe ser centralizada, *ver fig4.11.* así mismo para la configuración del servidor DHCP, se configuraron subinterfaces sobre la tarjeta física LAN y dentro de cada subinterfaz se configuró un rango de Ips privadas para cada VLAN.

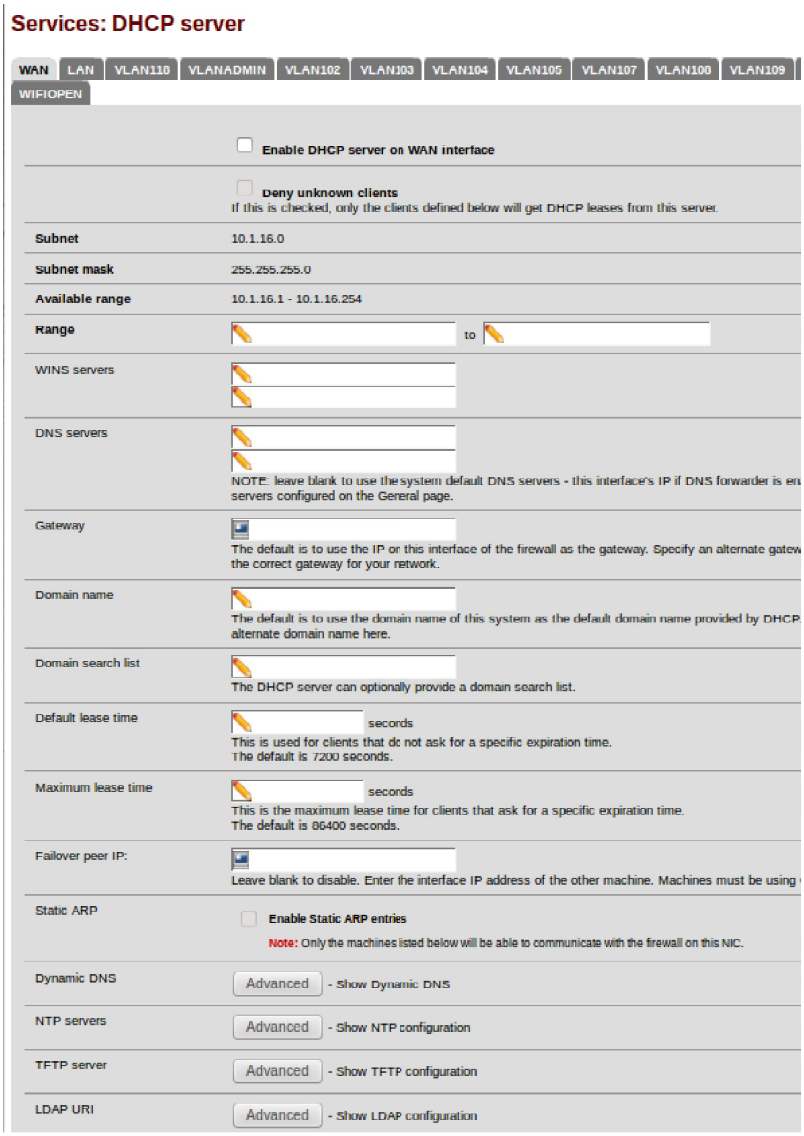


Figura 4.11: Configuración de interfaz DHCP.

Dentro de la administración del DHCP , en cada pool se reservaron diferentes rangos dentro de los segmentos de las VLANs para satisfacer la demanda y el crecimiento a futuro del servicio de internet. Así mismo como un segmento exclusivo para servicios con necesidades de dirección Ip fija, tales como equipos dedicados de cómputo, servicios de intranet, impresoras etc.

4.5. Enrutamiento InterVLAN

El enrutamiento entre VLANS o Inter VLAN routing resulta necesario una vez que se posee una infraestructura con VLANS implementadas, debido a que los usuarios necesitan intercambiar información de una red a otra. Por ello se genera esa necesidad de implementar este enrutamiento entre redes virtuales, cada una de estas redes son dominios de broadcast únicos *ver fig4.12*. Se define enrutamiento como un proceso para reenviar el tráfico de una red desde una VLAN a otra mediante un *router*,como las estan asociadas a subredes únicas, la configuración de estas en un *router* facilita el entorno te las VLANS. Tradicionalmente el enrutamiento de la LAN utiliza routers con interfaces físicas múltiples. Es necesario conectar cada interfaz a una red separada y configurarla en una subred diferente.

En una red tradicional con múltiples VLANS que segmentan el tráfico se realiza la conexión de diferentes interfaces físicas del *router* a diferentes puertos de un switch. Para la optimización de hardware, existe un tipo de configuración alternativa llamada *stub router, o one-armed router*, en donde la interfaz del *router* se configura para funcionar como enlace troncal y esta conectada a un puerto del switch también en modo troncal. El *router* acepta el tráfico etiquetado mediante subinterfaces, para después reenviar dicho tráfico hacia la VLAN destino. Las subinterfaces son interfaces virtuales múltiples,asociadas a una interfaz física, estas interfaces están configuradas en software en un *router* configurado en forma independiente con una dirección IP y un ID de VLAN.

Las interfaces físicas están configuradas para tener una interfaz por VLAN en la red. En las redes con muchas VLAN, no es posible utilizar un único *router* para realizar el enrutamiento. Los routers tienen limitaciones físicas para evitar que contengan una gran cantidad de interfaces físicas. En cambio si es prioridad este método se puede optar por múltiples routers.

Debido a que no existe contención para ancho de banda para las interfaces físicas existe un mejor rendimiento cuando se compara con el uso de las subinterfaces. El tráfico de cada VLAN conectada tiene acceso al ancho de banda completo de la interfaz física del *router*. A diferencia de las subinterfaces el tráfico enrutado compite por ancho de banda en la interfaz fisica única. En una red ocupada,esto puede causar un cuello de botella en la comunicación.Con respecto a la parte financiera, resulta más económico utilizar subinterfaces.Cuando se tienen redes diferentes estas no pueden comunicarse entre si dado que es el principal motivo de las redes virtuales,es el encapsulamiento de tráfico por medio de un mecanismo lógico de etiquetado en las tramas de red. Por lo tanto en este esquema es necesario utilizar un dispositivo que realice la división y enrutado de las VLANS. PFsense posee la capacidad de rutear InterVLAN de tal modo que por medio de subinterfaces se generaron los gateways independientes para cada VLAN de esta manera por medio de una sola interfaz de red se acepta y enruta el tráfico etiquetado hacia el destino correcto. Las ventajas de emplear este tipo de configuración se encuentra directamente relacionado con el costo, rendimiento y complejidad de la implementación. Dado que en esta topologia se emplea una sola interfaz de red, se aminora el costo de la interconexion física y se optimiza el rendimiento del equipo y la velocidad de transferencia de datos con una configuración un tanto compleja y eficiente.

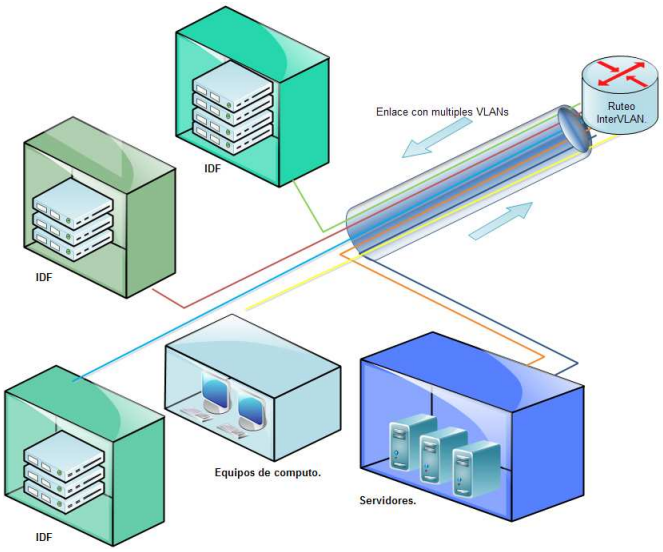


Figura 4.12: Ruteo InterVLAN.

4.6. Portal Cautivo para usuarios móviles.

Un portal cautivo o captivo es un programa en red que vigila en tráfico entrante y saliente hacia Internet.Uno de los objetivos es forzar el paso de tráfico a través del mismo,es decir una página especial para obtener el acceso a Internet de forma normal. El portal intercepta todo el tráfico HTTP hasta que el usuario cumple con requisitos de autenticidad *ver fig4.13*,así mismo el portal tiene la capacidad de controlar el ancho de banda de la conexión activa por cada cliente. Proporcionando a su vez calidad de servicio. Se usan sobre todo en redes inalambricas abiertas,donde interesa mostrar un mensaje de bienvenida a los usuarios y para informar las condiciones de acceso al medio. La razón de un portal cautivo es para concientizacion del usuario sobre las acciones en red y así entonces llevar una administración más eficiente sobre el uso del recurso informático. Su implementación puede ser por software o hardware. En este caso particular de tesis, el portal cautivo se utilizo para conceder el acceso inalambrico a la comunidad de la Instituto de Biología por medio de un portal el cual pudiera agilizar el registro y acceso del usuario móvil para la red inalambrica. Dicho portal obtiene por medio del usuario, datos generales sobre el mismo, para fines estadísticos y de control de conexión *ver fig4.14*. De no ser proporcionados los datos en el registro el administrador de red no podrá dar de alta el usuario en cuestión. Y este no podrá navegar en Internet, o no podrá ejecutar cierto tipo de conexiones dependiendo del perfil en que se encuentre, dicho perfil cuenta con distintas políticas de seguridad.

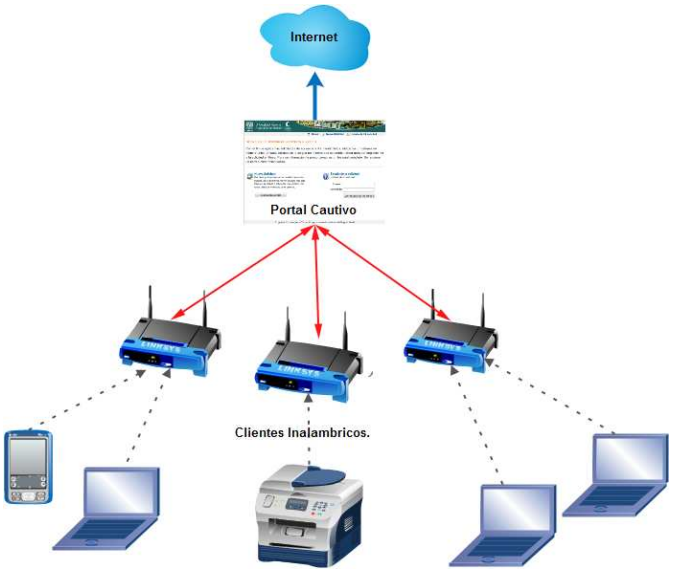


Figura 4.13: Operación de un Portal Cautivo.

Para la centralización de las antenas de servicio inalambrico se utilizo este mismo portal, es decir, inicialmente existe una VLAN exclusiva para red inalambrica, pero la administración era individual en cada Access Point, lo cual era sumamente complejo a nivel de administración y no ofrecía QoS.
Así bien conjuntando el sistema del portal cautivo con la infraestructura de red inalambrica, se crea un servicio único aúnque el usuario cambie de antena a la que se conecta. De allí en nombre de *usuario móvil.*
Con esta implementación se redujo el tiempo de registro por medio de la automatización del proceso de acceso inalambrico, y se obtuvo la centralización del servicio para ofrecerle al usuario red inalambrica en cada punto de las instalaciones.

Figura 4.14: Visualización de Portal Cautivo.

4.7. Firewall y control de acceso.

Como ya fue previamente mencionado en el capítulo 3 los objetivos de un firewall son: restringir, separar y analizar. Para esta tesis en particular el método de filtrado se basó sobre la plataforma PFsense la cual por medio del motor de filtrado *pf*, el cual ejercerá el filtrado principal a nivel de protocolo y puerto de conexión. Con esto el tráfico se vuelve más eficiente y ágil, dado que a medida de que fluye por los medios de comunicación este se va depurando por medio de dispositivos de esta índole.

Para esta tesis el principal instrumento de filtrado y control de acceso es el firewall. Cuyo dispositivo montado sobre la plataforma Pfsense tiene como objetivo el filtro principal de todo el tráfico entrante y saliente de la red de datos del IB el cual debe llegar al usuario final de una manera eficiente y pura. El firewall que realiza filtrado en capa 3 lo realiza por: interfaz, protocolo, source IP, destination IP, source OS, estado de la conexión, gateway, si es entrante o saliente y por bandera. Se pueden configurar reglas especificas para cada propósito diferente, en este caso el filtrado principal esta basado en las buenas practicas ejerciendo una depuración básica para aminorar la carga de procesamiento del equipo de cómputo en cuestión. Packet filter basado en *stateful* escrito originalmente por Daniel Hartmeier actualmente desarrollado y mantenido por OpenBSD. Fue publicado a finales de 2001 en la version 3.0 de Open, como reemplazo de IPFilter ambas sintaxis son parecidas, PF incluye características de Alta Disponibilidad como *pfsync* y un protocolo de redundancia para direcciones comunes CARP, identificador de sesion *authpf*, proxy ftp etc. Este se conforma por listas, macros, tablas, NAT, Forward de puertos, aliases etc *ver fig4.15* PF se desarrolla como parte del sistema base de OpenBSD, pese a ello, ha sido portado con gran éxito en otros sistemas. FreeBSD lo fue adoptando paulatinamente, primero como paquete y desde la version 5.3 como una de los tres subsistemas de filtrado que ofrece el núcleo. Así es como nace PFsense quien porta una interfaz gráfica de edición muy amigable para el administrador y facilita la configuración del dispositivo haciendo más eficaz y legible.

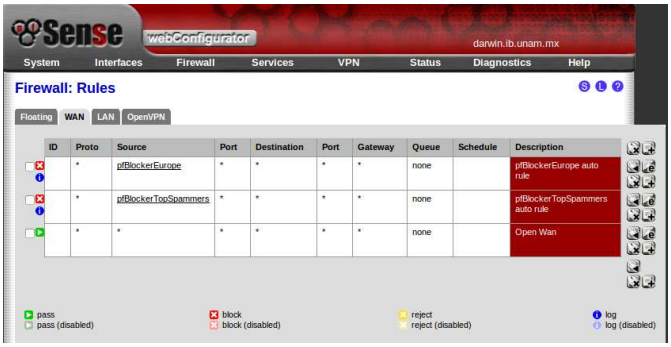


Figura 4.15: Visualización de interfaz de reglas del Firewall.

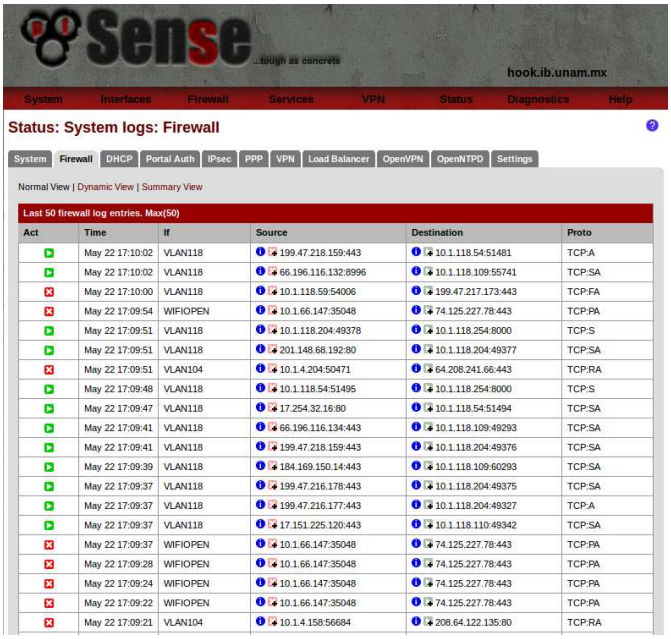


Figura 4.16: Visualización de la bitacora de Firewall.

4.8. NAT

Como se vio en le capítulo 3 el NAT es esencial para proveer servicio de Internet en una LAN, esta acción es realizada por el dispositivo PFsense. Dicho dispositivo realizara esa acción con el fin de aprovechar al máximo el segmento publico asignado.

Dentro de las capacidades del equipo para Natear están:

- *Port Forward.*
  Esta opción de NAT tiene la capacidad de realizar la correspondencia de dos puertos entre dos IPs diferentes para el reenvío de información por el *socket* [2] correcto por lo que el acceso hacia el dispositivo se hace más eficaz y de manera protegida, con ello no es necesaria la interacción directa con el servidor dado que existe un intermediario el cual gestiona los accesos *ver fig4.17.*

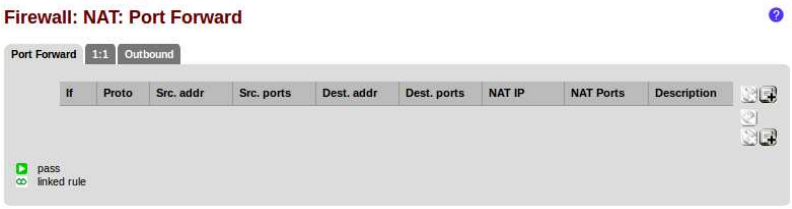


Figura 4.17: Visualización de Interfaz de configuración NAT con port forward.

[2]Un socket queda definido por un par de direcciones IP local y remota, un protocolo de transporte y un par de números de puerto local y remoto

- *NAT 1:1*
  También llamado NAT uno a uno, es la configuración de la traducción de dos IPs pública y privada, pero dicha correspondencia se hace con todos los puertos existentes en el server interno. Así mismo el dispositivo ubicado dentro de la zona protegida tiene la opción de abrir o cerrar los puertos necesarios a través del firewall *ver fig4.18*.

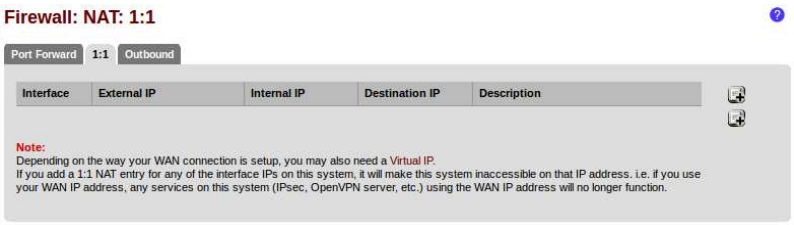


Figura 4.18: Visualización de configuración de NAT 1 a 1.

- *NAT Outbound.*
  El NAT saliente es un set de reglas que realizan la traducción de diferentes ips privadas hacia Internet con una dirección IP pública. Esta variedad de configuraciones permiten al administrador realizar cambios sobre el tráfico entrante y saliente con características particulares para su envió. Es posible realizar traducciones con diferentes IPs públicas en la interfaz WAN *ver fig4.19*, igualmente como por medio de sub-interfaces es posible la división de tráfico, en el caso de tráfico via WAN es posible por medio de IPs virtuales obtener diferentes direcciones activas sobre una sola interfaz de red. Con ello se agiliza la administración y gestión de un pool de IPs públicas con mejor desempeño y seguridad.

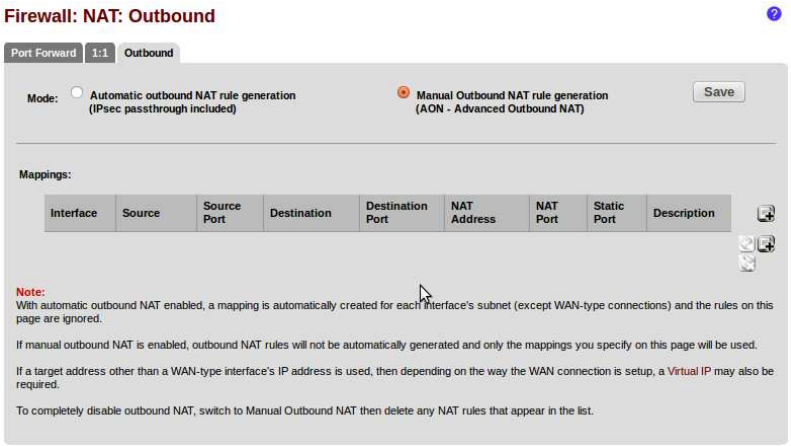


Figura 4.19: Visualización de NAT saliente.

4.9. Definición de DMZ y Data Center.

Derivado de la definición en el capítulo 3, la red que se encuentra entre la red protegida e Internet, es para fines de esta tesis y la arquitectura de red y seguridad propuesta para la implementación de un esquema de seguridad es, entre ambos firewalls. El objetivo del diseño es definir zonas especiales entre el tráfico LAN es decir tráfico exclusivo de , y el tráfico hacia Internet, de esta manera el tráfico que deba salir al exterior forzosamente deberá atravesar los dispositivos de seguridad implementados en las capas superiores de la misma *ver fig4.20*.

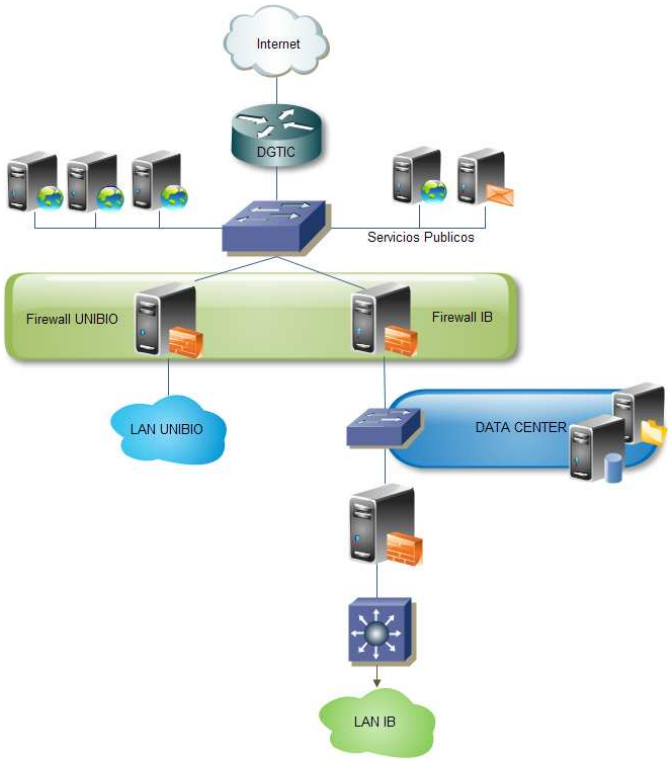


Figura 4.20: Ubicación de zona desmilitarizada y Data Center.

Como se describe en el diagrama anterior la arquitectura de red y seguridad propone la implementación de dos firewalls con capacidades de enrutamiento para la administración tráfico generado por la LAN del IB. De esta manera la ubicación del Data Center sera en medio de los dispositivos y la DMZ por encima de los filtros. Cabe mencionar que la ubicación de los mismos depende de varios factores tales como: propósito especifico del equipo, tipos de servicio, necesidades de red, características físicas y lógicas del equipo, entre otras.

4.10. Sistema de Filtrado

El mecanismo de seguridad lógico como el filtrado de contenido se propone bajo un esquema constituido por dos mecanismos de control de acceso. *Dansguardian* es un servicio que ejerce el filtrado de contenido y control de acceso, y en conjunto con Squid este ofrece el servicio de proxy cache *ver fig4.21*. La manera en la que funciona esta mancuerna se hace de la siguiente manera: primero el cliente solicita acceso a una página web, posterioremente *Dansguardian* filtra la página web, verificando si dicha página web solicitada esta permitida,dentro de las tablas de acceso previamente configuradas por el administrador del servicio, verificando de manera descendente si en esa página no hay palabras que no están permitidas,etc.

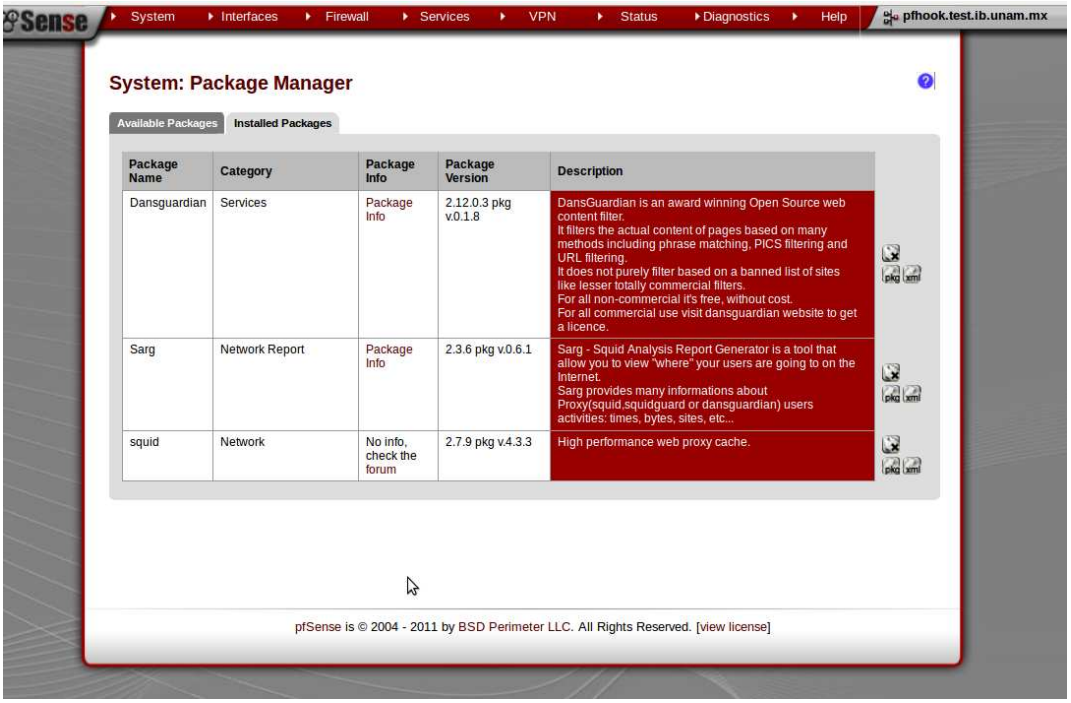


Figura 4.21: Instalacion de Paquetes.

El termino proxy tiene un significado muy general, así que el sinónimo del mismo sera intermediario para fines didácticos de esta tesis. Entre las utilidades de *Squid* esta el mejorar el rendimiento de las conexiones hacia internet, guardando en cache las peticiones recurrentes a los servidores WEB y DNS, por lo que se acelera el proceso de acceso a internet. Como se muestra en la lamina siguiente, el Proxy se configura fácilmente vía webGUI *ver fig4.22* para fines de esta tesis se opto por un modelo de proxy transparente el cual no afecte ningún tipo de configuración en el equipo de cómputo del usuario final. Este tipo de configuraciones son exitosas en redes LAN extensas en las que los cambios aplicados no deban ser detectados por el usuario, con ello también se obtiene un servicio limpio y transparente. Para el Instituto de Biología en cuyo caso representa una red en potencial crecimiento constante, el servicio de Internet es una demanda que debe satisfacer las necesidades de la institución, el proxy transparente permite al administrador proporcionar

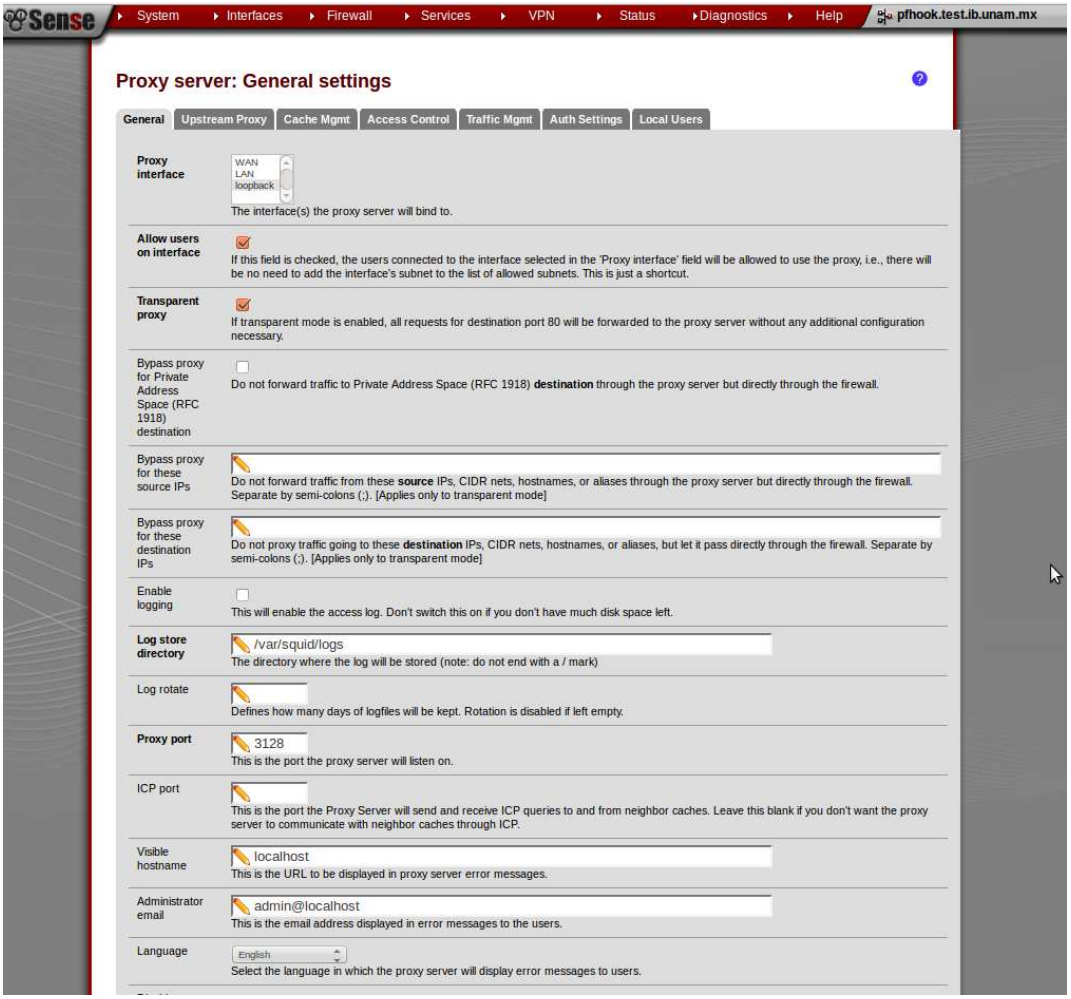


Figura 4.22: Configuración Proxy server.

un servicio centralizado y seguro. De los parámetros generales sobre la configuración existe la interfaz en la que se ejecutara la aplicación, el modo del proxy, las rutas de las bitácoras del mismo, puerto del servicio y datos de administración.

Dansguardian es un software para filtrado de contenido, diseñado para controlar el acceso a sitios web que incluye también un filtro antivirus, es principalmente utilizado en instituciones de educación, gobierno y sector empresarial. Es un software que se caracteriza por su alto grado de flexibilidad y adaptación durante la implementación. Este filtro se ubica entre el cliente web y el proxy, por medio del puerto 8080 y se conecta hacia el proxy por el 3128, el código fuente abierto garantiza la máxima flexibilidad de configuración, con lo cual se vuelve altamente versátil. En la siguiente lamina se observa la configuración inicial sobre la aplicación, tales como: Términos y condiciones de uso, interfaz y puerto, número máximo de conexiones y los datos indispensables del servidor proxy al cual deberá conectarse *ver fig4.23*.

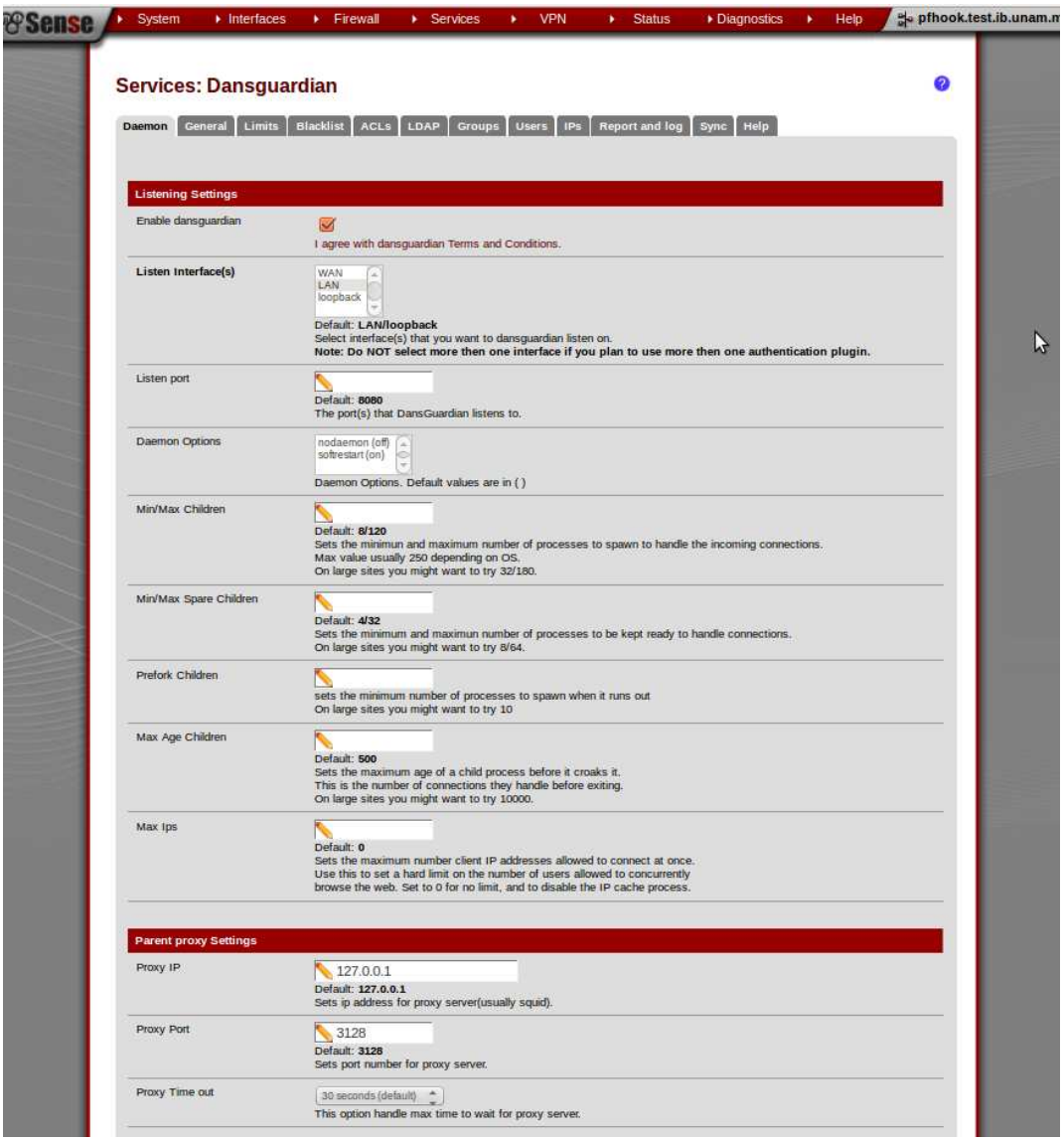


Figura 4.23: Configuración de Dansduardian.

Una vez configurados los dos servicios con los parámetros correctos se puede visualizar el estado de los mismos a través del *dashboard* de PFsense, el cual da oportunidad de reiniciar o detener alguno de ellos. En este caso ambos procesos deben aparecer en status como *running ver fig4.24*. De lo contrario deberán localizarse las bitácoras de ambos o del sistema para la detección de un posible fallo durante la configuración de los servicios.

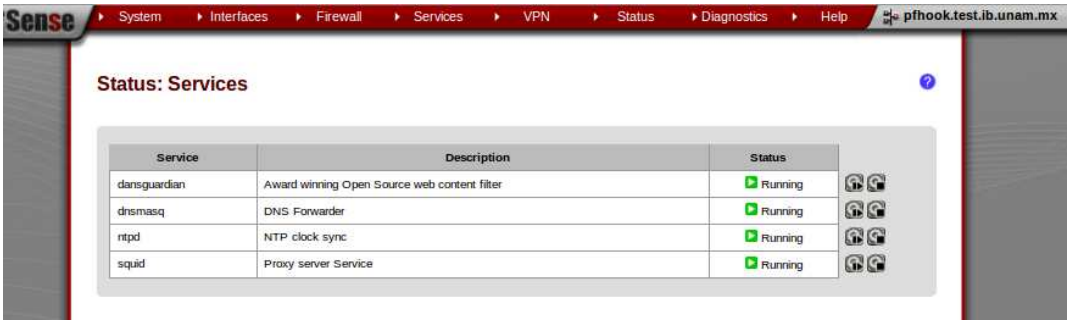


Figura 4.24: Verificación de servicios activos.

Dansguardian posee un *template* completamente configurable *ver fig4.25* a las necesidades del administrador, para fines prácticos de esta tesis, se utilizó el template original que instala Dansguardian por default. El contenido se controla por medio de urls, sitios completos, palabras,extension etc.

Figura 4.25: Portal de control de acceso Dansguardian.

4.11. Optimización de IDS

Un Sistema de Prevención de Intrusos es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas informáticos de ataques y abusos. La tecnología de prevención de intrusos es considerada como una extension de los Sistemas de Detección de Intrusos, sin embargo es algo más parecido a la tecnología de contención de tipo firewall. Los IPS fueron inventados de forma independiente por Jed Haile y Vern Paxon para resolver ambigüedades en la monitorización pasiva de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre los firewalls, dada su capacidad de contención de tráfico. La detección de tráfico malicioso se basa por varios métodos: Firmas, políticas, anomalías.
Las firmas reconocen una determinada cadena de bytes con cierto contexto y por lo tanto se generan alertas. Las políticas requieren la definición de los perfiles permitidos. Las anomalías difícilmente pueden determinar y medir condiciones normales. Sin embargo, debido a que con este enfoque los análisis no son dinámico y en tiempo real del uso de la red, por lo que suelen presentarse falsos positivos.

Snort es un sniffer de paquete y un detector de intrusos basado en red. Es un software muy flexible que ofrece capacidades de almacenamiento en bitácoras y BD. Implementa un motor de detección de ataques y barrido de puertos que permite registrar,alertar y responder ante cualquier anomalía previamente definida. Disponible de manera gratuita bajo las plataformas Windows y UNIX/Linux. El cual contiene filtros o patrones ya predefinidos, así como con las actualizaciones constantes de las bases de datos, la cual es una de las principales características de Snort dicha base de datos de ataques se actualiza y añade información en linea, la cual es compartida hacia los demás usuarios de Snort, esta ética de comunidad ha convertido a este IDS basado en red en uno de los más populares, actualizado y robusto.

Por medio de la Dirección General de Tecnologías de la Información y Comunicación a través de la Subdirección de seguridad de la Información, el Instituto de Biología es parte del Plan de Sensores de tráfico Malicioso (PSTM), cuyo programa de investigación brinda acceso a los recursos de información del plan de sensores, cuyas bases de datos se comparten entre los participantes, el objetivo del Plan de sensores es forman una red mediante estos mismos y generar una base de datos con datos estadísticos sobre el comportamiento del tráfico en internet de la red UNAM. El proyecto Honeynet *ver fig4.26* es un grupo compuesto por varios expertos en seguridad quienes llevan a cabo investigación y desarrollo abierta, disciplinaria y multiplataforma dentro de tan variante y complejo panorama de las amenazas existentes en internet.

Este sensor es de mucha ayuda a la infraestructura de red y seguridad durante en análisis de incidentes de seguridad que deban de corroborarse *ver fig4.27*, para la medición del impacto en el análisis de riesgo o simplemente como media higiénica sobre el tipo de datos salientes o entrantes de la LAN.

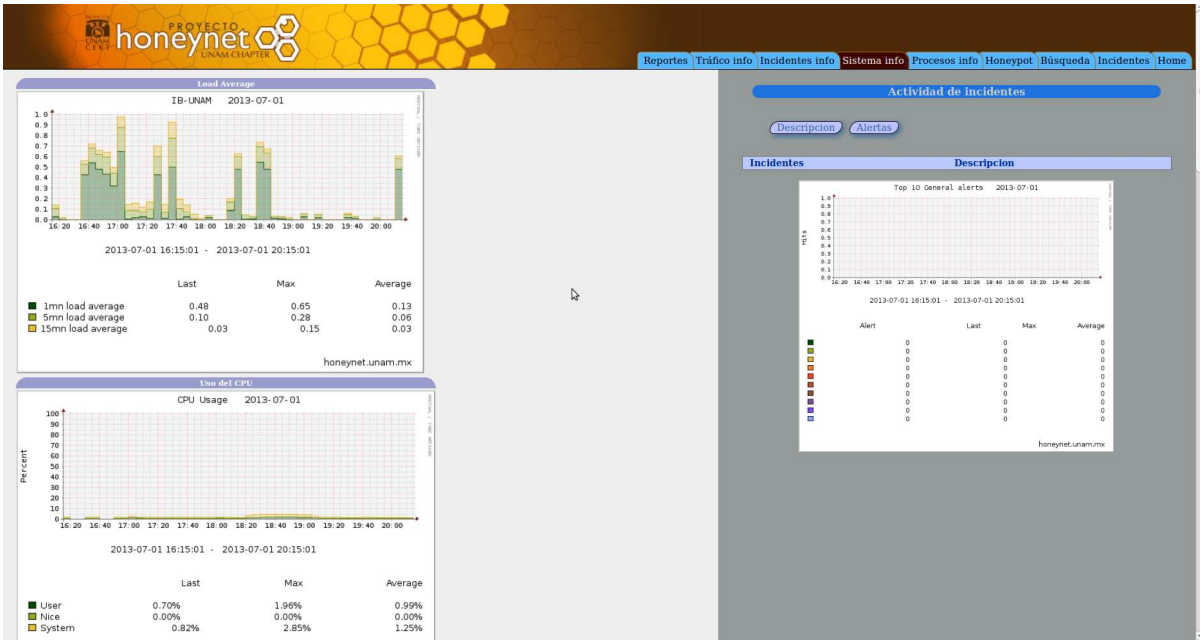
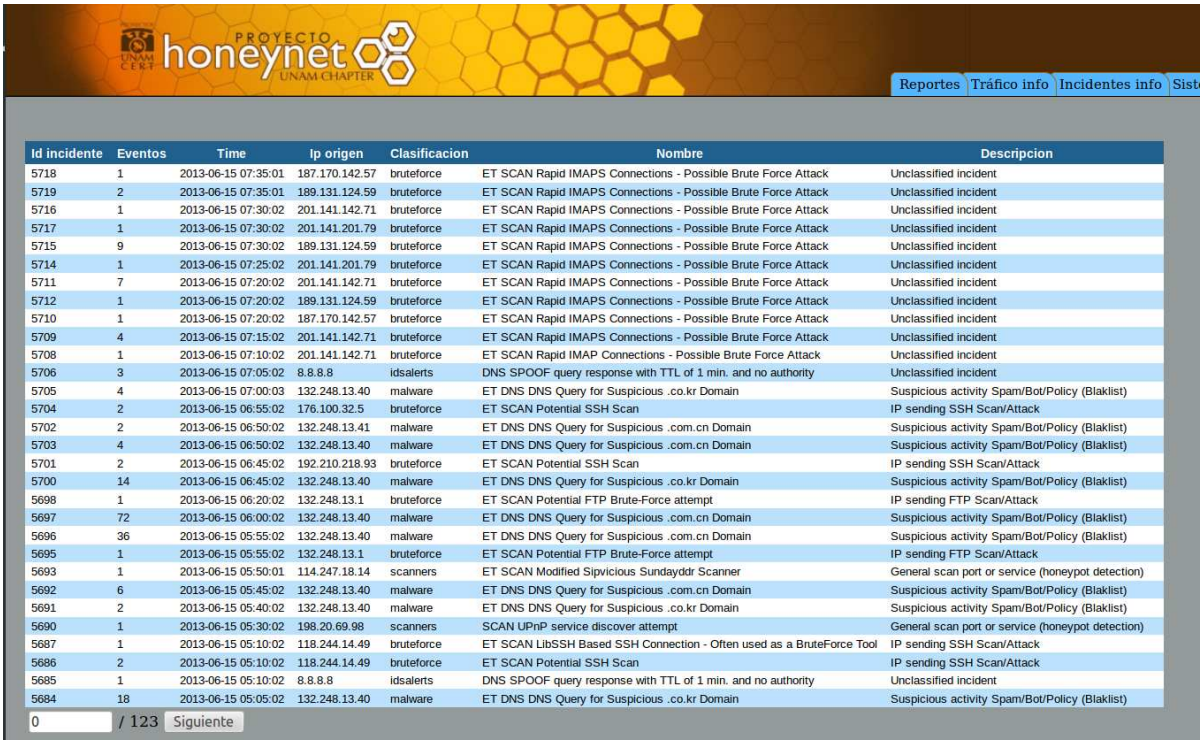


Figura 4.26: Pagina inicial de Sensor Honeynet UNAM.



Id incidente	Eventos	Time	Ip origen	Clasificacion	Nombre	Descripcion
5718	1	2013-06-15 07:35:01	187.170.142.57	bruteforce	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	Unclassified incident
5719	2	2013-06-15 07:35:01	189.131.124.59	bruteforce	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	Unclassified incident
5716	1	2013-06-15 07:30:02	201.141.142.71	bruteforce	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	Unclassified incident
5717	1	2013-06-15 07:30:02	201.141.201.79	bruteforce	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	Unclassified incident
5715	9	2013-06-15 07:30:02	189.131.124.59	bruteforce	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	Unclassified incident
5714	1	2013-06-15 07:25:02	201.141.201.79	bruteforce	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	Unclassified incident
5711	7	2013-06-15 07:20:02	201.141.142.71	bruteforce	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	Unclassified incident
5712	1	2013-06-15 07:20:02	189.131.124.59	bruteforce	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	Unclassified incident
5710	1	2013-06-15 07:20:02	187.170.142.57	bruteforce	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	Unclassified incident
5709	4	2013-06-15 07:15:02	201.141.142.71	bruteforce	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	Unclassified incident
5708	1	2013-06-15 07:10:02	201.141.142.71	bruteforce	ET SCAN Rapid IMAP Connections - Possible Brute Force Attack	Unclassified incident
5706	3	2013-06-15 07:05:02	8.8.8.8	idsalerts	DNS SPOOF query response with TTL of 1 min. and no authority	Unclassified incident
5705	4	2013-06-15 07:00:03	132.248.13.40	malware	ET DNS DNS Query for Suspicious .co.kr Domain	Suspicious activity Spam/Bot/Policy (Blaklist)
5704	2	2013-06-15 06:55:02	176.100.32.5	bruteforce	ET SCAN Potential SSH Scan	IP sending SSH Scan/Attack
5702	2	2013-06-15 06:50:02	132.248.13.41	malware	ET DNS DNS Query for Suspicious .com.cn Domain	Suspicious activity Spam/Bot/Policy (Blaklist)
5703	4	2013-06-15 06:50:02	132.248.13.40	malware	ET DNS DNS Query for Suspicious .com.cn Domain	Suspicious activity Spam/Bot/Policy (Blaklist)
5701	2	2013-06-15 06:45:02	192.210.218.93	bruteforce	ET SCAN Potential SSH Scan	IP sending SSH Scan/Attack
5700	14	2013-06-15 06:45:02	132.248.13.40	malware	ET DNS DNS Query for Suspicious .co.kr Domain	Suspicious activity Spam/Bot/Policy (Blaklist)
5698	1	2013-06-15 06:20:02	132.248.13.1	bruteforce	ET SCAN Potential FTP Brute-Force attempt	IP sending FTP Scan/Attack
5697	72	2013-06-15 06:00:02	132.248.13.40	malware	ET DNS DNS Query for Suspicious .com.cn Domain	Suspicious activity Spam/Bot/Policy (Blaklist)
5696	36	2013-06-15 05:55:02	132.248.13.40	malware	ET DNS DNS Query for Suspicious .com.cn Domain	Suspicious activity Spam/Bot/Policy (Blaklist)
5695	1	2013-06-15 05:55:02	132.248.13.1	bruteforce	ET SCAN Potential FTP Brute-Force attempt	IP sending FTP Scan/Attack
5693	1	2013-06-15 05:50:01	114.247.18.14	scanners	ET SCAN Modified Sipvicious Sundayddr Scanner	General scan port or service (honeypot detection)
5692	6	2013-06-15 05:45:02	132.248.13.40	malware	ET DNS DNS Query for Suspicious .com.cn Domain	Suspicious activity Spam/Bot/Policy (Blaklist)
5691	2	2013-06-15 05:40:02	132.248.13.40	malware	ET DNS DNS Query for Suspicious .co.kr Domain	Suspicious activity Spam/Bot/Policy (Blaklist)
5690	1	2013-06-15 05:30:02	198.20.69.98	scanners	SCAN UPnP service discover attempt	General scan port or service (honeypot detection)
5687	1	2013-06-15 05:10:02	118.244.14.49	bruteforce	ET SCAN LibSSH Based SSH Connection - Often used as a BruteForce Tool	IP sending SSH Scan/Attack
5686	2	2013-06-15 05:10:02	118.244.14.49	bruteforce	ET SCAN Potential SSH Scan	IP sending SSH Scan/Attack
5685	1	2013-06-15 05:10:02	8.8.8.8	idsalerts	DNS SPOOF query response with TTL of 1 min. and no authority	Unclassified incident
5684	18	2013-06-15 05:05:02	132.248.13.40	malware	ET DNS DNS Query for Suspicious .co.kr Domain	Suspicious activity Spam/Bot/Policy (Blaklist)

Figura 4.27: Pagina de reporte de incidentes.

4.12. Reintegración de la red de datos de la Unidad de Informática para la Biodiversidad (UNIBIO).

La Unidad de Información para la Biodiversidad del Instituto de Biología es la responsable de sistematización y publicación vía Internet la sobre biodiversidad que se encuentra custodiada en las distintas colecciones biológicas del IB. Dicha unidad es custodia y generadora de una gran cantidad de información sensible. Por ello sus sistemas, páginas web, bases de datos etc, deben y necesitan estar protegidas por un dispositivo con tal propósito. Por lo que la implementación de dicho dispositivo fue objeto también objeto de esta tesis. Para la optimización del esquema de red del IB, fue necesario realizar un análisis sobre la red LAN de UNIBIO, así como las necesidades y características propias de los servicios que presta e infraestructura de red. Por lo tanto el diseño de red y la ubicación de la LAN dentro de la infraestructura actual del IB se planteo de la siguiente manera.

Para el aislamiento de la LAN UNIBIO, se diseño un esquema de red y seguridad clásico, con firewall bajo PFsense con servicios básicos de red y seguridad *ver fig4.28*. Dicho PFsense hará las tareas de filtrado de contenido,NAT y DHCP para toda la LAN y *Data Center* [3]. Cuyo data center alberga las bases de datos nacionales con numerosos registros. La ventaja de esta arquitectura mutuamente excluyente es que ambas redes poseen infraestructura de red y seguridad independiente una de otra. Por lo que ambos dispositivos de seguridad son independientes, lo cual le da a ambas redes una estabilidad en conexión y ancho de banda. Separando los data center en ambas redes se generan zonas de seguridad aisladas para un mejor desempeño y conectividad. El direccionamiento lógico no se modificó, solo el acceso a Internet.

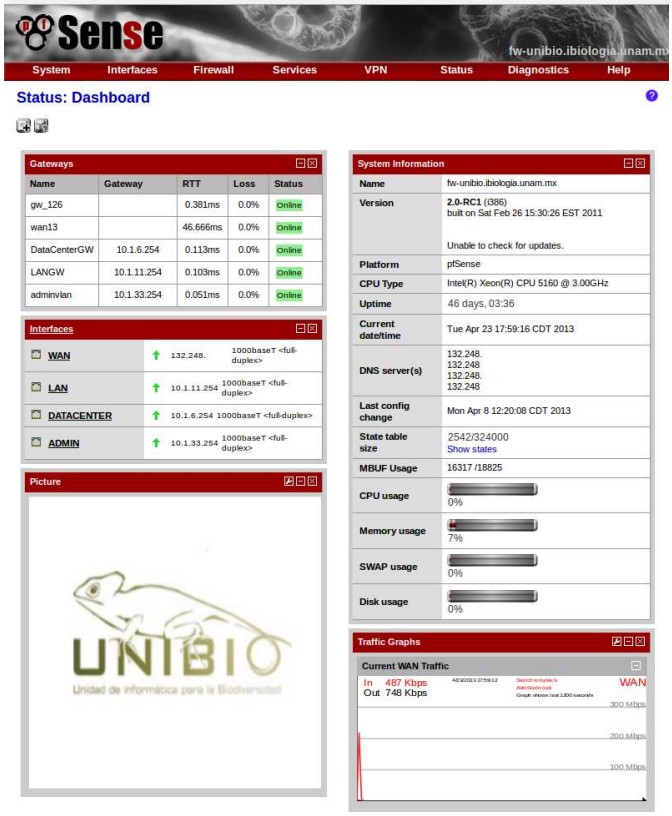


Figura 4.28: Firewall Unibio.

[3]Se denomina Data Center o centro de procesamiento de datos a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la informacion de una organizacion.

Capítulo 5

Análisis de Vulnerabilidades y Resultados

Como parte final de esta tesis, fue necesario un segundo análisis sobre los cambios efectuados sobre la infraestructura de red y seguridad del Instituto de Biología. Uno de los principales cambios con respecto a funcionalidad, ubicación física y lógica es el firewall, cuya ubicación deja claramente delimitado el perímetro de la red. Dejando a los dispositivos de comunicaciones e intranet bajo dos capas de seguridad.Dicho análisis de vulnerabilidades incluye una herramienta llamada Nessus, este es un programa que sirve para realizar escaneo de vulnerabilidades a servicios específicos, dichas pruebas disponen de una lista de plugins escritos en NASL (Nessus attack Scripting Language),para verificar los cambios efectuados sobre la seguridad del perímetro y los servicios se realizaron análisis a los servicios ya existentes, en producción del IB. Con dichas pruebas de obtendrán parámetros cuantificables los cuales arrojaran una diferencia en el rendimiento y seguridad antes y después de la implementación del firewall.

El rendimiento se define como la tasa de transferencia de datos libres de errores. Se mide por el tiempo de respuesta transcurrido de una petición de un equipo de cómputo hacia la red como por ejemplo una solicitud de una transferencia de archivos o acceso a Internet. Los factores que afectan el tiempo de respuesta son los siguientes:

- Número de usuarios: Entre más usuarios, más lenta la red.
- Velocidad de transmisión: La velocidad de transmisión es medida en bits por segundo (bps).
- Tipo de medio: La conexión física utilizada para conectar los nodos entre si.
- Tipo de hardware: Los dispositivos dependiendo de la tecnología que empleen los haga más rápidos.
- Software: El funcionamiento del Sistema Operativo dado el diseño del mismo.

Todos estos factores en conjunto ofrecen una calidad de servicio la cual se traduce en tecnologías que permiten un tratamiento especifico a un determinado tipo de tráfico. En las gráficas presentadas a continuación se muestran los parámetros de tiempo de respuesta en mili-segundos a través del tiempo sobre el tráfico que atraviesa cada una de las subinterfaces del firewall. A esto se le llama latencia, las señales entre computadoras viajan a la velocidad de la luz con un valor de 299.792.458 m/s, en un cable de fibra óptica la des-aceleración es de 195.200 km/s. La pérdida de velocidad es de 8.2 ms por cada 160 Km. Por lo que se tienen valores aproximados y/o recomendados con los cuales se puede tener una métrica, por ejemplo un valor inferior a 150ms es óptimo *ver fig 5.1.* En la lamina siguiente se puede apreciar dos subinterfaces en un intervalo de 3 meses con una media de 52.5 ms lo cual ha sido una velocidad constante para la la primera gráfica y para la segunda se tiene otro valor aún más majo en la media de 42.5 de acuerdo a las necesidades y demanda de cada VLAN este valor puede verse afectado con respecto a la carga que la VLAN tenga en ese lapso.

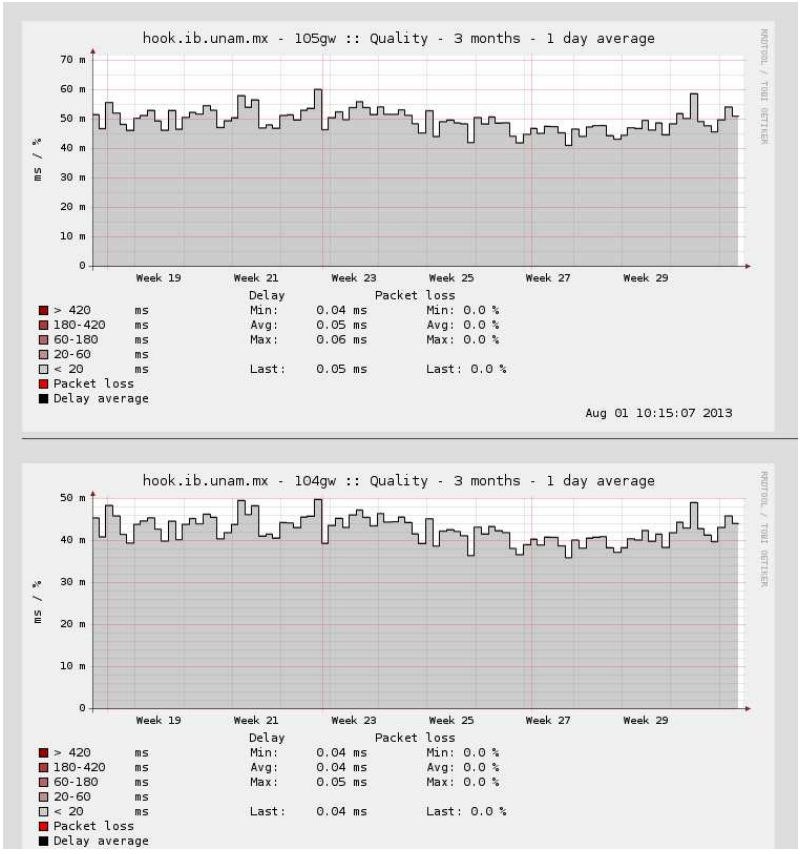


Figura 5.1: Gráficas de Latencia.

De los puntos anteriores se puede concluir que si se tiene una red con deficiencias y de un tamaño considerable, esta es más propensa a colapsar durante su operación, por ejemplo; una red que no tenga implementado un control de acceso o asignación de ancho de banda homogéneo, puede sufrir interrupciones en horas pico dado que la carga de tráfico aumenta considerablemente.PFsense posee herramientas para asignación de ancho de banda y visualización de tráfico entrante y saliente con el cual se puede tener un control sobre el comportamiento de la red de datos. La lamina siguiente muestra gráficas en las que se denota la graficación de una semana y tres meses *ver fig 5.2* y *ver fig5.3*.

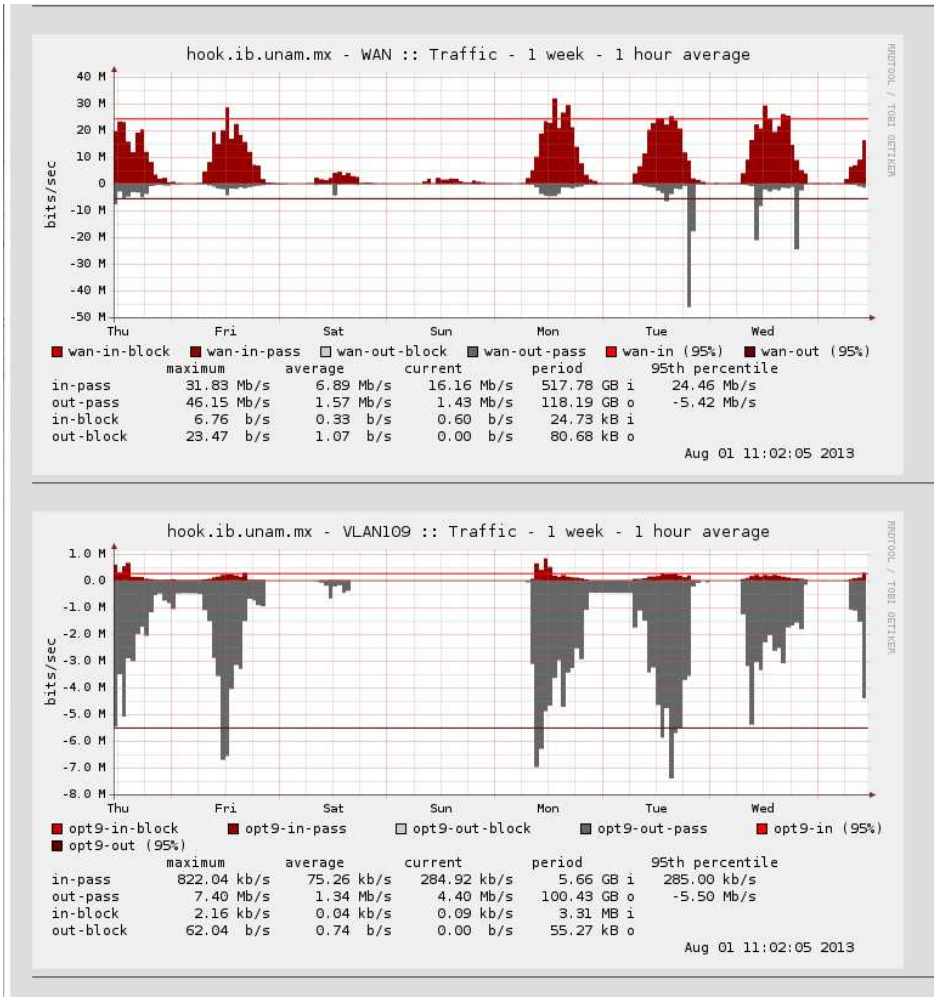


Figura 5.2: Gráficas de tráfico de una semana.

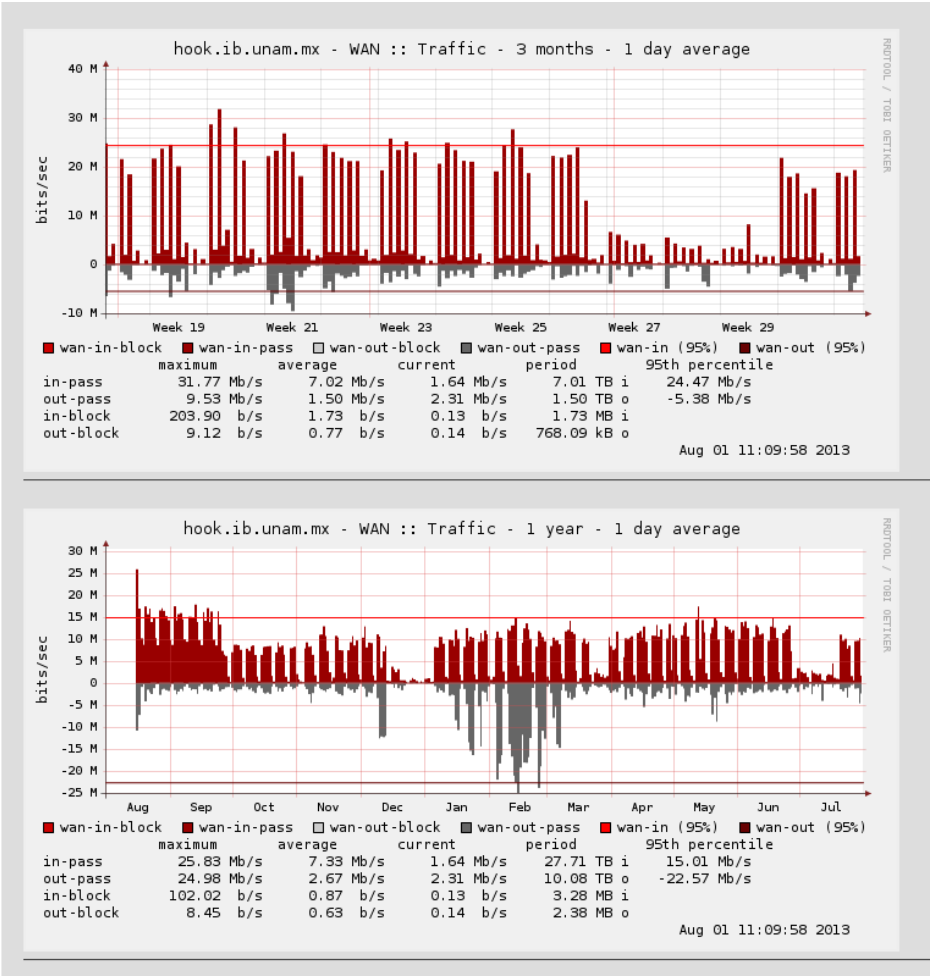


Figura 5.3: Gráficas de tráfico de tres meses.

De lo antes mencionado, surge la necesidad de la asignación de velocidad en transmisión, para aprovechar al máximo la infraestructura de red que se este utilizando, teniendo en cuenta el tipo de *hardware*, software y medio de comunicaciones que conforme la red de datos. Si las condiciones son propicias para un crecimiento u optimización a largo plazo, dentro de la infraestructura, es recomendable hacer uso óptimo de la misma. En la siguiente gráfica se muestra el tráfico en tiempo real de entrada y salida sobre las interfaces del firewall *ver fig 5.4* y *ver fig 5.5*.

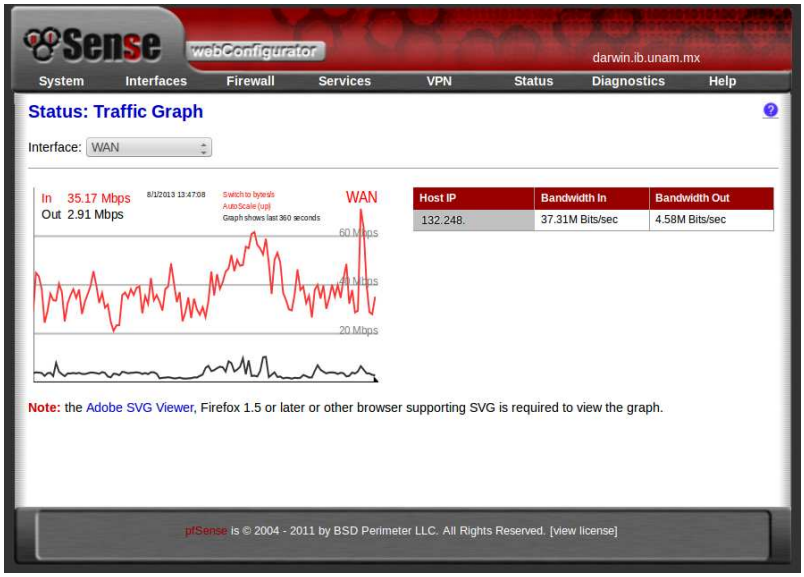


Figura 5.4: Gráficas de trafico WAN.

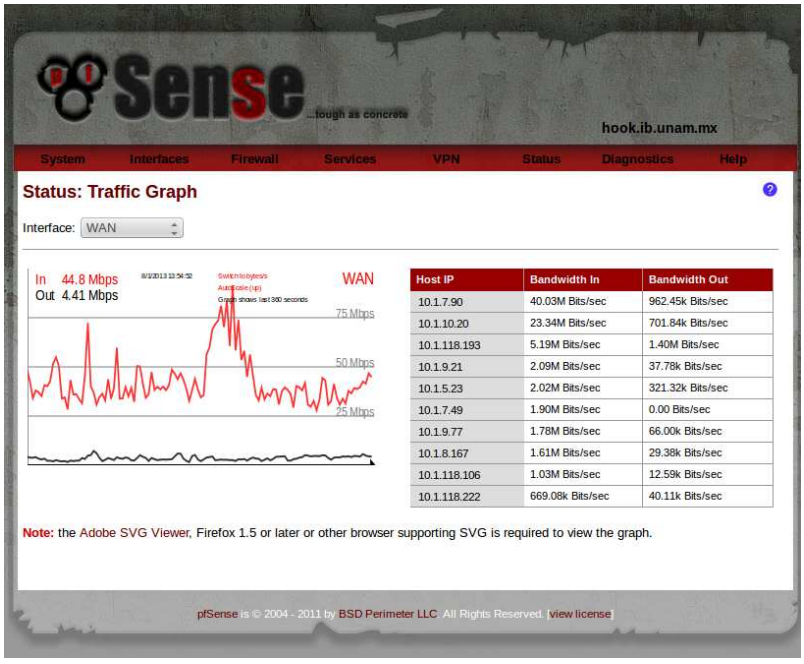


Figura 5.5: Gráficas de trafico WAN firewall 2.

Todos los parámetros mencionados anteriormente sirven como herramienta en la administración, análisis y control en una red en producción plena, con un optimo y tolerante a fallos.

5.0.1. Análisis de Vulnerabilidades después de la optimización.

Correo Electrónico.

La transformación del servicio de publico a privado es de gran ayuda para generar un ambiente seguro en la navegación del usuario en *intranet*[1], dado que la consulta y envío de correos se realiza por este medio, con este cambio se minimizó el *spam* y la calidad del servicio es mejor. Para complementar con la renovación del servicio se realizó la actualización de version del software y se instaló de manera virtual. Este servicio realmente significa el inicio de un proceso de optimización de recursos informáticos para contribuir con el consumo eficiente de energía eléctrica. Por lo que la nueva interfaz del correo quedo como en la imagen *ver fig 5.6*.

Figura 5.6: Interfaz web de correo actualizado y seguro.

Una vez realizado los cambios dentro del servidor con respecto a la aplicación y colocándolo dentro de una zona segura, se vuelve a ejecutar el escaneo con la misma herramienta para visualizar los resultados. Estos muestran cero vulnerabilidades criticas, una en alto y varias con el valor en medio, con lo cual se esta realizando un cambio drástico en la seguridad del equipo. Por lo que se nota la ausencia de vulnerabilidades que realmente afecten al servidor o lo comprometan seriamente. En la lamina siguiente se muestra el desplegado de dichas vulnerabilidades *ver fig 5.7* el haber reducido las vulnerabilidades que eran de impacto crítico minimiza el riesgo al que el servicio esta expuesto, el mitigar o transferir riesgos es a favor de las buenas practicas de seguridad informática. En conclusión de haber realizado esta prueba al correo electrónico radica en que la ubicación y falta de seguridad en un servicio crítico puede representar una pérdida o incidente de seguridad de alto impacto, el cual pudiera comprometer la información contenida en el servidor de correo electrónico, y las cuentas de los usuarios que conforman la comunidad del IB.

[1]Una intranet es una red de computadoras que realiza operaciones privadas que utiliza tecnologia Internet para compartir dentro de una institucion parte de sus sistemas de informacion y sistemas operacionales.

Por ello es de suma importancia que la seguridad tome un papel importante durante la implementación de sistemas informáticos sobre todo aquellos que se denominen de misión critica tales como los que se muestran en esta tesis.

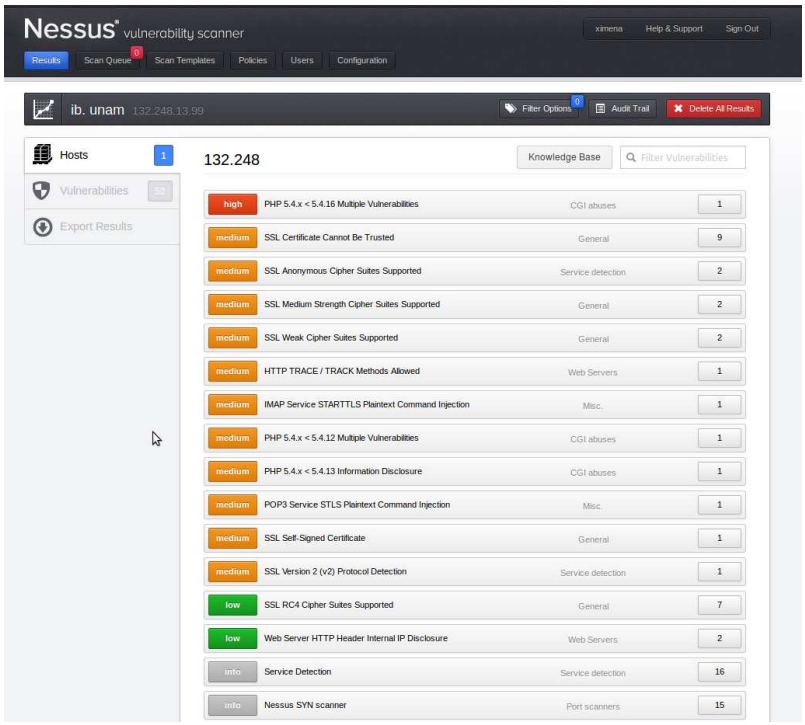


Figura 5.7: Despliegue de vulnerabilidades de correo seguro

Página Web.

Se ubicó la página web dentro de una zona de servicios críticos, lo cual genera un espacio dedicado a solo servicios de carácter especifico, este anidamiento de servicios también se dio gracias a la virtualizacion, como se menciona anteriormente, al englobar varios servicios en un dispositivo seguro y haciéndolo virtual, se aprovecha más el hardware disponible por medio de software y se aseguran los servicios de manera más eficiente, durante el proceso de migración el portal fue renovado para su nueva imagen *ver fig 5.8*.

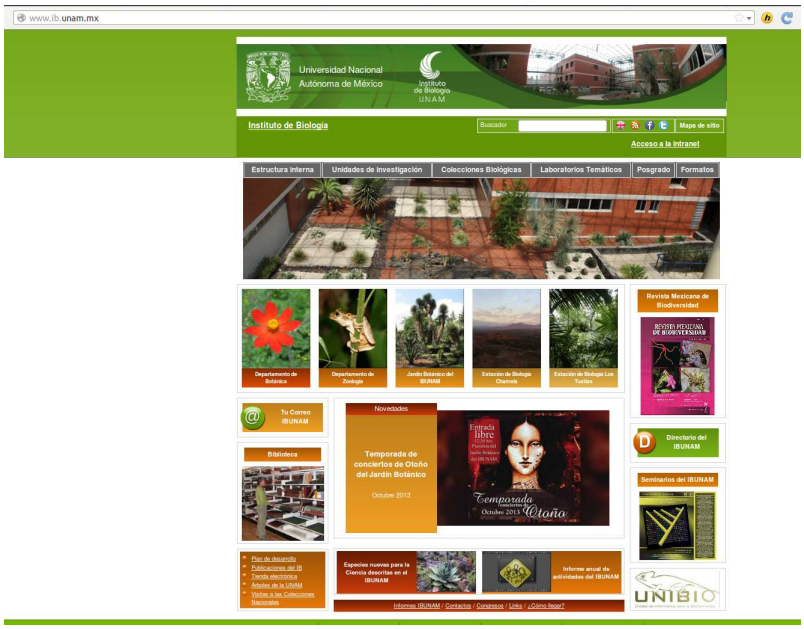


Figura 5.8: Pagina Web nueva.

Una vez hecho esto se ejecuto el mismo análisis de vulnerabilidades con los mismos parámetros sobre el servicio renovado el cual arrojo resultados drásticos en los cuales se nota la diferencia, ya que no hay vulnerabilidades criticas ni altas, solo de carácter medio e informativas.Con lo que se marca la diferencia sobre la ubicación de la página web. En este caso el server esta bajo el firewall PFsense que protege las conexiones entrantes y salientes del mismo, así mismo como el número de peticiones enviadas hacia la página web. En la imagen siguiente se tiene la suma total de las vulnerabilidades *ver fig 5.9* y *ver fig 5.10*

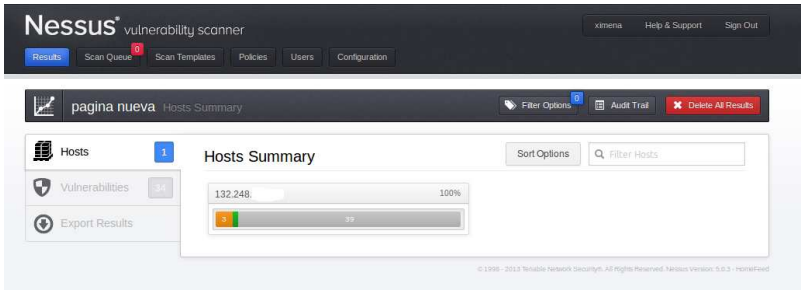


Figura 5.9: Porcentaje de vulnerabilidades de pagina web bajo pfsense

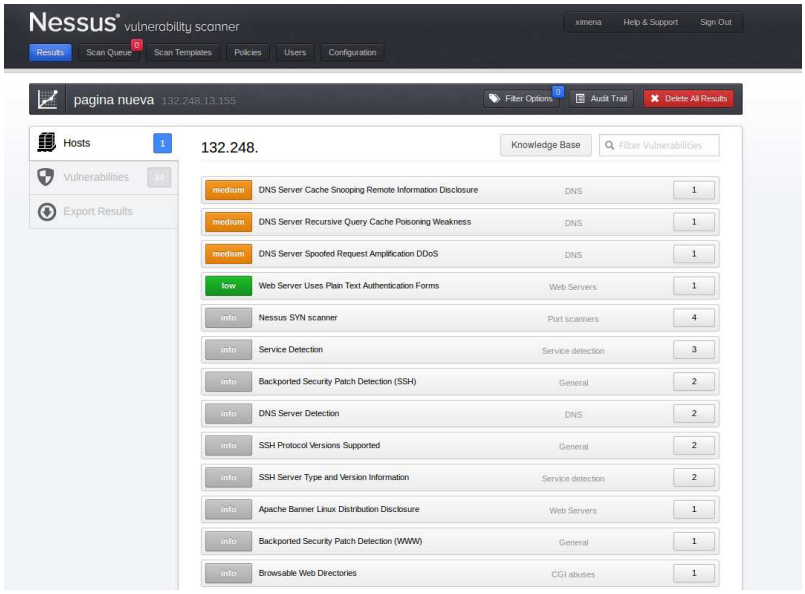


Figura 5.10: Despliegue de vulnerabilidades de pagina web bajo pfsense

La ubicación de los servicios está como se menciona en el capítulo anterior: *Estudio de caso e Implementacion*, sobre dos firewalls tipo statefull, los cuales reparten carga sobre el manejo del tráfico, es decir; el tráfico intranet es manejado por medio de dos dispositivos de telecomunicaciones: primero, un switch multicapa que realiza la función de convergencia a nivel de acceso, por lo que es el encargado de fusionar las comunicaciones por medio de un enlace troncal el cual proporciona todo el tráfico con y sin etiqueta hacia dos firewalls con propósito especifico, el primer firewall conjunta todas las VLANs para realizar el enrutamiento entre estas y generar así la intranet, por medio de DNS internos y reglas de acceso entre ellas, justo en esta zona se encuentran los servicios críticos. Entonces las actividades de enrutamiento y convergencia se reparten entre dos, con esto es menos el procesamiento de los equipos, el switch que gobernaba la intranet deja de ser publico, al remover la Ip real que este poseía, así mismo se removió el *helper-address* el cual reforzaba la interacción de la LAN con el DHCP. Cuyo servicio también se alojaba dentro de un servidor publico, es decir; cuando una petición interna se realizaba hacia el DHCP el switch multicapa daba acceso por medio de la subinterfaz pública/privada hacia el server de la página Web, donde estaba el demonio de DHCP con el pool de direcciones y este

regresaba hacia la intranet. A la par de los cambios este servicio de red fue ubicado en la intranet para eficientar la comunicación hacia él, por lo que esta función se absorbe por el firewall PFsense cuyo objetivo es el perímetro interno. Este firewall-router ejerce el control de ancho de banda y tráfico intranet. El segundo recibe una VLAN sin tag el cual filtra en capa 3 las conexiones entrantes y salientes sin necesidad de ser enruteable en ninguna dirección. Por lo que este *tubo* transparente se separa hacia su salida a Internet.

El segundo firewall quien gestiona el control de acceso de tipo WAN, procesa una cantidad mayor de conexiones entrantes desde el exterior, dado que es el dispositivo que realiza en contacto directo con Internet. Su tarea es separar el tráfico publico y privado, restringir las conexiones entrantes y contener incidentes de seguridad.Algunas de las herramientas, técnicas y mecanismos utilizados en este tesis incluyen acciones correctivas y preventivas las cuales transformaron a la institución a nivel infraestructura en una institución capaz de soportar procesos y crecimiento dentro de marco de la investigación e innovación.

Conclusiones.

Con base en los objetivos de la institución, esta tesis implementa un proceso de mejora continua en los procesos de red y seguridad informática, estos procesos describen el significado de la calidad y reflejan en el Instituto de Biología la necesidad de continuar con la misión de desarrollo de investigación científica. La seguridad se ha vuelto una característica ya obligatoria para con los datos y la tecnología, debe tomarse como un proceso natural dentro de cualquier institución,empresa etc. Dado que es un tema universal, es de suma importancia que el análisis, implementacion y administración de la seguridad se lleve a cabo por un experto en la materia, para de esta manera cubrir todos aspectos relacionados con los sistemas críticos y sus aseguramiento pertinente. Es esencial que se vea este proceso como un ciclo que no termina. El objeto de esta tesis comienza con la aportación hacia el IB, con el inicio de la identificación de los procesos críticos ligados con la tecnología, los cuales hacen posible muchos de los objetivos del IB tales como correo electrónico, página web, servicio de almacenamiento masivo, intranet etc. Esto implica la inversión por parte de la institución en infraestructura y servicios de alta tecnología lo cual haga más eficiente y mejore la calidad del servicio hacia los usuarios,con el aumento en los niveles de desempeño del recurso humano, a través de la capacitación continua se garantiza la actualización y se extienden las aptitudes del personal, de esta manera los objetivos y misión institucional se alinean con la investigación y desarrollo científico lo cual permite al Instituto de Biología esta la día con las TICs.

Bibliografía

[1] LOPEZ BARRIENTOS Ma. Jaquelina. Criptografia. Mexico, Universidad Nacional Autonoma de Mexico, Facultad de Ingenieria, 2009,275p, Pag 36.

[2] ZWICKY, Elizabeth D; Simon Cooper and Brent Chapman, 2nd ed.Building Internet Firewalls,O'Reilly, Second Edition, Morris Street, Sebastopol.

[3] CISCO Certified Network Associate Routing and Switching curricula. 2012. www.netacad.com

[4] FALL Kevin R,W. Richard Stevens, TCP/IP Illustraded, Volume 1: The protocols, 2nd Edition.Addison-Wesley.

[5] KORFF Yanek, Paco Hope, Cruce Potter. Mastering FreeBSD and OpenBSD Security. O'Reilly Media Inc.http://proquestcombo.safaribooksonline.com/book/operating-systems-and-server-administration/freebsd/0596006268/8dotfirewalls/

[6] NORTHCUTT, Stephen; Lenny Zeltser;Scott Winters;Ronald W. Ritchey,Inside Network Security Perimeter Sams,2nd Ed.

[7] BLANK Andrew G. TCP/IP Foundations, Sybex.

[8] ALLEN, Lee, Advanced Penetration Testing for Highly-Secured Enviroments: The Ultimate Security Guide, Packt Publishing. http://proquestcombo.safaribooksonline.com/book/software-engineering-and-development/software-testing/9781849517744

[9] ISO/IEC 27001 International Stantard, Information technology-Security techniques-Information Security management system-Requirements.

[10] ISO/IEC 27003 International Standard, Information technology/ Security techniques-Information Security management system guidance. First Edition.

[11] ISO/IEC 17799 Intermational Standard, Information technology-Security techniques-Code of practice for information security management.

[12] ISO/IEC 15408:2009 International Standard, Information technology, Security techniques-Evaluation criteria fo IT security–Part1: Introduction and general model.

[13] ISO/IEC 7498-1 International Standard, Information technology -Open Systems Interconnection- Basic Reference Model: The Basic Model.

[14] IBM BUECKER Axel, Andreas Per, Scott Paisley, Red Paper Understanding IT Perimeter Security.

[15] HERZOG Pete, ISECOM, OSSTMM 2.1 Manual de la metodologia abierta de testeo de seguridad.

[16] NIST National Institute of Standards and Technology, Guide to IPsec VPNs.

Anexo

Código Fuente Firewall 1

El código fuente se encuentra en formato *xml* el cual se puede almacenar con la misma extención y cargar en el firewall para la restauración del sistema.

```
1  <?xml version="1.0"?>
2  <pfsense>
3    <version>8.0</version>
4    <lastchange/>
5    <theme>metallic</theme>
6    <sysctl>
7      <item>
8        <descr><![CDATA[Disable the pf ftp proxy handler.]]></descr>
9        <tunable>debug.pfftpproxy</tunable>
10       <value>default</value>
11     </item>
12     <item>
13       <descr><![CDATA[Increase UFS read-ahead speeds to match ↩
             current state of hard drives and NCQ. More information ↩
             here: http://ivoras.sharanet.org/blog/tree/2010-11-19.ufs-↩
             read-ahead.html]]></descr>
14       <tunable>vfs.read_max</tunable>
15       <value>default</value>
16     </item>
17     <item>
18       <descr><![CDATA[Set the ephemeral port range to be lower.]]><↩
             /descr>
19       <tunable>net.inet.ip.portrange.first</tunable>
20       <value>default</value>
21     </item>
22     <item>
23       <descr><![CDATA[Drop packets to closed TCP ports without ↩
             returning a RST]]></descr>
24       <tunable>net.inet.tcp.blackhole</tunable>
25       <value>default</value>
26     </item><?xml version="1.0"?>
```

```
<pfsense>
  <version>8.0</version>
  <lastchange/>
  <theme>the_wall</theme>
  <sysctl>
    <item>
      <descr><![CDATA[Disable the pf ftp proxy handler.]]></descr>
      <tunable>debug.pfftpproxy</tunable>
      <value>default</value>
    </item>
    <item>
      <descr><![CDATA[Increase UFS read-ahead speeds to match ↩
          current state of hard drives and NCQ. More information ↩
          here: http://ivoras.sharanet.org/blog/tree/2010-11-19.ufs-↩
          read-ahead.html]]></descr>
      <tunable>vfs.read_max</tunable>
      <value>default</value>
    </item>
    <item>
      <descr><![CDATA[Set the ephemeral port range to be lower.]]><↩
          /descr>
      <tunable>net.inet.ip.portrange.first</tunable>
      <value>default</value>
    </item>
    <item>
      <descr><![CDATA[Drop packets to closed TCP ports without ↩
          returning a RST]]></descr>
      <tunable>net.inet.tcp.blackhole</tunable>
      <value>default</value>
    </item>
    <item>
      <descr><![CDATA[Do not send ICMP port unreachable messages ↩
          for closed UDP ports]]></descr>
      <tunable>net.inet.udp.blackhole</tunable>
      <value>default</value>
    </item>
    <item>
      <descr><![CDATA[Randomize the ID field in IP packets (default↩
           is 0: sequential IP IDs)]]></descr>
      <tunable>net.inet.ip.random_id</tunable>
      <value>default</value>
    </item>
    <item>
      <descr><![CDATA[Drop SYN-FIN packets (breaks RFC1379, but ↩
          nobody uses it anyway)]]></descr>
      <tunable>net.inet.tcp.drop_synfin</tunable>
      <value>default</value>
```

```
66      </item>
67      <item>
68        <descr><![CDATA[Enable sending IPv4 redirects]]></descr>
69        <tunable>net.inet.ip.redirect</tunable>
70        <value>default</value>
71      </item>
72      <item>
73        <descr><![CDATA[Enable sending IPv6 redirects]]></descr>
74        <tunable>net.inet6.ip6.redirect</tunable>
75        <value>default</value>
76      </item>
77      <item>
78        <descr><![CDATA[Generate SYN cookies for outbound SYN-ACK ↩
              packets]]></descr>
79        <tunable>net.inet.tcp.syncookies</tunable>
80        <value>default</value>
81      </item>
82      <item>
83        <descr><![CDATA[Maximum incoming/outgoing TCP datagram size (↩
              receive)]]></descr>
84        <tunable>net.inet.tcp.recvspace</tunable>
85        <value>default</value>
86      </item>
87      <item>
88        <descr><![CDATA[Maximum incoming/outgoing TCP datagram size (↩
              send)]]></descr>
89        <tunable>net.inet.tcp.sendspace</tunable>
90        <value>default</value>
91      </item>
92      <item>
93        <descr><![CDATA[IP Fastforwarding]]></descr>
94        <tunable>net.inet.ip.fastforwarding</tunable>
95        <value>default</value>
96      </item>
97      <item>
98        <descr><![CDATA[Do not delay ACK to try and piggyback it onto↩
              a data packet]]></descr>
99        <tunable>net.inet.tcp.delayed_ack</tunable>
100       <value>default</value>
101     </item>
102     <item>
103       <descr><![CDATA[Maximum outgoing UDP datagram size]]></descr>
104       <tunable>net.inet.udp.maxdgram</tunable>
105       <value>default</value>
106     </item>
107     <item>
```

```
108       <descr><![CDATA[Handling of non-IP packets which are not ↩
              passed to pfil (see if_bridge(4))]]></descr>
109       <tunable>net.link.bridge.pfil_onlyip</tunable>
110       <value>default</value>
111     </item>
112     <item>
113       <descr><![CDATA[Set to 0 to disable filtering on the incoming↩
              and outgoing member interfaces.]]></descr>
114       <tunable>net.link.bridge.pfil_member</tunable>
115       <value>default</value>
116     </item>
117     <item>
118       <descr><![CDATA[Set to 1 to enable filtering on the bridge ↩
              interface]]></descr>
119       <tunable>net.link.bridge.pfil_bridge</tunable>
120       <value>default</value>
121     </item>
122     <item>
123       <descr><![CDATA[Allow unprivileged access to tap(4) device ↩
              nodes]]></descr>
124       <tunable>net.link.tap.user_open</tunable>
125       <value>default</value>
126     </item>
127     <item>
128       <descr><![CDATA[Randomize PIDs (see src/sys/kern/kern_fork.c:↩
              sysctl_kern_randompid())]]></descr>
129       <tunable>kern.randompid</tunable>
130       <value>default</value>
131     </item>
132     <item>
133       <descr><![CDATA[Maximum size of the IP input queue]]></descr>
134       <tunable>net.inet.ip.intr_queue_maxlen</tunable>
135       <value>default</value>
136     </item>
137     <item>
138       <descr><![CDATA[Disable CTRL+ALT+Delete reboot from keyboard.↩
              ]]></descr>
139       <tunable>hw.syscons.kbd_reboot</tunable>
140       <value>default</value>
141     </item>
142     <item>
143       <descr><![CDATA[Enable TCP Inflight mode]]></descr>
144       <tunable>net.inet.tcp.inflight.enable</tunable>
145       <value>default</value>
146     </item>
147     <item>
148       <descr><![CDATA[Enable TCP extended debugging]]></descr>
```

```
149         <tunable>net.inet.tcp.log_debug</tunable>
150         <value>default</value>
151       </item>
152       <item>
153         <descr><![CDATA[Set ICMP Limits]]></descr>
154         <tunable>net.inet.icmp.icmplim</tunable>
155         <value>default</value>
156       </item>
157       <item>
158         <descr><![CDATA[TCP Offload Engine]]></descr>
159         <tunable>net.inet.tcp.tso</tunable>
160         <value>default</value>
161       </item>
162       <item>
163         <descr><![CDATA[Maximum socket buffer size]]></descr>
164         <tunable>kern.ipc.maxsockbuf</tunable>
165         <value>default</value>
166       </item>
167     </sysctl>
168     <system>
169       <optimization>normal</optimization>
170       <hostname>hook</hostname>
171       <domain>ib.unam.mx</domain>
172       <group>
173         <name>all</name>
174         <description><![CDATA[All Users]]></description>
175         <scope>system</scope>
176         <gid>1998</gid>
177       </group>
178       <group>
179         <name>admins</name>
180         <description><![CDATA[System Administrators]]></description>
181         <scope>system</scope>
182         <gid>1999</gid>
183         <member>0</member>
184         <priv>page-all</priv>
185       </group>
186
187       <user>
188         <scope>user</scope>
189         <name>alfredo</name>
190         <descr><![CDATA[Alfredo Wong]]></descr>
191         <expires/>
192         <authorizedkeys/>
193         <ipsecpsk/>
194         <uid>2000</uid>
195         <priv>page-dashboard-all</priv>
```

```
196         <priv>page-diagnostics-crash-reporter</priv>
197         <priv>page-diagnostics-logs-dhcp</priv>
198         <priv>page-diagnostics-logs-firewall</priv>
199         <priv>page-diagnostics-packetcapture</priv>
200         <priv>page-diagnostics-ping</priv>
201         <priv>page-diagnostics-routingtables</priv>
202         <priv>page-diagnostics-showstates</priv>
203         <priv>page-diagnostics-wirelessstatus</priv>
204         <priv>page-services-captiveportal</priv>
205         <priv>page-services-captiveportal-allowedhostnames</priv>
206         <priv>page-services-captiveportal-allowedips</priv>
207         <priv>page-services-captiveportal-editallowedhostnames</priv>
208         <priv>page-services-captiveportal-editallowedips</priv>
209         <priv>page-services-captiveportal-editmacaddresses</priv>
210         <priv>page-services-captiveportal-filemanager</priv>
211         <priv>page-services-captiveportal-macaddresses</priv>
212         <priv>page-services-captiveportal-voucher-edit</priv>
213         <priv>page-services-captiveportal-vouchers</priv>
214         <priv>page-services-dhcpserver</priv>
215         <priv>page-services-dhcpserver-editstaticmapping</priv>
216         <priv>page-status-captiveportal</priv>
217         <priv>page-status-captiveportal-test</priv>
218         <priv>page-status-captiveportal-voucher-rolls</priv>
219         <priv>page-status-captiveportal-vouchers</priv>
220         <priv>page-status-dhcpleases</priv>
221         <priv>page-status-filterreloadstatus</priv>
222         <priv>page-status-trafficgraph</priv>
223         <priv>page-diagnostics-arptable</priv>
224         <priv>page-diagnostics-backup/restore</priv>
225         <priv>page-diagnostics-command</priv>
226         <priv>page-diagnostics-configurationhistory</priv>
227         <priv>page-diagnostics-tables</priv>
228         <priv>page-diagnostics-traceroute</priv>
229       </user>
230       <nextuid>2001</nextuid>
231       <nextgid>2000</nextgid>
232       <timezone>America/Mexico_City</timezone>
233       <time-update-interval/>
234       <timeservers>0.pfsense.pool.ntp.org</timeservers>
235       <webgui>
236         <protocol>http</protocol>
237         <ssl-certref>4fe4a0973902d</ssl-certref>
238         <port/>
239         <max_procs>2</max_procs>
240         <nohttpreferercheck/>
241         <noantilockout/>
242       </webgui>
```

```
243     <disablenatreflection>yes</disablenatreflection>
244     <disablesegmentationoffloading/>
245     <disablelargereceiveoffloading/>
246     <enablesshd>enabled</enablesshd>
247     <dns1gwint>none</dns1gwint>
248     <dns2gwint>none</dns2gwint>
249     <dns3gwint>none</dns3gwint>
250     <dns4gwint>none</dns4gwint>
251     <dnsserver>10.1.16.253</dnsserver>
252   </system>
253   <interfaces>
254     <wan>
255       <enable/>
256       <if>bce1</if>
257       <ipaddr>10.1.16.2</ipaddr>
258       <subnet>24</subnet>
259       <gateway>WANGW</gateway>
260       <media/>
261       <mediaopt/>
262       <descr><![CDATA[WAN]]></descr>
263     </wan>
264     <lan>
265       <enable/>
266       <if>bce3</if>
267       <descr><![CDATA[LAN]]></descr>
268       <ipaddr>10.1.0.253</ipaddr>
269       <subnet>24</subnet>
270       <spoofmac/>
271     </lan>
272     <opt1>
273       <descr><![CDATA[vlan118]]></descr>
274       <if>bce3_vlan118</if>
275       <enable/>
276       <spoofmac/>
277       <ipaddr>10.1.118.254</ipaddr>
278       <subnet>24</subnet>
279     </opt1>
280     <opt2>
281       <descr><![CDATA[VlanAdmin]]></descr>
282       <if>bce3_vlan399</if>
283       <spoofmac/>
284       <ipaddr>10.1.251.14</ipaddr>
285       <subnet>16</subnet>
286     </opt2>
287     <opt3>
288       <descr><![CDATA[vlan102]]></descr>
289       <if>bce3_vlan102</if>
```

```
290         <enable/>
291         <spoofmac/>
292         <ipaddr>10.1.2.254</ipaddr>
293         <subnet>24</subnet>
294       </opt3>
295       <opt4>
296         <descr><![CDATA[vlan103]]></descr>
297         <if>bce3_vlan103</if>
298         <enable/>
299         <spoofmac/>
300         <ipaddr>10.1.3.254</ipaddr>
301         <subnet>24</subnet>
302       </opt4>
303       <opt5>
304         <descr><![CDATA[vlan104]]></descr>
305         <if>bce3_vlan104</if>
306         <enable/>
307         <spoofmac>78:2b:cb:3c:ce:d9</spoofmac>
308         <ipaddr>10.1.4.254</ipaddr>
309         <subnet>24</subnet>
310       </opt5>
311       <opt6>
312         <descr><![CDATA[vlan105]]></descr>
313         <if>bce3_vlan105</if>
314         <enable/>
315         <ipaddr>10.1.5.254</ipaddr>
316         <subnet>24</subnet>
317         <spoofmac/>
318       </opt6>
319       <opt7>
320         <descr><![CDATA[vlan107]]></descr>
321         <if>bce3_vlan107</if>
322         <enable/>
323         <ipaddr>10.1.7.254</ipaddr>
324         <subnet>24</subnet>
325         <spoofmac/>
326       </opt7>
327       <opt8>
328         <descr><![CDATA[vlan108]]></descr>
329         <if>bce3_vlan108</if>
330         <enable/>
331         <ipaddr>10.1.8.254</ipaddr>
332         <subnet>24</subnet>
333         <spoofmac/>
334       </opt8>
335       <opt9>
336         <descr><![CDATA[vlan109]]></descr>
```

```
337         <if>bce3_vlan109</if>
338         <enable/>
339         <ipaddr>10.1.9.254</ipaddr>
340         <subnet>24</subnet>
341         <spoofmac/>
342       </opt9>
343       <opt10>
344         <descr><![CDATA[vlan110]]></descr>
345         <if>bce3_vlan110</if>
346         <enable/>
347         <ipaddr>10.1.10.254</ipaddr>
348         <subnet>24</subnet>
349         <spoofmac/>
350       </opt10>
351       <opt11>
352         <descr><![CDATA[CAM]]></descr>
353         <if>bce3_vlan500</if>
354         <enable/>
355         <ipaddr>10.1.100.254</ipaddr>
356         <subnet>24</subnet>
357         <spoofmac/>
358       </opt11>
359       <opt12>
360         <descr><![CDATA[WifiOpen]]></descr>
361         <if>bce3_vlan66</if>
362         <enable/>
363         <ipaddr>10.1.66.254</ipaddr>
364         <subnet>24</subnet>
365         <spoofmac/>
366       </opt12>
367       <opt13>
368         <descr><![CDATA[LAB]]></descr>
369         <if>bce3_vlan23</if>
370         <enable/>
371         <ipaddr>10.1.23.254</ipaddr>
372         <subnet>24</subnet>
373         <spoofmac/>
374       </opt13>
375     </interfaces>
376     <staticroutes>
377       <route>
378         <network>10.1.0.0/16</network>
379         <gateway>WANGW</gateway>
380         <descr/>
381       </route>
382     </staticroutes>
383     <dhcpd>
```

```
384     <lan>
385       <range>
386         <from>10.1.0.1</from>
387         <to>10.1.0.252</to>
388       </range>
389       <defaultleasetime/>
390       <maxleasetime/>
391       <netmask/>
392       <failover_peerip/>
393       <gateway/>
394       <domain/>
395       <domainsearchlist/>
396       <ddnsdomain/>
397       <tftp/>
398       <ldap/>
399       <next-server/>
400       <filename/>
401       <rootpath/>
402       <numberoptions/>
403     </lan>
404     <opt3>
405       <range>
406         <from>10.1.2.1</from>
407         <to>10.1.2.253</to>
408       </range>
409       <defaultleasetime/>
410       <maxleasetime/>
411       <netmask/>
412       <failover_peerip/>
413       <gateway>10.1.2.254</gateway>
414       <domain/>
415       <domainsearchlist/>
416       <enable/>
417       <ddnsdomain/>
418       <tftp/>
419       <ldap/>
420       <next-server/>
421       <filename/>
422       <rootpath/>
423       <numberoptions/>
424     </opt3>
425     <opt4>
426       <range>
427         <from>10.1.3.1</from>
428         <to>10.1.3.240</to>
429       </range>
430       <defaultleasetime/>
```

```
431         <maxleasetime/>
432         <netmask/>
433         <failover_peerip/>
434         <gateway>10.1.3.254</gateway>
435         <domain/>
436         <domainsearchlist/>
437         <enable/>
438         <ddnsdomain/>
439         <tftp/>
440         <ldap/>
441         <next-server/>
442         <filename/>
443         <rootpath/>
444         <numberoptions/>
445         <staticmap>
446           <mac>00:25:b3:fb:5f:bd</mac>
447           <ipaddr>10.1.3.241</ipaddr>
448           <hostname>hp_laserjet_P2035n</hostname>
449           <descr><![CDATA[Dra. helga Ochoterena]]></descr>
450           <netbootfile/>
451         </staticmap>
452       </opt4>
453       <opt5>
454         <range>
455           <from>10.1.4.1</from>
456           <to>10.1.4.220</to>
457         </range>
458         <defaultleasetime/>
459         <maxleasetime/>
460         <netmask/>
461         <failover_peerip/>
462         <gateway>10.1.4.254</gateway>
463         <domain/>
464         <domainsearchlist/>
465         <enable/>
466         <ddnsdomain/>
467         <tftp/>
468         <ldap/>
469         <next-server/>
470         <filename/>
471         <rootpath/>
472         <numberoptions/>
473         <staticmap>
474           ALL Static ips
475         <range>
476           <from>10.1.100.10</from>
477           <to>10.1.100.20</to>
```

```
478         </range>
479         <defaultleasetime/>
480         <maxleasetime/>
481         <netmask/>
482         <failover_peerip/>
483         <gateway>10.1.100.254</gateway>
484         <domain/>
485         <domainsearchlist/>
486         <enable/>
487         <ddnsdomain/>
488         <tftp/>
489         <ldap/>
490         <next-server/>
491         <filename/>
492         <rootpath/>
493         <numberoptions/>
494       </opt11>
495       <opt12>
496         <range>
497           <from>10.1.66.20</from>
498           <to>10.1.66.250</to>
499         </range>
500         <defaultleasetime/>
501         <maxleasetime/>
502         <netmask/>
503         <failover_peerip/>
504         <gateway>10.1.66.254</gateway>
505         <domain/>
506         <domainsearchlist/>
507         <enable/>
508         <ddnsdomain/>
509         <tftp/>
510         <ldap/>
511         <next-server/>
512         <filename/>
513         <rootpath/>
514         <numberoptions/>
515         <staticmap>
516           <mac>00:11:88:92:68:33</mac>
517           <ipaddr>10.1.66.1</ipaddr>
518           <hostname>ap_videoconferencia</hostname>
519           <descr/>
520           <netbootfile/>
521         </staticmap>
522         <staticmap>
523           <mac>68:7f:74:6a:88:a8</mac>
524           <ipaddr>10.1.66.2</ipaddr>
```

```
525         <hostname>ap_biblioteca</hostname>
526         <descr/>
527         <netbootfile/>
528       </staticmap>
529       <staticmap>
530         <mac>00:12:17:74:b6:8f</mac>
531         <ipaddr>10.1.66.3</ipaddr>
532         <hostname>ap_UDC</hostname>
533         <descr/>
534         <netbootfile/>
535       </staticmap>
536       <staticmap>
537         <mac>00:12:17:7b:2f:3a</mac>
538         <ipaddr>10.1.66.5</ipaddr>
539         <hostname/>
540         <descr/>
541         <netbootfile/>
542       </staticmap>
543       <staticmap>
544         <mac>a0:f3:c1:6c:49:8d</mac>
545         <ipaddr>10.1.66.6</ipaddr>
546         <hostname>biblioteca</hostname>
547         <descr/>
548         <netbootfile/>
549       </staticmap>
550     </opt12>
551     <opt1>
552       <range>
553         <from>10.1.118.40</from>
554         <to>10.1.118.250</to>
555       </range>
556       <defaultleasetime/>
557       <maxleasetime/>
558       <netmask></netmask>
559       <failover_peerip/>
560       <gateway>10.1.118.254</gateway>
561       <domain/>
562       <domainsearchlist/>
563       <enable/>
564       <ddnsdomain/>
565       <tftp/>
566       <ldap/>
567       <next-server/>
568       <filename/>
569       <rootpath/>
570       <numberoptions/>
571       <staticmap>
```

```
572           <mac>64:66:b3:8c:36:da</mac>
573           <ipaddr>10.1.118.1</ipaddr>
574           <hostname>ap_mastozologia</hostname>
575           <descr/>
576           <netbootfile/>
577         </staticmap>
578         <staticmap>
579           <mac>a0:f3:c1:64:30:6e</mac>
580           <ipaddr>10.1.118.2</ipaddr>
581           <hostname>ap_helmintos</hostname>
582           <descr><![CDATA[Dr. Gerardo Perez Ponce de Leon Ed.D–2pp ↩
                LAB]]></descr>
583           <netbootfile/>
584         </staticmap>
585         <staticmap>
586           <mac>00:0c:41:d8:0f:c3</mac>
587           <ipaddr>10.1.118.3</ipaddr>
588           <hostname>ap_carcinologia</hostname>
589           <descr/>
590           <netbootfile/>
591         </staticmap>
592         <staticmap>
593           <mac>64:70:02:ca:4f:f7</mac>
594           <ipaddr>10.1.118.4</ipaddr>
595           <hostname>ap_gernandt</hostname>
596           <descr><![CDATA[Tp–Link]]></descr>
597           <netbootfile/>
598         </staticmap>
599         <staticmap>
600           <mac>68:7f:74:69:57:8e</mac>
601           <ipaddr>10.1.118.5</ipaddr>
602           <hostname>ap_restauracion</hostname>
603           <descr/>
604           <netbootfile/>
605         </staticmap>
606         <staticmap>
607           <mac>00:12:17:70:6d:f7</mac>
608           <ipaddr>10.1.118.6</ipaddr>
609           <hostname>ap_emm</hostname>
610           <descr/>
611           <netbootfile/>
612         </staticmap>
613         <staticmap>
614           <mac>00:12:17:a9:ef:29</mac>
615           <ipaddr>10.1.118.7</ipaddr>
616           <hostname>ap_cgonzalez</hostname>
617           <descr/>
```

```
618         <netbootfile/>
619       </staticmap>
620       <staticmap>
621         <mac>00:0f:66:75:26:a8</mac>
622         <ipaddr>10.1.118.8</ipaddr>
623         <hostname>ap_molecular</hostname>
624         <descr/>
625         <netbootfile/>
626       </staticmap>
627       <staticmap>
628         <mac>00:0f:66:19:7b:d2</mac>
629         <ipaddr>10.1.118.9</ipaddr>
630         <hostname>ap_espaciales</hostname>
631         <descr/>
632         <netbootfile/>
633       </staticmap>
634       <staticmap>
635         <mac>00:12:17:7a:ea:91</mac>
636         <ipaddr>10.1.118.10</ipaddr>
637         <hostname>ap_magdac</hostname>
638         <descr/>
639         <netbootfile/>
640       </staticmap>
641       <staticmap>
642         <mac>00:21:29:98:7b:46</mac>
643         <ipaddr>10.1.118.11</ipaddr>
644         <hostname>ap_sanchezcordero</hostname>
645         <descr/>
646         <netbootfile/>
647       </staticmap>
648       <staticmap>
649         <mac>00:12:17:74:b8:e8</mac>
650         <ipaddr>10.1.118.12</ipaddr>
651         <hostname>ap_malacologia</hostname>
652         <descr/>
653         <netbootfile/>
654       </staticmap>
655       <staticmap>
656         <mac>00:22:3f:0b:78:59</mac>
657         <ipaddr>10.1.118.13</ipaddr>
658         <hostname>ap_zaragoza</hostname>
659         <descr/>
660         <netbootfile/>
661       </staticmap>
662       <staticmap>
663         <mac>00:1e:58:ec:79:9a</mac>
664         <ipaddr>10.1.118.16</ipaddr>
```

```
665         <hostname>ap_psilva</hostname>
666         <descr/>
667         <netbootfile/>
668       </staticmap>
669       <staticmap>
670         <mac>00:14:bf:7d:96:58</mac>
671         <ipaddr>10.1.118.17</ipaddr>
672         <hostname>ap_smagallon</hostname>
673         <descr/>
674         <netbootfile/>
675       </staticmap>
676       <staticmap>
677         <mac>68:7f:74:69:1b:72</mac>
678         <ipaddr>10.1.118.19</ipaddr>
679         <hostname>ap_pescados</hostname>
680         <descr/>
681         <netbootfile/>
682       </staticmap>
683       <staticmap>
684         <mac>00:25:9c:9e:ee:f1</mac>
685         <ipaddr>10.1.118.20</ipaddr>
686         <hostname>ap_atilano</hostname>
687         <descr/>
688         <netbootfile/>
689       </staticmap>
690       <staticmap>
691         <mac>08:00:46:d0:04:be</mac>
692         <ipaddr>10.1.118.21</ipaddr>
693         <hostname>ap_acaros</hostname>
694         <descr/>
695         <netbootfile/>
696       </staticmap>
697       <staticmap>
698         <mac>00:12:17:70:0a:a8</mac>
699         <ipaddr>10.1.118.23</ipaddr>
700         <hostname>ap_orquideas</hostname>
701         <descr/>
702         <netbootfile/>
703       </staticmap>
704       <staticmap>
705         <mac>00:1d:0f:d8:cd:e8</mac>
706         <ipaddr>10.1.118.25</ipaddr>
707         <hostname>ap_taniat</hostname>
708         <descr><![CDATA[Router Tania Terrazas JB Colecciones]]></↩
              descr>
709         <netbootfile/>
710       </staticmap>
```

```
711         <staticmap>
712           <mac>64:66:b3:8c:33:31</mac>
713           <ipaddr>10.1.118.26</ipaddr>
714           <hostname>ap_ornitologia</hostname>
715           <descr><![CDATA[Coleccion Nacional de Aves]]></descr>
716           <netbootfile/>
717         </staticmap>
718         <staticmap>
719           <mac>64:70:02:e0:4b:04</mac>
720           <ipaddr>10.1.118.27</ipaddr>
721           <hostname>ap_presup</hostname>
722           <descr><![CDATA[ap Jefe Comi]]></descr>
723           <netbootfile/>
724         </staticmap>
725         <staticmap>
726           <mac>64:70:02:bb:8f:2a</mac>
727           <ipaddr>10.1.118.28</ipaddr>
728           <hostname>ap_jardin2</hostname>
729           <descr><![CDATA[Ap del Lobby del Jardin]]></descr>
730           <netbootfile/>
731         </staticmap>
732         <staticmap>
733           <mac>64:70:02:bb:a1:08</mac>
734           <ipaddr>10.1.118.29</ipaddr>
735           <hostname>ap_jardin1</hostname>
736           <descr><![CDATA[Lugar por definir por Don Dogor]]></descr>
737           <netbootfile/>
738         </staticmap>
739         <staticmap>
740           <mac>9c:2a:70:6d:0c:94</mac>
741           <ipaddr>10.1.118.30</ipaddr>
742           <hostname>HP_David_Gernard</hostname>
743           <descr/>
744           <netbootfile/>
745         </staticmap>
746         <staticmap>
747           <mac>f8:1a:67:d6:d4:f5</mac>
748           <ipaddr>10.1.118.31</ipaddr>
749           <hostname>ap_agaves</hostname>
750           <descr><![CDATA[Dr. Abisai]]></descr>
751           <netbootfile/>
752         </staticmap>
753         <staticmap>
754           <mac>a0:f3:c1:5e:d3:9a</mac>
755           <ipaddr>10.1.118.32</ipaddr>
756           <hostname>ap_col</hostname>
757           <descr><![CDATA[colecciones]]></descr>
```

```
758           <netbootfile/>
759         </staticmap>
760         <staticmap>
761           <mac>00:18:39:02:bc:a6</mac>
762           <ipaddr>10.1.118.33</ipaddr>
763           <hostname>ap_Olson</hostname>
764           <descr><![CDATA[Cubiculo Dr. Mark Olson]]></descr>
765           <netbootfile/>
766         </staticmap>
767         <staticmap>
768           <mac>f8:1a:67:d6:d5:45</mac>
769           <ipaddr>10.1.118.34</ipaddr>
770           <hostname>ap_Ponce</hostname>
771           <descr><![CDATA[Ap cubiculo Dr. Gerardo Perez Ponce de Leon↩
                ]]></descr>
772           <netbootfile/>
773         </staticmap>
774       </opt1>
775       <wan>
776         <range>
777           <from/>
778           <to/>
779         </range>
780         <defaultleasetime/>
781         <maxleasetime/>
782         <netmask/>
783         <failover_peerip/>
784         <gateway/>
785         <domain/>
786         <domainsearchlist/>
787         <ddnsdomain/>
788         <tftp/>
789         <ldap/>
790         <next-server/>
791         <filename/>
792         <rootpath/>
793         <numberoptions/>
794       </wan>
795     </dhcpd>
796     <pptpd>
797       <mode/>
798       <redir/>
799       <localip/>
800       <remoteip/>
801     </pptpd>
802     <dnsmasq>
803       <enable/>
```

```
804       <custom_options/>
805       <hosts>
806         <host>app</host>
807         <domain>ib.unam.mx</domain>
808         <ip>10.1.100.3</ip>
809         <descr><![CDATA[Ed A primer piso]]></descr>
810       </hosts>
811       <hosts>
812         <host>colecciones</host>
813         <domain>ib.unam.mx</domain>
814         <ip>10.1.100.7</ip>
815         <descr><![CDATA[col]]></descr>
816       </hosts>
817       <hosts>
818         <host>congresoslccs</host>
819         <domain>unam.mx</domain>
820         <ip>10.1.4.239</ip>
821         <descr><![CDATA[Congreso cactaceas]]></descr>
822       </hosts>
823       <hosts>
824         <host>correo</host>
825         <domain>ib.unam.mx</domain>
826         <ip>10.1.4.98</ip>
827         <descr/>
828       </hosts>
829       <hosts>
830         <host>jb</host>
831         <domain>ib.unam.mx</domain>
832         <ip>10.1.100.6</ip>
833         <descr><![CDATA[dvr jb]]></descr>
834       </hosts>
835       <hosts>
836         <host>secuenciador</host>
837         <domain>ib.unam.mx</domain>
838         <ip>10.1.5.240</ip>
839         <descr><![CDATA[hacia secuenciador]]></descr>
840       </hosts>
841     </dnsmasq>
842     <snmpd>
843       <syslocation/>
844       <syscontact/>
845       <rocommunity>public</rocommunity>
846     </snmpd>
847     <diag>
848       <ipv6nat>
849         <ipaddr/>
850       </ipv6nat>
```

```
851   </diag>
852   <bridge/>
853   <syslog>
854     <reverse/>
855     <nentries>100</nentries>
856     <filter/>
857     <system/>
858     <remoteserver>10.1.4.20</remoteserver>
859     <remoteserver2/>
860     <remoteserver3/>
861     <dhcp/>
862     <enable/>
863   </syslog>
864   <nat>
865     <ipsecpassthru>
866       <enable/>
867     </ipsecpassthru>
868     <advancedoutbound>
869       <enable/>
870     </advancedoutbound>
871   </nat>
872   <filter>
873     <rule>
874       <id/>
875       <type>pass</type>
876       <interface>lan,opt1</interface>
877       <tag/>
878       <tagged/>
879       <direction>any</direction>
880       <floating>yes</floating>
881       <max/>
882       <max-src-nodes/>
883       <max-src-conn/>
884       <max-src-states/>
885       <statetimeout/>
886       <statetype>keep state</statetype>
887       <os/>
888       <source>
889         <any/>
890       </source>
891       <destination>
892         <any/>
893       </destination>
894       <descr/>
895     </rule>
896     <rule>
897       <id/>
```

```
898         <type>pass</type>
899         <interface>wan</interface>
900         <tag/>
901         <tagged/>
902         <max/>
903         <max-src-nodes/>
904         <max-src-conn/>
905         <max-src-states/>
906         <statetimeout/>
907         <statetype>keep state</statetype>
908         <os/>
909         <source>
910           <any/>
911         </source>
912         <destination>
913           <any/>
914         </destination>
915         <log/>
916         <descr><![CDATA[Open Wan]]></descr>
917       </rule>
918       <rule>
919         <id/>
920         <type>pass</type>
921         <interface>lan</interface>
922         <tag/>
923         <tagged/>
924         <max/>
925         <max-src-nodes/>
926         <max-src-conn/>
927         <max-src-states/>
928         <statetimeout/>
929         <statetype>keep state</statetype>
930         <os/>
931         <source>
932           <any/>
933         </source>
934         <destination>
935           <any/>
936         </destination>
937         <descr><![CDATA[Default allow LAN to any rule]]></descr>
938       </rule>
939       <rule>
940         <id/>
941         <type>pass</type>
942         <interface>opt1</interface>
943         <tag/>
944         <tagged/>
```

```
945         <max/>
946         <max-src-nodes/>
947         <max-src-conn/>
948         <max-src-states/>
949         <statetimeout/>
950         <statetype>keep state</statetype>
951         <os/>
952         <source>
953           <any/>
954         </source>
955         <destination>
956           <any/>
957         </destination>
958         <descr/>
959       </rule>
960       <rule>
961         <id/>
962         <type>pass</type>
963         <interface>opt2</interface>
964         <tag/>
965         <tagged/>
966         <max/>
967         <max-src-nodes/>
968         <max-src-conn/>
969         <max-src-states/>
970         <statetimeout/>
971         <statetype>keep state</statetype>
972         <os/>
973         <source>
974           <any/>
975         </source>
976         <destination>
977           <any/>
978         </destination>
979         <descr><![CDATA[Trafico administrativo]]></descr>
980       </rule>
981       <rule>
982         <id/>
983         <type>pass</type>
984         <interface>opt3</interface>
985         <tag/>
986         <tagged/>
987         <max/>
988         <max-src-nodes/>
989         <max-src-conn/>
990         <max-src-states/>
991         <statetimeout/>
```

```
992         <statetype>keep state</statetype>
993         <os/>
994         <source>
995           <any/>
996         </source>
997         <destination>
998           <any/>
999         </destination>
1000        <descr/>
1001        <dnpipe>1</dnpipe>
1002        <pdnpipe>2</pdnpipe>
1003      </rule>
1004      <rule>
1005        <id/>
1006        <type>pass</type>
1007        <interface>opt4</interface>
1008        <tag/>
1009        <tagged/>
1010        <max/>
1011        <max-src-nodes/>
1012        <max-src-conn/>
1013        <max-src-states/>
1014        <statetimeout/>
1015        <statetype>keep state</statetype>
1016        <os/>
1017        <source>
1018          <any/>
1019        </source>
1020        <destination>
1021          <any/>
1022        </destination>
1023        <descr/>
1024      </rule>
1025      <rule>
1026        <id/>
1027        <type>block</type>
1028        <interface>opt5</interface>
1029        <tag/>
1030        <tagged/>
1031        <max/>
1032        <max-src-nodes/>
1033        <max-src-conn/>
1034        <max-src-states/>
1035        <statetimeout/>
1036        <statetype>keep state</statetype>
1037        <os/>
1038        <protocol>tcp/udp</protocol>
```

```
1039        <source>
1040          <address>10.1.4.238</address>
1041        </source>
1042        <destination>
1043          <any/>
1044        </destination>
1045        <log/>
1046        <descr><![CDATA[block internet]]></descr>
1047      </rule>
1048      <rule>
1049        <id/>
1050        <type>pass</type>
1051        <interface>opt5</interface>
1052        <tag/>
1053        <tagged/>
1054        <max/>
1055        <max-src-nodes/>
1056        <max-src-conn/>
1057        <max-src-states/>
1058        <statetimeout/>
1059        <statetype>keep state</statetype>
1060        <os/>
1061        <source>
1062          <any/>
1063        </source>
1064        <destination>
1065          <any/>
1066        </destination>
1067        <descr/>
1068      </rule>
1069      <rule>
1070        <id/>
1071        <type>pass</type>
1072        <interface>opt6</interface>
1073        <tag/>
1074        <tagged/>
1075        <max/>
1076        <max-src-nodes/>
1077        <max-src-conn/>
1078        <max-src-states/>
1079        <statetimeout/>
1080        <statetype>keep state</statetype>
1081        <os/>
1082        <source>
1083          <any/>
1084        </source>
1085        <destination>
```

```
1086          <any/>
1087        </destination>
1088        <descr/>
1089        <dnpipe>1</dnpipe>
1090        <pdnpipe>2</pdnpipe>
1091      </rule>
1092      <rule>
1093        <id/>
1094        <type>pass</type>
1095        <interface>opt7</interface>
1096        <tag/>
1097        <tagged/>
1098        <max/>
1099        <max-src-nodes/>
1100        <max-src-conn/>
1101        <max-src-states/>
1102        <statetimeout/>
1103        <statetype>keep state</statetype>
1104        <os/>
1105        <source>
1106          <any/>
1107        </source>
1108        <destination>
1109          <any/>
1110        </destination>
1111        <descr/>
1112      </rule>
1113      <rule>
1114        <id/>
1115        <type>pass</type>
1116        <interface>opt8</interface>
1117        <tag/>
1118        <tagged/>
1119        <max/>
1120        <max-src-nodes/>
1121        <max-src-conn/>
1122        <max-src-states/>
1123        <statetimeout/>
1124        <statetype>keep state</statetype>
1125        <os/>
1126        <source>
1127          <any/>
1128        </source>
1129        <destination>
1130          <any/>
1131        </destination>
1132        <descr/>
```

```
1133      </rule>
1134      <rule>
1135        <id/>
1136        <type>pass</type>
1137        <interface>opt9</interface>
1138        <tag/>
1139        <tagged/>
1140        <max/>
1141        <max-src-nodes/>
1142        <max-src-conn/>
1143        <max-src-states/>
1144        <statetimeout/>
1145        <statetype>keep state</statetype>
1146        <os/>
1147        <source>
1148          <any/>
1149        </source>
1150        <destination>
1151          <any/>
1152        </destination>
1153        <descr/>
1154        <dnpipe>1</dnpipe>
1155        <pdnpipe>2</pdnpipe>
1156      </rule>
1157      <rule>
1158        <id/>
1159        <type>pass</type>
1160        <interface>opt9</interface>
1161        <tag/>
1162        <tagged/>
1163        <max/>
1164        <max-src-nodes/>
1165        <max-src-conn/>
1166        <max-src-states/>
1167        <statetimeout/>
1168        <statetype>keep state</statetype>
1169        <os/>
1170        <protocol>tcp/udp</protocol>
1171        <source>
1172
1173        </source>
1174        <destination>
1175          <any/>
1176          <port>3050</port>
1177        </destination>
1178        <descr/>
1179      </rule>
```

```
1180      <rule>
1181        <id/>
1182        <type>pass</type>
1183        <interface>opt10</interface>
1184        <tag/>
1185        <tagged/>
1186        <max/>
1187        <max-src-nodes/>
1188        <max-src-conn/>
1189        <max-src-states/>
1190        <statetimeout/>
1191        <statetype>keep state</statetype>
1192        <os/>
1193        <source>
1194          <any/>
1195        </source>
1196        <destination>
1197          <any/>
1198        </destination>
1199        <descr/>
1200        <dnpipe>1</dnpipe>
1201        <pdnpipe>2</pdnpipe>
1202      </rule>
1203      <rule>
1204        <id/>
1205        <type>pass</type>
1206        <interface>opt11</interface>
1207        <tag/>
1208        <tagged/>
1209        <max/>
1210        <max-src-nodes/>
1211        <max-src-conn/>
1212        <max-src-states/>
1213        <statetimeout/>
1214        <statetype>keep state</statetype>
1215        <os/>
1216        <source>
1217          <any/>
1218        </source>
1219        <destination>
1220          <any/>
1221        </destination>
1222        <descr/>
1223      </rule>
1224      <rule>
1225        <id/>
1226        <type>pass</type>
```

```
1227        <interface>opt12</interface>
1228        <tag/>
1229        <tagged/>
1230        <max/>
1231        <max-src-nodes/>
1232        <max-src-conn/>
1233        <max-src-states/>
1234        <statetimeout/>
1235        <statetype>keep state</statetype>
1236        <os/>
1237        <source>
1238          <any/>
1239        </source>
1240        <destination>
1241          <any/>
1242        </destination>
1243        <descr/>
1244        <dnpipe>1</dnpipe>
1245        <pdnpipe>2</pdnpipe>
1246      </rule>
1247      <rule>
1248        <id/>
1249        <type>pass</type>
1250        <interface>opt13</interface>
1251        <tag/>
1252        <tagged/>
1253        <max/>
1254        <max-src-nodes/>
1255        <max-src-conn/>
1256        <max-src-states/>
1257        <statetimeout/>
1258        <statetype>keep state</statetype>
1259        <os/>
1260        <source>
1261          <any/>
1262        </source>
1263        <destination>
1264          <any/>
1265        </destination>
1266        <descr><![CDATA[Open cisco]]></descr>
1267      </rule>
1268    </filter>
1269    <shaper/>
1270    <ipsec>
1271      <preferoldsa/>
1272    </ipsec>
1273    <aliases/>
```

```
1274    <proxyarp/>
1275    <cron>
1276      <item>
1277        <minute>0</minute>
1278        <hour>*</hour>
1279        <mday>*</mday>
1280        <month>*</month>
1281        <wday>*</wday>
1282        <who>root</who>
1283        <command>/usr/bin/nice -n20 newsyslog</command>
1284      </item>
1285      <item>
1286        <minute>1,31</minute>
1287        <hour>0-5</hour>
1288        <mday>*</mday>
1289        <month>*</month>
1290        <wday>*</wday>
1291        <who>root</who>
1292        <command>/usr/bin/nice -n20 adjkerntz -a</command>
1293      </item>
1294      <item>
1295        <minute>1</minute>
1296        <hour>3</hour>
1297        <mday>1</mday>
1298        <month>*</month>
1299        <wday>*</wday>
1300        <who>root</who>
1301        <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command↩
              >
1302      </item>
1303      <item>
1304        <minute>*/60</minute>
1305        <hour>*</hour>
1306        <mday>*</mday>
1307        <month>*</month>
1308        <wday>*</wday>
1309        <who>root</who>
1310        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t↩
              3600 sshlockout</command>
1311      </item>
1312      <item>
1313        <minute>1</minute>
1314        <hour>1</hour>
1315        <mday>*</mday>
1316        <month>*</month>
1317        <wday>*</wday>
1318        <who>root</who>
```

```
1319        <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
1320      </item>
1321      <item>
1322        <minute>*/60</minute>
1323        <hour>*</hour>
1324        <mday>*</mday>
1325        <month>*</month>
1326        <wday>*</wday>
1327        <who>root</who>
1328        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t↩
                3600 virusprot</command>
1329      </item>
1330      <item>
1331        <minute>30</minute>
1332        <hour>12</hour>
1333        <mday>*</mday>
1334        <month>*</month>
1335        <wday>*</wday>
1336        <who>root</who>
1337        <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command↩
              >
1338      </item>
1339      <item>
1340        <task_name>squid_rotate_logs</task_name>
1341        <minute>0</minute>
1342        <hour>0</hour>
1343        <mday>*</mday>
1344        <month>*</month>
1345        <wday>*</wday>
1346        <who>root</who>
1347        <command>/bin/rm /var/squid/cache/swap.state; /usr/local/sbin↩
              /squid -k rotate</command>
1348      </item>
1349      <item>
1350        <task_name>squid_check_swapstate</task_name>
1351        <minute>*/15</minute>
1352        <hour>*</hour>
1353        <mday>*</mday>
1354        <month>*</month>
1355        <wday>*</wday>
1356        <who>root</who>
1357        <command>/usr/local/pkg/swapstate_check.php</command>
1358      </item>
1359    </cron>
1360    <wol>
1361      <wolentry>
1362        <interface>opt12</interface>
```

```
1363        <mac>00:12:17:7b:2f:3a</mac>
1364        <descr/>
1365      </wolentry>
1366      <wolentry>
1367        <interface>opt5</interface>
1368        <mac>00:10:b5:72:8d:54</mac>
1369        <descr><![CDATA[Pfsense_UDC]]></descr>
1370      </wolentry>
1371      <wolentry>
1372        <interface>opt5</interface>
1373        <mac>00:14:22:27:26:6a</mac>
1374        <descr><![CDATA[admon_ds009]]></descr>
1375      </wolentry>
1376      <wolentry>
1377        <interface>opt8</interface>
1378        <mac>64:66:b3:5d:46:1a</mac>
1379        <descr><![CDATA[ap_caseta2]]></descr>
1380      </wolentry>
1381      <wolentry>
1382        <interface>opt1</interface>
1383        <mac>68:7f:74:12:0c:1c</mac>
1384        <descr><![CDATA[ap_presup]]></descr>
1385      </wolentry>
1386    </wol>
1387    <rrd>
1388      <enable/>
1389    </rrd>
1390    <load_balancer>
1391      <monitor_type>
1392        <name>ICMP</name>
1393        <type>icmp</type>
1394        <descr><![CDATA[ICMP]]></descr>
1395        <options/>
1396      </monitor_type>
1397      <monitor_type>
1398        <name>TCP</name>
1399        <type>tcp</type>
1400        <descr><![CDATA[Generic TCP]]></descr>
1401        <options/>
1402      </monitor_type>
1403      <monitor_type>
1404        <name>HTTP</name>
1405        <type>http</type>
1406        <descr><![CDATA[Generic HTTP]]></descr>
1407        <options>
1408          <path>/</path>
1409          <host/>
```

```
1410            <code>200</code>
1411          </options>
1412        </monitor_type>
1413        <monitor_type>
1414          <name>HTTPS</name>
1415          <type>https</type>
1416          <descr><![CDATA[Generic HTTPS]]></descr>
1417          <options>
1418            <path>/</path>
1419            <host/>
1420            <code>200</code>
1421          </options>
1422        </monitor_type>
1423        <monitor_type>
1424          <name>SMTP</name>
1425          <type>send</type>
1426          <descr><![CDATA[Generic SMTP]]></descr>
1427          <options>
1428            <send>EHLO nosuchhost</send>
1429            <expect>250-</expect>
1430          </options>
1431        </monitor_type>
1432      </load_balancer>
1433      <widgets>
1434        <sequence>gateways-container:col1:show,system_information-↩
               container:col1:show,captive_portal_status-↩
               container:col1:close,carp_status-container:col1:close,↩
               cpu_graphs-container:col1:close,gmirror_status-↩
               container:col1:close,installed_packages-container:col1:close↩
               ,interface_statistics-container:col1:close,picture-↩
               container:col2:show,interfaces-container:col2:show,ipsec-↩
               container:col2:close,load_balancer_status-↩
               container:col2:close,log-container:col2:close,rss-↩
               container:col2:close,services_status-container:col2:close,↩
               traffic_graphs-container:col2:close,openvpn-↩
               container:col2:none,wake_on_lan-container:col2:none</↩
               sequence>
1435
1436      </widgets>
1437      <revision>
1438        <time>1381165008</time>
1439        <description><![CDATA[admin@10.1.4.233: /services_dhcp.php made↩
                unknown change]]></description>
1440        <username>admin@10.1.4.233</username>
1441      </revision>
1442      <openvpn/>
1443      <l7shaper>
```

```
1444      <container/>
1445    </l7shaper>
1446    <dnshaper>
1447      <queue>
1448        <name>2MbS</name>
1449        <number/>
1450        <qlimit/>
1451        <plr/>
1452        <description><![CDATA[Para Evento LB]]></description>
1453        <bandwidth>2</bandwidth>
1454        <bandwidthtype>Mb</bandwidthtype>
1455        <enabled>on</enabled>
1456        <buckets/>
1457        <mask>srcaddress</mask>
1458        <delay>0</delay>
1459      </queue>
1460      <queue>
1461        <name>2MBD</name>
1462        <number/>
1463        <qlimit/>
1464        <plr/>
1465        <description/>
1466        <bandwidth>2</bandwidth>
1467        <bandwidthtype>Mb</bandwidthtype>
1468        <enabled>on</enabled>
1469        <buckets/>
1470        <mask>dstaddress</mask>
1471        <delay>0</delay>
1472      </queue>
1473    </dnshaper>
1474
1475    <ppps/>
1476    <gateways>
1477      <gateway_item>
1478        <interface>wan</interface>
1479        <gateway>10.1.10.253</gateway>
1480        <name>WANGW</name>
1481        <weight>1</weight>
1482        <descr><![CDATA[WAN Gateway]]></descr>
1483        <defaultgw/>
1484      </gateway_item>
1485      <gateway_item>
1486        <interface>opt3</interface>
1487        <gateway>10.1.2.254</gateway>
1488        <name>102gw</name>
1489        <weight>1</weight>
1490        <interval/>
```

```
1491        <descr/>
1492      </gateway_item>
1493      <gateway_item>
1494        <interface>opt4</interface>
1495        <gateway>10.1.3.254</gateway>
1496        <name>103gw</name>
1497        <weight>1</weight>
1498        <interval/>
1499        <descr/>
1500      </gateway_item>
1501      <gateway_item>
1502        <interface>opt5</interface>
1503        <gateway>10.1.4.254</gateway>
1504        <name>104gw</name>
1505        <weight>1</weight>
1506        <interval/>
1507        <descr/>
1508      </gateway_item>
1509      <gateway_item>
1510        <interface>opt6</interface>
1511        <gateway>10.1.5.254</gateway>
1512        <name>105gw</name>
1513        <weight>1</weight>
1514        <interval/>
1515        <descr/>
1516      </gateway_item>
1517      <gateway_item>
1518        <interface>opt7</interface>
1519        <gateway>10.1.7.254</gateway>
1520        <name>107gw</name>
1521        <weight>1</weight>
1522        <interval/>
1523        <descr/>
1524      </gateway_item>
1525      <gateway_item>
1526        <interface>opt8</interface>
1527        <gateway>10.1.8.254</gateway>
1528        <name>108gw</name>
1529        <weight>1</weight>
1530        <interval/>
1531        <descr/>
1532      </gateway_item>
1533      <gateway_item>
1534        <interface>opt9</interface>
1535        <gateway>10.1.9.254</gateway>
1536        <name>109gw</name>
1537        <weight>1</weight>
```

```
1538        <interval/>
1539        <descr/>
1540      </gateway_item>
1541      <gateway_item>
1542        <interface>opt10</interface>
1543        <gateway>10.1.10.254</gateway>
1544        <name>110gw</name>
1545        <weight>1</weight>
1546        <interval/>
1547        <descr/>
1548      </gateway_item>
1549      <gateway_item>
1550        <interface>opt1</interface>
1551        <gateway>10.1.118.254</gateway>
1552        <name>118gw</name>
1553        <weight>1</weight>
1554        <interval/>
1555        <descr/>
1556      </gateway_item>
1557      <gateway_item>
1558        <interface>opt2</interface>
1559        <gateway>10.1.251.14</gateway>
1560        <name>admin</name>
1561        <weight>1</weight>
1562        <interval/>
1563        <descr/>
1564      </gateway_item>
1565      <gateway_item>
1566        <interface>opt11</interface>
1567        <gateway>10.1.1.254</gateway>
1568        <name>gwCAM</name>
1569        <weight>1</weight>
1570        <interval/>
1571        <descr/>
1572      </gateway_item>
1573      <gateway_item>
1574        <interface>opt12</interface>
1575        <gateway>10.1.9.254</gateway>
1576        <name>gwifi</name>
1577        <weight>1</weight>
1578        <interval/>
1579        <descr/>
1580      </gateway_item>
1581      <gateway_item>
1582        <interface>opt13</interface>
1583        <gateway>10.1.23.254</gateway>
1584        <name>cisco</name>
```

```
1585        <weight>1</weight>
1586        <interval/>
1587        <descr><![CDATA[lab cisco]]></descr>
1588      </gateway_item>
1589    </gateways>
1590    <vlans>
1591      <vlan>
1592        <if>bce3</if>
1593        <tag>102</tag>
1594        <descr><![CDATA[A-PB]]></descr>
1595        <vlanif>bce3_vlan102</vlanif>
1596      </vlan>
1597      <vlan>
1598        <if>bce3</if>
1599        <tag>103</tag>
1600        <descr><![CDATA[A-PP,SP]]></descr>
1601        <vlanif>bce3_vlan103</vlanif>
1602      </vlan>
1603      <vlan>
1604        <if>bce3</if>
1605        <tag>104</tag>
1606        <descr><![CDATA[B-PB]]></descr>
1607        <vlanif>bce3_vlan104</vlanif>
1608      </vlan>
1609      <vlan>
1610        <if>bce3</if>
1611        <tag>105</tag>
1612        <descr><![CDATA[B-PP,SP]]></descr>
1613        <vlanif>bce3_vlan105</vlanif>
1614      </vlan>
1615      <vlan>
1616        <if>bce3</if>
1617        <tag>107</tag>
1618        <descr><![CDATA[C-PB,PP,SP]]></descr>
1619        <vlanif>bce3_vlan107</vlanif>
1620      </vlan>
1621      <vlan>
1622        <if>bce3</if>
1623        <tag>108</tag>
1624        <descr><![CDATA[D-PB,PP,SP]]></descr>
1625        <vlanif>bce3_vlan108</vlanif>
1626      </vlan>
1627      <vlan>
1628        <if>bce3</if>
1629        <tag>109</tag>
1630        <descr><![CDATA[JB-PB]]></descr>
1631        <vlanif>bce3_vlan109</vlanif>
```

```
1632      </vlan>
1633      <vlan>
1634        <if>bce3</if>
1635        <tag>110</tag>
1636        <descr><![CDATA[COLECCIONES]]></descr>
1637        <vlanif>bce3_vlan110</vlanif>
1638      </vlan>
1639      <vlan>
1640        <if>bce3</if>
1641        <tag>118</tag>
1642        <descr><![CDATA[wifi]]></descr>
1643        <vlanif>bce3_vlan118</vlanif>
1644      </vlan>
1645      <vlan>
1646        <if>bce3</if>
1647        <tag>399</tag>
1648        <descr><![CDATA[VlanAdmin]]></descr>
1649        <vlanif>bce3_vlan399</vlanif>
1650      </vlan>
1651      <vlan>
1652        <if>bce3</if>
1653        <tag>500</tag>
1654        <descr><![CDATA[C]]></descr>
1655        <vlanif>bce3_vlan500</vlanif>
1656      </vlan>
1657      <vlan>
1658        <if>bce3</if>
1659        <tag>66</tag>
1660        <descr><![CDATA[WIFI]]></descr>
1661        <vlanif>bce3_vlan66</vlanif>
1662      </vlan>
1663      <vlan>
1664        <if>bce3</if>
1665        <tag>23</tag>
1666        <descr><![CDATA[Laboratorio Cisco]]></descr>
1667        <vlanif>bce3_vlan23</vlanif>
1668      </vlan>
1669    </vlans>
1670    <installedpackages>
1671      <menu>
1672        <name>NMap</name>
1673        <tooltiptext>NMap is a utility for network exploration or ↩
              security auditing. It supports ping scanning (determine ↩
              which hosts are up), many port scanning techniques (↩
              determine what services the hosts are offering), version ↩
              detection (determine what application/service is runing on↩
               a port), and TCP/IP fingerprinting (remote host OS or ↩
```

```
            device identification). It also offers flexible target and↩
             port specification, decoy/stealth scanning, SunRPC ↩
            scanning, and more. Most Unix and Windows platforms are ↩
            supported in both GUI and command line modes. Several ↩
            popular handheld devices are also supported, including the↩
             Sharp Zaurus and the iPAQ.</tooltiptext>
1674        <section>Diagnostics</section>
1675        <configfile>nmap.xml</configfile>
1676      </menu>
1677      <menu>
1678        <name>phpsysinfo</name>
1679        <tooltiptext/>
1680        <section>Status</section>
1681        <url>/pkg_edit.php?xml=phpsysinfo.xml&amp;id=0</url>
1682      </menu>
1683      <menu>
1684        <name>BandwidthD</name>
1685        <tooltiptext/>
1686        <section>Services</section>
1687        <url>/pkg_edit.php?xml=bandwidthd.xml&amp;id=0</url>
1688      </menu>
1689      <menu>
1690        <name>TFTP</name>
1691        <tooltiptext>Add or Remove files for TFTP.</tooltiptext>
1692        <section>Services</section>
1693        <configfile>tftp.xml</configfile>
1694        <url>tftp_files.php</url>
1695      </menu>
1696      <menu>
1697        <name>Proxy server</name>
1698        <tooltiptext>Modify the proxy servers settings</tooltiptext>
1699        <section>Services</section>
1700        <url>/pkg_edit.php?xml=squid.xml&amp;id=0</url>
1701      </menu>
1702      <menu>
1703        <name>Dansguardian</name>
1704        <tooltiptext>Configure dansguardian</tooltiptext>
1705        <section>Services</section>
1706        <url>/pkg_edit.php?xml=dansguardian.xml</url>
1707      </menu>
1708      <service/>
1709      <service>
1710        <name>bandwidthd</name>
1711        <rcfile>bandwidthd.sh</rcfile>
1712        <executable>bandwidthd</executable>
1713      </service>
1714      <service>
```

```
1715        <name>tftp</name>
1716        <executable>inetd</executable>
1717        <description><![CDATA[Trivial File Transport Protocol is a ↩
                very simple file transfer protocol. Often used with ↩
                routers, voip phones and more.]]></description>
1718      </service>
1719      <service>
1720        <name>squid</name>
1721        <rcfile>squid.sh</rcfile>
1722        <executable>squid</executable>
1723        <description><![CDATA[Proxy server Service]]></description>
1724      </service>
1725      <service>
1726        <name>dansguardian</name>
1727        <rcfile>dansguardian</rcfile>
1728        <executable>dansguardian</executable>
1729        <description><![CDATA[Award winning Open Source web content ↩
                filter]]></description>
1730      </service>
1731      <package>
1732        <name>nmap</name>
1733        <maintainer>jimp@pfsense.org</maintainer>
1734        <descr><![CDATA[NMap is a utility for network exploration or ↩
                security auditing. It supports ping scanning (determine ↩
                which hosts are up), many port scanning techniques (↩
                determine what services the hosts are offering), version ↩
                detection (determine what application/service is runing on↩
                 a port), and TCP/IP fingerprinting (remote host OS or ↩
                device identification). It also offers flexible target and↩
                 port specification, decoy/stealth scanning, SunRPC ↩
                scanning, and more. Most Unix and Windows platforms are ↩
                supported in both GUI and command line modes. Several ↩
                popular handheld devices are also supported, including the↩
                 Sharp Zaurus and the iPAQ.]]></descr>
1735        <category>Security</category>
1736        <depends_on_package_base_url>http://files.pfsense.org/↩
                packages/amd64/8/All/</depends_on_package_base_url>
1737        <depends_on_package>lua-5.1.5_4.tbz</depends_on_package>
1738        <depends_on_package>nmap-6.01.tbz</depends_on_package>
1739        <depends_on_package>libpcap-1.2.1.tbz</depends_on_package>
1740        <depends_on_package_pbi>nmap-6.01_1-amd64.pbi</↩
                depends_on_package_pbi>
1741        <config_file>http://www.pfsense.com/packages/config/nmap/nmap↩
                .xml</config_file>
1742        <version>nmap-6.01 pkg v1.2</version>
1743        <status>Stable</status>
```

```
1744        <pkginfolink>http://doc.pfsense.org/index.php/Nmap_package</↩
                pkginfolink>
1745        <required_version>2.0</required_version>
1746        <configurationfile>nmap.xml</configurationfile>
1747        <build_port_path>/usr/ports/security/nmap</build_port_path>
1748      </package>
1749      <package>
1750        <name>phpSysInfo</name>
1751        <website>http://phpsysinfo.sourceforge.net/</website>
1752        <descr><![CDATA[PHPSysInfo is a customizable PHP Script that ↩
                parses /proc, and formats information nicely. It will ↩
                display information about system facts like Uptime, CPU, ↩
                Memory, PCI devices, SCSI devices, IDE devices, Network ↩
                adapters, Disk usage, and more.]]></descr>
1753        <category>System</category>
1754        <version>2.5.4</version>
1755        <status>Beta</status>
1756        <required_version>1.0</required_version>
1757        <depends_on_package_base_url>http://files.pfsense.org/↩
                packages/amd64/8/All/</depends_on_package_base_url>
1758        <depends_on_package>mbmon-205_5.tbz</depends_on_package>
1759        <depends_on_package_pbi>mbmon-205_6-amd64.pbi</↩
                depends_on_package_pbi>
1760        <build_port_path>/usr/ports/sysutils/mbmon</build_port_path>
1761        <config_file>http://www.pfsense.com/packages/config/↩
                phpsysinfo/phpsysinfo.xml</config_file>
1762        <configurationfile>phpsysinfo.xml</configurationfile>
1763        <noembedded>true</noembedded>
1764      </package>
1765      <package>
1766        <name>bandwidthd</name>
1767        <website>http://bandwidthd.sourceforge.net/</website>
1768        <descr><![CDATA[BandwidthD tracks usage of TCP/IP network ↩
                subnets and builds html files with graphs to display ↩
                utilization. Charts are built by individual IPs, and by ↩
                default display utilization over 2 day, 8 day, 40 day, and↩
                 400 day periods. Furthermore, each ip address utilization↩
                 can be logged out at intervals of 3.3 minutes, 10 minutes↩
                , 1 hour or 12 hours in cdf format, or to a backend ↩
                database server. HTTP, TCP, UDP, ICMP, VPN, and P2P ↩
                traffic are color coded.]]></descr>
1769        <category>System</category>
1770        <version>2.0.1_5</version>
1771        <status>BETA</status>
1772        <required_version>1.2.1</required_version>
1773        <depends_on_package_base_url>http://files.pfsense.org/↩
                packages/amd64/8/All/</depends_on_package_base_url>
```

```
1774        <depends_on_package>bandwidthd-2.0.1_5.tbz</depends_on_package>
1775        <depends_on_package>libpcap-1.1.1.tbz</depends_on_package>
1776        <depends_on_package>postgresql-client-8.4.12.tbz</depends_on_package>
1777        <depends_on_package_pbi>bandwidthd-2.0.1_5-amd64.pbi</depends_on_package_pbi>
1778        <config_file>http://www.pfsense.org/packages/config/bandwidthd/bandwidthd.xml</config_file>
1779        <configurationfile>bandwidthd.xml</configurationfile>
1780        <build_port_path>/usr/ports/net/libpcap</build_port_path>
1781        <build_port_path>/usr/ports/databases/postgresql84-client</build_port_path>
1782        <build_port_path>/usr/ports/net-mgmt/bandwidthd</build_port_path>
1783        <build_pbi>
1784          <ports_before>net/libpcap databases/postgresql91-client graphics/gd</ports_before>
1785          <port>net-mgmt/bandwidthd</port>
1786        </build_pbi>
1787        <build_options>WITH_NLS=true;WITHOUT_PAM=true;WITHOUT_LDAP=true;WITHOUT_MIT_KRB5=true;WITHOUT_HEIMDAL_KRB5=true;WITHOUT_OPTIMIZED_CFLAGS=true;WITHOUT_XML=true;WITHOUT_TZDATA=true;WITHOUT_DEBUG=true;WITHOUT_GSSAPI=true;WITHOUT_ICU=true;WITH_INTDATE=true</build_options>
1788      </package>
1789      <package>
1790        <name>TFTP</name>
1791        <website/>
1792        <descr><![CDATA[Trivial File Transport Protocol is a very simple file transfer protocol. Often used with routers, voip phones and more.]]></descr>
1793        <category>Services</category>
1794        <pkginfolink/>
1795        <config_file>http://www.pfsense.com/packages/config/tftp2/tftp.xml</config_file>
1796        <depends_on_package_base_url>http://files.pfsense.org/packages/amd64/8/All/</depends_on_package_base_url>
1797        <version>2.0</version>
1798        <status>Stable</status>
1799        <required_version>2.0</required_version>
1800        <configurationfile>tftp.xml</configurationfile>
1801        <filter_rule_function>tftp_generate_rules</filter_rule_function>
1802      </package>
1803      <package>
1804        <name>squid</name>
```

```
1805        <descr><![CDATA[High performance web proxy cache.]]></descr>
1806        <website>http://www.squid-cache.org/</website>
1807        <category>Network</category>
1808        <version>2.7.9 pkg v.4.3.3</version>
1809        <status>Stable</status>
1810        <required_version>2</required_version>
1811        <maintainer>fernando@netfilter.com.br seth.mos@dds.nl ↩
               mfuchs77@googlemail.com jimp@pfsense.org</maintainer>
1812        <depends_on_package_base_url>http://files.pfsense.org/↩
               packages/amd64/8/All/</depends_on_package_base_url>
1813        <depends_on_package>squid-2.7.9_3.tbz</depends_on_package>
1814        <depends_on_package>squid_radius_auth-1.10.tbz</↩
               depends_on_package>
1815        <depends_on_package>libwww-5.4.0_4.tbz</depends_on_package>
1816        <depends_on_package_pbi>squid-2.7.9_3-amd64.pbi</↩
               depends_on_package_pbi>
1817        <build_port_path>/usr/ports/www/squid</build_port_path>
1818        <build_port_path>/usr/ports/www/squid_radius_auth</↩
               build_port_path>
1819        <build_port_path>/usr/ports/www/libwww</build_port_path>
1820        <build_pbi>
1821          <ports_before>www/libwww</ports_before>
1822          <port>www/squid</port>
1823          <ports_after>www/squid_radius_auth</ports_after>
1824        </build_pbi>
1825        <build_options>squid_UNSET=DNS_HELPER IPFILTER PINGER ↩
               STACKTRACES STRICT_HTTP_DESC USERAGENT_LOG WCCPV2;↩
               squid_SET=PF LDAP_AUTH NIS_AUTH SASL_AUTH ARP_ACL AUFS ↩
               CACHE_DIGESTS CARP COSS DELAY_POOLS FOLLOW_XFF HTCP IDENT ↩
               KERB_AUTH KQUEUE LARGEFILE REFERER_LOG SNMP SSL VIA_DB ↩
               WCCP;SQUID_UID=proxy;SQUID_GID=proxy</build_options>
1826        <config_file>http://www.pfsense.org/packages/config/squid/↩
               squid.xml</config_file>
1827        <configurationfile>squid.xml</configurationfile>
1828      </package>
1829      <package>
1830        <name>Dansguardian</name>
1831        <website>http://www.dansguardian.org/</website>
1832        <descr><![CDATA[DansGuardian is an award winning Open Source ↩
               web content filter.&lt;br /&gt;
1833             It filters the actual content of pages based on many ↩
                    methods including phrase matching, PICS filtering ↩
                    and URL filtering.&lt;br /&gt;
1834             It does not purely filter based on a banned list of ↩
                    sites like lesser totally commercial filters.&lt;br ↩
                    /&gt;
```

```
1835            For all non-commercial its free, without cost.&lt;br /&gt;
                For all commercial use visit dansguardian website to get a licence.]]></descr>
1837        <category>Services</category>
1838        <config_file>http://www.pfsense.com/packages/config/dansguardian/dansguardian.xml</config_file>
1839        <pkginfolink>http://forum.pfsense.org/index.php/topic,43786.0.html</pkginfolink>
1840        <depends_on_package_base_url>http://files.pfsense.org/packages/amd64/8/All/</depends_on_package_base_url>
1841        <depends_on_package>dansguardian-2.12.0.3.tbz</depends_on_package>
1842        <depends_on_package>ca_root_nss-3.14.1.tbz</depends_on_package>
1843        <depends_on_package_pbi>dansguardian-2.12.0.3-amd64.pbi</depends_on_package_pbi>
1844        <version>2.12.0.3 pkg v.0.1.8</version>
1845        <status>beta</status>
1846        <required_version>2.0</required_version>
1847        <configurationfile>dansguardian.xml</configurationfile>
1848        <build_port_path>/usr/ports/www/dansguardian-devel</build_port_path>
1849        <build_port_path>/usr/ports/www/ca_root_nss</build_port_path>
1850        <build_options>dansguardian-devel_UNSET=APACHE;dansguardian-devel_SET=TRICKLE CLAMD ICAP NTLM SSL</build_options>
1851      </package>
1852      <phpsysinfo>
1853        <config>
1854          <hidepicklist/>
1855          <sensorprogram/>
1856          <showmountpoint>on</showmountpoint>
1857          <showinodes>on</showinodes>
1858          <loadbar>on</loadbar>
1859          <showerrors/>
1860        </config>
1861      </phpsysinfo>
1862      <bandwidthd>
1863        <config>
1864          <enable>on</enable>
1865          <active_interface>wan</active_interface>
1866          <subnets_custom>10.1.0.0/16</subnets_custom>
1867          <skipintervals/>
1868          <graphcutoff/>
1869          <promiscuous>on</promiscuous>
1870          <outputcdf/>
1871          <recovercdf>on</recovercdf>
```

```
1872          <filter/>
1873          <drawgraphs>on</drawgraphs>
1874          <meta_refresh/>
1875          <graph_log_info/>
1876        </config>
1877      </bandwidthd>
1878      <tab>
1879        <text>General</text>
1880        <url>/pkg_edit.php?xml=squid.xml&amp;id=0</url>
1881        <active/>
1882      </tab>
1883      <dansguardian>
1884        <config>
1885          <interface>lo0</interface>
1886          <daemon_options>softrestart</daemon_options>
1887        </config>
1888      </dansguardian>
1889      <dansguardianconfig>
1890        <config>
1891          <auth_plugin/>
1892          <scan_options>scancleancache,createlistcachefiles,↩
                deletedownloadedtempfiles</scan_options>
1893          <weightedphrasemode>2</weightedphrasemode>
1894          <preservecase>0</preservecase>
1895          <phrasefiltermode>2</phrasefiltermode>
1896          <cron>day</cron>
1897        </config>
1898      </dansguardianconfig>
1899      <dansguardianlog>
1900        <config>
1901          <report_level>3</report_level>
1902          <report_language>ukenglish</report_language>
1903          <report_options>showweightedfound,usecustombannedimage,↩
                nonstandarddelimiter</report_options>
1904          <logging_options>logconnectionhandlingerrors</↩
                logging_options>
1905          <loglevel>2</loglevel>
1906          <logexceptionhits>2</logexceptionhits>
1907          <logfileformat>1</logfileformat>
1908          </config>
1909      </dansguardianips>
1910      <dansguardiangroups>
1911        <config>
1912          <name>Default</name>
1913          <description><![CDATA[Default dansguardian filtergroup]]></↩
                description>
1914          <picsacl>Default</picsacl>
```

```
1915          <phraseacl>Default</phraseacl>
1916          <siteacl>Default</siteacl>
1917          <extensionacl>Default</extensionacl>
1918          <headeracl>Default</headeracl>
1919          <contentacl>Default</contentacl>
1920          <searchacl>Default</searchacl>
1921          <urlacl>Default</urlacl>
1922          <group_options>scancleancache,infectionbypasserrorsonly</↩
                  group_options>
1923          <reportinglevel>3</reportinglevel>
1924          <group_name_source>name</group_name_source>
1925          <mode>1</mode>
1926          <report_level>global</report_level>
1927        </config>
1928      </dansguardiangroups>
1929      <dansguardianphraselistsweighted>
1930        <config>
1931          <descr><![CDATA[badwords weighted_dutch]]></descr>
1932          <list>badwords</list>
1933          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  badwords/weighted_dutch</file>
1934        </config>
1935        <config>
1936          <descr><![CDATA[badwords weighted_french]]></descr>
1937          <list>badwords</list>
1938          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  badwords/weighted_french</file>
1939        </config>
1940        <config>
1941          <descr><![CDATA[badwords weighted_german]]></descr>
1942          <list>badwords</list>
1943          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  badwords/weighted_german</file>
1944        </config>
1945        <config>
1946          <descr><![CDATA[badwords weighted_portuguese]]></descr>
1947          <list>badwords</list>
1948          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  badwords/weighted_portuguese</file>
1949        </config>
1950        <config>
1951          <descr><![CDATA[badwords weighted_spanish]]></descr>
1952          <list>badwords</list>
1953          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  badwords/weighted_spanish</file>
1954        </config>
1955        <config>
```

```
1956          <descr><![CDATA[chat weighted]]></descr>
1957          <list>chat</list>
1958          <file>/usr/local/etc/dansguardian/lists/phraselists/chat/↩
                 weighted</file>
1959        </config>
1960        <config>
1961          <descr><![CDATA[chat weighted_italian]]></descr>
1962          <list>chat</list>
1963          <file>/usr/local/etc/dansguardian/lists/phraselists/chat/↩
                 weighted_italian</file>
1964        </config>
1965        <config>
1966          <descr><![CDATA[conspiracy weighted]]></descr>
1967          <list>conspiracy</list>
1968          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 conspiracy/weighted</file>
1969        </config>
1970        <config>
1971          <descr><![CDATA[domainsforsale weighted]]></descr>
1972          <list>domainsforsale</list>
1973          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 domainsforsale/weighted</file>
1974        </config>
1975        <config>
1976          <descr><![CDATA[drugadvocacy weighted]]></descr>
1977          <list>drugadvocacy</list>
1978          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 drugadvocacy/weighted</file>
1979        </config>
1980        <config>
1981          <descr><![CDATA[forums weighted]]></descr>
1982          <list>forums</list>
1983          <file>/usr/local/etc/dansguardian/lists/phraselists/forums/↩
                 weighted</file>
1984        </config>
1985        <config>
1986          <descr><![CDATA[gambling weighted]]></descr>
1987          <list>gambling</list>
1988          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 gambling/weighted</file>
1989        </config>
1990        <config>
1991          <descr><![CDATA[gambling weighted_portuguese]]></descr>
1992          <list>gambling</list>
1993          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 gambling/weighted_portuguese</file>
1994        </config>
```

```
1995        <config>
1996          <descr><![CDATA[games weighted]]></descr>
1997          <list>games</list>
1998          <file>/usr/local/etc/dansguardian/lists/phraselists/games/↩
                weighted</file>
1999        </config>
2000        <config>
2001          <descr><![CDATA[goodphrases weighted_general]]></descr>
2002          <list>goodphrases</list>
2003          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                goodphrases/weighted_general</file>
2004        </config>
2005        <config>
2006          <descr><![CDATA[goodphrases weighted_general_danish]]></↩
                descr>
2007          <list>goodphrases</list>
2008          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                goodphrases/weighted_general_danish</file>
2009        </config>
2010        <config>
2011          <descr><![CDATA[goodphrases weighted_general_dutch]]></↩
                descr>
2012          <list>goodphrases</list>
2013          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                goodphrases/weighted_general_dutch</file>
2014        </config>
2015        <config>
2016          <descr><![CDATA[goodphrases weighted_general_malay]]></↩
                descr>
2017          <list>goodphrases</list>
2018          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                goodphrases/weighted_general_malay</file>
2019        </config>
2020        <config>
2021          <descr><![CDATA[goodphrases weighted_general_polish]]></↩
                descr>
2022          <list>goodphrases</list>
2023          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                goodphrases/weighted_general_polish</file>
2024        </config>
2025        <config>
2026          <descr><![CDATA[goodphrases weighted_general_portuguese]]><↩
                /descr>
2027          <list>goodphrases</list>
2028          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                goodphrases/weighted_general_portuguese</file>
2029        </config>
```

```
2030        <config>
2031          <descr><![CDATA[goodphrases weighted_general_swedish]]></descr>
2032          <list>goodphrases</list>
2033          <file>/usr/local/etc/dansguardian/lists/phraselists/goodphrases/weighted_general_swedish</file>
2034        </config>
2035        <config>
2036          <descr><![CDATA[goodphrases weighted_news]]></descr>
2037          <list>goodphrases</list>
2038          <file>/usr/local/etc/dansguardian/lists/phraselists/goodphrases/weighted_news</file>
2039        </config>
2040        <config>
2041          <descr><![CDATA[gore weighted]]></descr>
2042          <list>gore</list>
2043          <file>/usr/local/etc/dansguardian/lists/phraselists/gore/weighted</file>
2044        </config>
2045        <config>
2046          <descr><![CDATA[gore weighted_portuguese]]></descr>
2047          <list>gore</list>
2048          <file>/usr/local/etc/dansguardian/lists/phraselists/gore/weighted_portuguese</file>
2049        </config>
2050        <config>
2051          <descr><![CDATA[idtheft weighted]]></descr>
2052          <list>idtheft</list>
2053          <file>/usr/local/etc/dansguardian/lists/phraselists/idtheft/weighted</file>
2054        </config>
2055        <config>
2056          <descr><![CDATA[illegaldrugs weighted]]></descr>
2057          <list>illegaldrugs</list>
2058          <file>/usr/local/etc/dansguardian/lists/phraselists/illegaldrugs/weighted</file>
2059        </config>
2060        <config>
2061          <descr><![CDATA[illegaldrugs weighted_portuguese]]></descr>
2062          <list>illegaldrugs</list>
2063          <file>/usr/local/etc/dansguardian/lists/phraselists/illegaldrugs/weighted_portuguese</file>
2064        </config>
2065        <config>
2066          <descr><![CDATA[intolerance weighted]]></descr>
2067          <list>intolerance</list>
```

```
2068          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 intolerance/weighted</file>
2069        </config>
2070        <config>
2071          <descr><![CDATA[intolerance weighted_portuguese]]></descr>
2072          <list>intolerance</list>
2073          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 intolerance/weighted_portuguese</file>
2074        </config>
2075        <config>
2076          <descr><![CDATA[legaldrugs weighted]]></descr>
2077          <list>legaldrugs</list>
2078          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 legaldrugs/weighted</file>
2079        </config>
2080        <config>
2081          <descr><![CDATA[malware weighted]]></descr>
2082          <list>malware</list>
2083          <file>/usr/local/etc/dansguardian/lists/phraselists/malware↩
                 /weighted</file>
2084        </config>
2085        <config>
2086          <descr><![CDATA[music weighted]]></descr>
2087          <list>music</list>
2088          <file>/usr/local/etc/dansguardian/lists/phraselists/music/↩
                 weighted</file>
2089        </config>
2090        <config>
2091          <descr><![CDATA[news weighted]]></descr>
2092          <list>news</list>
2093          <file>/usr/local/etc/dansguardian/lists/phraselists/news/↩
                 weighted</file>
2094        </config>
2095        <config>
2096          <descr><![CDATA[nudism weighted]]></descr>
2097          <list>nudism</list>
2098          <file>/usr/local/etc/dansguardian/lists/phraselists/nudism/↩
                 weighted</file>
2099        </config>
2100        <config>
2101          <descr><![CDATA[peer2peer weighted]]></descr>
2102          <list>peer2peer</list>
2103          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 peer2peer/weighted</file>
2104        </config>
2105        <config>
2106          <descr><![CDATA[personals weighted]]></descr>
```

```
2107          <list>personals</list>
2108          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  personals/weighted</file>
2109        </config>
2110        <config>
2111          <descr><![CDATA[personals weighted_portuguese]]></descr>
2112          <list>personals</list>
2113          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  personals/weighted_portuguese</file>
2114        </config>
2115        <config>
2116          <descr><![CDATA[pornography weighted]]></descr>
2117          <list>pornography</list>
2118          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted</file>
2119        </config>
2120        <config>
2121          <descr><![CDATA[pornography weighted_chinese]]></descr>
2122          <list>pornography</list>
2123          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_chinese</file>
2124        </config>
2125        <config>
2126          <descr><![CDATA[pornography weighted_danish]]></descr>
2127          <list>pornography</list>
2128          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_danish</file>
2129        </config>
2130        <config>
2131          <descr><![CDATA[pornography weighted_dutch]]></descr>
2132          <list>pornography</list>
2133          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_dutch</file>
2134        </config>
2135        <config>
2136          <descr><![CDATA[pornography weighted_french]]></descr>
2137          <list>pornography</list>
2138          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_french</file>
2139        </config>
2140        <config>
2141          <descr><![CDATA[pornography weighted_german]]></descr>
2142          <list>pornography</list>
2143          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_german</file>
2144        </config>
2145        <config>
```

```
2146          <descr><![CDATA[pornography weighted_italian]]></descr>
2147          <list>pornography</list>
2148          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_italian</file>
2149        </config>
2150        <config>
2151          <descr><![CDATA[pornography weighted_japanese]]></descr>
2152          <list>pornography</list>
2153          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_japanese</file>
2154        </config>
2155        <config>
2156          <descr><![CDATA[pornography weighted_malay]]></descr>
2157          <list>pornography</list>
2158          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_malay</file>
2159        </config>
2160        <config>
2161          <descr><![CDATA[pornography weighted_norwegian]]></descr>
2162          <list>pornography</list>
2163          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_norwegian</file>
2164        </config>
2165        <config>
2166          <descr><![CDATA[pornography weighted_polish]]></descr>
2167          <list>pornography</list>
2168          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_polish</file>
2169        </config>
2170        <config>
2171          <descr><![CDATA[pornography weighted_portuguese]]></descr>
2172          <list>pornography</list>
2173          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_portuguese</file>
2174        </config>
2175        <config>
2176          <descr><![CDATA[pornography weighted_russian]]></descr>
2177          <list>pornography</list>
2178          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_russian</file>
2179        </config>
2180        <config>
2181          <descr><![CDATA[pornography weighted_russian_utf8]]></descr↩
                 >
2182          <list>pornography</list>
2183          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_russian_utf8</file>
```

```
2184        </config>
2185        <config>
2186          <descr><![CDATA[pornography weighted_spanish]]></descr>
2187          <list>pornography</list>
2188          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                pornography/weighted_spanish</file>
2189        </config>
2190        <config>
2191          <descr><![CDATA[pornography weighted_swedish]]></descr>
2192          <list>pornography</list>
2193          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                pornography/weighted_swedish</file>
2194        </config>
2195        <config>
2196          <descr><![CDATA[proxies weighted]]></descr>
2197          <list>proxies</list>
2198          <file>/usr/local/etc/dansguardian/lists/phraselists/proxies↩
                /weighted</file>
2199        </config>
2200        <config>
2201          <descr><![CDATA[secretsocieties weighted]]></descr>
2202          <list>secretsocieties</list>
2203          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                secretsocieties/weighted</file>
2204        </config>
2205        <config>
2206          <descr><![CDATA[sport weighted]]></descr>
2207          <list>sport</list>
2208          <file>/usr/local/etc/dansguardian/lists/phraselists/sport/↩
                weighted</file>
2209        </config>
2210        <config>
2211          <descr><![CDATA[translation weighted]]></descr>
2212          <list>translation</list>
2213          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                translation/weighted</file>
2214        </config>
2215        <config>
2216          <descr><![CDATA[travel weighted]]></descr>
2217          <list>travel</list>
2218          <file>/usr/local/etc/dansguardian/lists/phraselists/travel/↩
                weighted</file>
2219        </config>
2220        <config>
2221          <descr><![CDATA[upstreamfilter weighted]]></descr>
2222          <list>upstreamfilter</list>
```

```
2223          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 upstreamfilter/weighted</file>
2224        </config>
2225        <config>
2226          <descr><![CDATA[violence weighted]]></descr>
2227          <list>violence</list>
2228          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 violence/weighted</file>
2229        </config>
2230        <config>
2231          <descr><![CDATA[violence weighted_portuguese]]></descr>
2232          <list>violence</list>
2233          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 violence/weighted_portuguese</file>
2234        </config>
2235        <config>
2236          <descr><![CDATA[warezhacking weighted]]></descr>
2237          <list>warezhacking</list>
2238          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 warezhacking/weighted</file>
2239        </config>
2240        <config>
2241          <descr><![CDATA[weapons weighted]]></descr>
2242          <list>weapons</list>
2243          <file>/usr/local/etc/dansguardian/lists/phraselists/weapons↩
                 /weighted</file>
2244        </config>
2245        <config>
2246          <descr><![CDATA[weapons weighted_portuguese]]></descr>
2247          <list>weapons</list>
2248          <file>/usr/local/etc/dansguardian/lists/phraselists/weapons↩
                 /weighted_portuguese</file>
2249        </config>
2250        <config>
2251          <descr><![CDATA[webmail weighted]]></descr>
2252          <list>webmail</list>
2253          <file>/usr/local/etc/dansguardian/lists/phraselists/webmail↩
                 /weighted</file>
2254        </config>
2255      </dansguardianphraselistsweighted>
2256      <dansguardianphraselistsbanned>
2257        <config>
2258          <descr><![CDATA[gambling banned]]></descr>
2259          <list>gambling</list>
2260          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 gambling/banned</file>
2261        </config>
```

```
2262        <config>
2263          <descr><![CDATA[gambling banned_portuguese]]></descr>
2264          <list>gambling</list>
2265          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 gambling/banned_portuguese</file>
2266        </config>
2267        <config>
2268          <descr><![CDATA[googlesearches banned]]></descr>
2269          <list>googlesearches</list>
2270          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 googlesearches/banned</file>
2271        </config>
2272        <config>
2273          <descr><![CDATA[illegaldrugs banned]]></descr>
2274          <list>illegaldrugs</list>
2275          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 illegaldrugs/banned</file>
2276        </config>
2277        <config>
2278          <descr><![CDATA[intolerance banned_portuguese]]></descr>
2279          <list>intolerance</list>
2280          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 intolerance/banned_portuguese</file>
2281        </config>
2282        <config>
2283          <descr><![CDATA[pornography banned]]></descr>
2284          <list>pornography</list>
2285          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/banned</file>
2286        </config>
2287        <config>
2288          <descr><![CDATA[pornography banned_portuguese]]></descr>
2289          <list>pornography</list>
2290          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/banned_portuguese</file>
2291        </config>
2292        <config>
2293          <descr><![CDATA[rta banned]]></descr>
2294          <list>rta</list>
2295          <file>/usr/local/etc/dansguardian/lists/phraselists/rta/↩
                 banned</file>
2296        </config>
2297        <config>
2298          <descr><![CDATA[safelabel banned]]></descr>
2299          <list>safelabel</list>
2300          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 safelabel/banned</file>
```

```
2301        </config>
2302      </dansguardianphraselistsbanned>
2303      <dansguardianphraselistsexception>
2304        <config>
2305          <descr><![CDATA[goodphrases exception]]></descr>
2306          <list>goodphrases</list>
2307          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                goodphrases/exception</file>
2308        </config>
2309        <config>
2310          <descr><![CDATA[goodphrases exception_email]]></descr>
2311          <list>goodphrases</list>
2312          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                goodphrases/exception_email</file>
2313        </config>
2314      </dansguardianphraselistsexception>
2315      <dansguardianblacklistsdomains>
2316        <config>
2317          <descr><![CDATA[ads domains]]></descr>
2318          <list>ads</list>
2319          <file>/usr/local/etc/dansguardian/lists/blacklists/ads/↩
                domains</file>
2320        </config>
2321      </dansguardianblacklistsdomains>
2322      <dansguardianblacklistsurls>
2323        <config>
2324          <descr><![CDATA[ads urls]]></descr>
2325          <list>ads</list>
2326          <file>/usr/local/etc/dansguardian/lists/blacklists/ads/urls↩
                </file>
2327        </config>
2328      </dansguardianblacklistsurls>
2329    </installedpackages>
2330    <dhcrelay/>
2331
2332      <allowedip>
2333        <ip>132.248.x.y</ip>
2334        <sn>32</sn>
2335        <dir>both</dir>
2336        <descr><![CDATA[ibiologia]]></descr>
2337        <bw_up>1000</bw_up>
2338        <bw_down>1000</bw_down>
2339      </allowedip>
2340      <allowedip>
2341        <ip>132.248.x.y</ip>
2342        <sn>32</sn>
2343        <dir>both</dir>
```

```
2344        <descr><![CDATA[apoyo.ibiologia]]></descr>
2345        <bw_up>1000</bw_up>
2346        <bw_down>1000</bw_down>
2347      </allowedip>
2348      <allowedip>
2349        <ip>132.248.x.y</ip>
2350        <sn>32</sn>
2351        <dir>both</dir>
2352        <descr><![CDATA[web]]></descr>
2353        <bw_up>1000</bw_up>
2354        <bw_down>1000</bw_down>
2355      </allowedip>
2356      <interface>opt1</interface>
2357      <timeout/>
2358      <idletimeout/>
2359      <freelogins_count/>
2360      <freelogins_resettimeout/>
2361      <auth_method>none</auth_method>
2362      <reauthenticateacct/>
2363      <httpsname/>
2364      <preauthurl/>
2365      <bwdefaultdn/>
2366      <bwdefaultup/>
2367      <certificate/>
2368      <cacertificate/>
2369      <private-key/>
2370      <redirurl/>
2371      <radiusip/>
2372      <radiusip2/>
2373      <radiusport/>
2374      <radiusport2/>
2375      <radiusacctport/>
2376      <radiuskey/>
2377      <radiuskey2/>
2378      <radiusvendor>default</radiusvendor>
2379      <radiussrcip_attribute>wan</radiussrcip_attribute>
2380      <radmac_format>default</radmac_format>
2381      <page>
2382        <htmltext>PEhUTUw+↩
              CjxIRUFEPgoKPFRJVExFPnJlZGlyZWN0PC9USVRMRT4KPE1FVEEgSFRUUC1FUVVJV↩

2383        j0icmVmcmVzaCIgCkNPTlRFTlQ9IjA7VVJMPWh0dHA6Ly9hcG95by5pYmlvbG9naWEudW5hbS5teC

2384        pL3VwbG9hZC9pbmRleC5waHAiPgo8L0hFQUQ+↩
              CjxCT0RZPgpSZWRpcmVjY2lvbmFuZG8
2385        uLgo8L2E+LiAKPC9CT0RZPgo8L0hUTUw+Cg==</htmltext>
2386      </page>
```

```
2387      <enable/>
2388    </captiveportal>
2389    <ezshaper>
2390      <step1>
2391        <numberofconnections>5</numberofconnections>
2392      </step1>
2393    </ezshaper>
2394  </pfsense>
2395      <item>
2396        <descr><![CDATA[Do not send ICMP port unreachable messages ↩
              for closed UDP ports]]></descr>
2397        <tunable>net.inet.udp.blackhole</tunable>
2398        <value>default</value>
2399      </item>
2400      <item>
2401        <descr><![CDATA[Randomize the ID field in IP packets (default↩
               is 0: sequential IP IDs)]]></descr>
2402        <tunable>net.inet.ip.random_id</tunable>
2403        <value>default</value>
2404      </item>
2405      <item>
2406        <descr><![CDATA[Drop SYN-FIN packets (breaks RFC1379, but ↩
              nobody uses it anyway)]]></descr>
2407        <tunable>net.inet.tcp.drop_synfin</tunable>
2408        <value>default</value>
2409      </item>
2410      <item>
2411        <descr><![CDATA[Enable sending IPv8 redirects]]></descr>
2412        <tunable>net.inet.ip.redirect</tunable>
2413        <value>default</value>
2414      </item>
2415      <item>
2416        <descr><![CDATA[Enable sending IPv6 redirects]]></descr>
2417        <tunable>net.inet6.ip6.redirect</tunable>
2418        <value>default</value>
2419      </item>
2420      <item>
2421        <descr><![CDATA[Generate SYN cookies for outbound SYN-ACK ↩
              packets]]></descr>
2422        <tunable>net.inet.tcp.syncookies</tunable>
2423        <value>default</value>
2424      </item>
2425      <item>
2426        <descr><![CDATA[Maximum incoming/outgoing TCP datagram size (↩
              receive)]]></descr>
2427        <tunable>net.inet.tcp.recvspace</tunable>
2428        <value>default</value>
```

```
2429      </item>
2430      <item>
2431        <descr><![CDATA[Maximum incoming/outgoing TCP datagram size (↩
              send)]]></descr>
2432        <tunable>net.inet.tcp.sendspace</tunable>
2433        <value>default</value>
2434      </item>
2435      <item>
2436        <descr><![CDATA[IP Fastforwarding]]></descr>
2437        <tunable>net.inet.ip.fastforwarding</tunable>
2438        <value>default</value>
2439      </item>
2440      <item>
2441        <descr><![CDATA[Do not delay ACK to try and piggyback it onto↩
              a data packet]]></descr>
2442        <tunable>net.inet.tcp.delayed_ack</tunable>
2443        <value>default</value>
2444      </item>
2445      <item>
2446        <descr><![CDATA[Maximum outgoing UDP datagram size]]></descr>
2447        <tunable>net.inet.udp.maxdgram</tunable>
2448        <value>default</value>
2449      </item>
2450      <item>
2451        <descr><![CDATA[Handling of non-IP packets which are not ↩
              passed to pfil (see if_bridge(8))]]></descr>
2452        <tunable>net.link.bridge.pfil_onlyip</tunable>
2453        <value>default</value>
2454      </item>
2455      <item>
2456        <descr><![CDATA[Set to 0 to disable filtering on the incoming↩
              and outgoing member interfaces.]]></descr>
2457        <tunable>net.link.bridge.pfil_member</tunable>
2458        <value>default</value>
2459      </item>
2460      <item>
2461        <descr><![CDATA[Set to 1 to enable filtering on the bridge ↩
              interface]]></descr>
2462        <tunable>net.link.bridge.pfil_bridge</tunable>
2463        <value>default</value>
2464      </item>
2465      <item>
2466        <descr><![CDATA[Allow unprivileged access to tap(8) device ↩
              nodes]]></descr>
2467        <tunable>net.link.tap.user_open</tunable>
2468        <value>default</value>
2469      </item>
```

```
2470      <item>
2471        <descr><![CDATA[Randomize PIDs (see src/sys/kern/kern_fork.c:↩
              sysctl_kern_randompid())]]></descr>
2472        <tunable>kern.randompid</tunable>
2473        <value>default</value>
2474      </item>
2475      <item>
2476        <descr><![CDATA[Maximum size of the IP input queue]]></descr>
2477        <tunable>net.inet.ip.intr_queue_maxlen</tunable>
2478        <value>default</value>
2479      </item>
2480      <item>
2481        <descr><![CDATA[Disable CTRL+ALT+Delete reboot from keyboard.↩
            ]]></descr>
2482        <tunable>hw.syscons.kbd_reboot</tunable>
2483        <value>default</value>
2484      </item>
2485      <item>
2486        <descr><![CDATA[Enable TCP Inflight mode]]></descr>
2487        <tunable>net.inet.tcp.inflight.enable</tunable>
2488        <value>default</value>
2489      </item>
2490      <item>
2491        <descr><![CDATA[Enable TCP extended debugging]]></descr>
2492        <tunable>net.inet.tcp.log_debug</tunable>
2493        <value>default</value>
2494      </item>
2495      <item>
2496        <descr><![CDATA[Set ICMP Limits]]></descr>
2497        <tunable>net.inet.icmp.icmplim</tunable>
2498        <value>default</value>
2499      </item>
2500      <item>
2501        <descr><![CDATA[TCP Offload Engine]]></descr>
2502        <tunable>net.inet.tcp.tso</tunable>
2503        <value>default</value>
2504      </item>
2505      <item>
2506        <descr><![CDATA[Maximum socket buffer size]]></descr>
2507        <tunable>kern.ipc.maxsockbuf</tunable>
2508        <value>default</value>
2509      </item>
2510    </sysctl>
2511    <system>
2512      <optimization>normal</optimization>
2513      <hostname>darwin</hostname>
2514      <domain>ib.unam.mx</domain>
```

```
2515      <group>
2516        <name>all</name>
2517        <description><![CDATA[All Users]]></description>
2518        <scope>system</scope>
2519        <gid>1998</gianalisis yd>
2520      </group>
2521      <group>
2522        <name>admins</name>
2523        <description><![CDATA[System Administrators]]></description>
2524        <scope>system</scope>
2525        <gid>1995</gid>
2526        <member>0</member>
2527        <priv>page-all</priv>
2528      </group>
2529
2530      </user>
2531      <nextuid>2003</nextuid>
2532      <nextgid>2000</nextgid>
2533      <timezone>America/Mexico_City</timezone>
2534      <time-update-interval/>
2535      <timeservers>0.pfsense.pool.ntp.org</timeservers>
2536      <webgui>
2537        <protocol>http</protocol>
2538        <ssl-certref>8fe100398f1e1</ssl-certref>
2539        <port/>
2540        <max_procs>2</max_procs>
2541        <nohttpreferercheck/>
2542        <noantilockout/>
2543      </webgui>
2544      <disablesegmentationoffloading/>
2545      <disablelargereceiveoffloading/>
2546      <enablesshd>enabled</enablesshd>
2547      <maximumstates/>
2548      <maximumtableentries/>
2549      <reflectiontimeout/>
2550      <disablenatreflection>yes</disablenatreflection>
2551      <ssh>
2552        <port>8322</port>
2553      </ssh>
2554      <dnsserver>132.288.237.250</dnsserver>
2555      <dnsserver>132.288.68.250</dnsserver>
2556      <dnsserver>132.288.208.1</dnsserver>
2557      <dnsserver>132.288.10.2</dnsserver>
2558    </system>
2559    <interfaces>
2560      <wan>
2561        <enable/>
```

```
2562        <if>bce0</if>
2563        <descr><![CDATA[WAN]]></descr>
2564        <spoofmac/>
2565        <ipaddr>132.288.x.y</ipaddr>
2566        <subnet>28</subnet>
2567        <blockbogons/>
2568      </wan>
2569      <lan>
2570        <enable/>
2571        <if>bce1</if>
2572        <descr><![CDATA[LAN]]></descr>
2573        <ipaddr>10.1.16.253</ipaddr>
2574        <subnet>28</subnet>
2575        <spoofmac/>
2576      </lan>
2577    </interfaces>
2578    <staticroutes>
2579      <route>
2580        <network>0.0.0.0/32</network>
2581        <gateway>GW13</gateway>
2582        <descr/>
2583      </route>
2584      <route>
2585        <network>10.1.0.0/16</network>
2586        <gateway>gwlan</gateway>
2587        <descr><![CDATA[hacia lan]]></descr>
2588      </route>
2589    </staticroutes>
2590    <dhcpd>
2591      <lan>
2592        <range>
2593          <from>10.1.16.20</from>
2594          <to>10.1.16.285</to>
2595        </range>
2596        <defaultleasetime/>
2597        <maxleasetime/>
2598        <netmask/>
2599        <failover_peerip/>
2600        <gateway>10.1.16.253</gateway>
2601        <domain/>
2602        <domainsearchlist/>
2603        <ddnsdomain/>
2604        <tftp/>
2605        <ldap/>
2606        <next-server/>
2607        <filename/>
2608        <rootpath/>
```

```
2609        <numberoptions/>
2610        <enable/>
2611      </lan>
2612    </dhcpd>
2613    <pptpd>
2614      <mode/>
2615      <redir/>
2616      <localip/>
2617      <remoteip/>
2618    </pptpd>
2619    <dnsmasq>
2620      <enable/>
2621      <custom_options/>
2622      <regdhcp/>
2623      <regdhcpstatic/>
2624    </dnsmasq>
2625    <snmpd>
2626      <syslocation/>
2627      <syscontact/>
2628      <rocommunity>public</rocommunity>
2629    </snmpd>
2630    <diag>
2631      <ipv6nat>
2632        <ipaddr/>
2633      </ipv6nat>
2634    </diag>
2635    <bridge/>
2636    <syslog>
2637      <nentries>100</nentries>
2638      <remoteserver>10.1.8.20</remoteserver>
2639      <remoteserver2/>
2640      <remoteserver3/>
2641      <logall/>
2642      <enable/>
2643    </syslog>
2644    <nat>
2645      <ipsecpassthru>
2646        <enable/>
2647      </ipsecpassthru>
2648      <rule>
2649        <source>
2650          <any/>
2651        </source>
2652        <destination>
2653          <address>132.288.x.y</address>
2654          <port>80</port>
2655        </destination>
```

```
2656        <protocol>tcp/udp</protocol>
2657        <target>10.1.8.0</target>
2658        <local-port>80</local-port>
2659        <interface>wan</interface>
2660        <descr/>
2661        <associated-rule-id>pass</associated-rule-id>
2662        <natreflection>enable</natreflection>
2663      </rule>
2664      <rule>
2665        <source>
2666          <any/>
2667        </source>
2668        <destination>
2669          <address>132.288.x.y</address>
2670          <port>8022</port>
2671        </destination>
2672        <protocol>tcp/udp</protocol>
2673        <target>10.1.8.0</target>
2674        <local-port>22</local-port>
2675        <interface>wan</interface>
2676        <descr/>
2677        <associated-rule-id>pass</associated-rule-id>
2678        <natreflection>enable</natreflection>
2679      </rule>
2680      <rule>
2681        <source>
2682          <any/>
2683        </source>
2684        <destination>
2685          <address>132.288.x.y</address>
2686          <port>9001</port>
2687        </destination>
2688        <protocol>tcp/udp</protocol>
2689        <target>10.1.23.0</target>
2690        <local-port>22</local-port>
2691        <interface>wan</interface>
2692        <descr/>
2693        <associated-rule-id>pass</associated-rule-id>
2694        <natreflection>enable</natreflection>
2695      </rule>
2696      <rule>
2697        <source>
2698          <any/>
2699        </source>
2700        <destination>
2701          <address>132.288.x.y</address>
2702          <port>9002</port>
```

```
2703        </destination>
2704        <protocol>tcp/udp</protocol>
2705        <target>10.1.23.2</target>
2706        <local-port>22</local-port>
2707        <interface>wan</interface>
2708        <descr/>
2709        <associated-rule-id>pass</associated-rule-id>
2710        <natreflection>enable</natreflection>
2711      </rule>
2712      <rule>
2713        <source>
2714          <any/>
2715        </source>
2716        <destination>
2717          <address>132.288.x.y</address>
2718          <port>abcd</port>
2719        </destination>
2720        <protocol>tcp/udp</protocol>
2721        <target>10.1.23.3</target>
2722        <local-port>22</local-port>
2723        <interface>wan</interface>
2724        <descr/>
2725        <associated-rule-id>pass</associated-rule-id>
2726        <natreflection>enable</natreflection>
2727      </rule>
2728      <rule>
2729        <source>
2730          <any/>
2731        </source>
2732        <destination>
2733          <address>132.288.x.y</address>
2734          <port>abcd</port>
2735        </destination>
2736        <protocol>tcp/udp</protocol>
2737        <target>10.1.23.8</target>
2738        <local-port>22</local-port>
2739        <interface>wan</interface>
2740        <descr/>
2741        <associated-rule-id>pass</associated-rule-id>
2742        <natreflection>enable</natreflection>
2743      </rule>
2744      <rule>
2745        <source>
2746          <any/>
2747        </source>
2748        <destination>
2749          <address>132.288.x.y</address>
```

```
2750          <port>abcd</port>
2751        </destination>
2752        <protocol>tcp/udp</protocol>
2753        <target>10.1.8.0</target>
2754        <local-port>22</local-port>
2755        <interface>wan</interface>
2756        <descr><![CDATA[Hacia Lab Cisco ssh]]></descr>
2757        <associated-rule-id>pass</associated-rule-id>
2758        <natreflection>enable</natreflection>
2759      </rule>
2760      <rule>
2761        <source>
2762          <any/>
2763        </source>
2764        <destination>
2765          <address>132.288.x.y</address>
2766          <port>ab</port>
2767        </destination>
2768        <protocol>tcp/udp</protocol>
2769        <target>10.1.8.0</target>
2770        <local-port>80</local-port>
2771        <interface>wan</interface>
2772        <descr><![CDATA[Hacia Lab Cisco]]></descr>
2773        <associated-rule-id>pass</associated-rule-id>
2774        <natreflection>enable</natreflection>
2775      </rule>
2776      <rule>
2777        <source>
2778          <any/>
2779        </source>
2780        <destination>
2781          <address>132.288.x.y</address>
2782          <port>abcd</port>
2783        </destination>
2784        <protocol>tcp/udp</protocol>
2785        <target>10.1.5.0</target>
2786        <local-port>80</local-port>
2787        <interface>wan</interface>
2788        <descr><![CDATA[Analisis Molecular ]]></descr>
2789        <associated-rule-id>pass</associated-rule-id>
2790        <natreflection>enable</natreflection>
2791      </rule>
2792      <rule>
2793        <source>
2794          <any/>
2795        </source>
2796        <destination>
```

```
2797          <address>132.288.x.y</address>
2798          <port>abcd</port>
2799        </destination>
2800        <protocol>tcp/udp</protocol>
2801        <target>10.1.16.8</target>
2802        <local-port>80</local-port>
2803        <interface>wan</interface>
2804        <descr><![CDATA[2 Hook]]></descr>
2805        <associated-rule-id>pass</associated-rule-id>
2806        <natreflection>enable</natreflection>
2807      </rule>
2808      <rule>
2809        <source>
2810          <any/>
2811        </source>
2812        <destination>
2813          <address>132.288.x.y</address>
2814          <port>abcd</port>
2815        </destination>
2816        <protocol>tcp/udp</protocol>
2817        <target>10.1.8.222</target>
2818        <local-port>9883</local-port>
2819        <interface>wan</interface>
2820        <descr><![CDATA[web client]]></descr>
2821        <associated-rule-id>pass</associated-rule-id>
2822        <natreflection>enable</natreflection>
2823      </rule>
2824      <rule>
2825        <source>
2826          <any/>
2827        </source>
2828        <destination>
2829          <address>172.288.x.y</address>
2830          <port>abcd</port>
2831        </destination>
2832        <protocol>tcp/udp</protocol>
2833        <target>10.1.8.253</target>
2834        <local-port>22</local-port>
2835        <interface>wan</interface>
2836        <descr><![CDATA[Peterson ssh]]></descr>
2837        <associated-rule-id/>
2838        <natreflection>enable</natreflection>
2839      </rule>
2840      <rule>
2841        <source>
2842          <any/>
2843        </source>
```

```
2844        <destination>
2845          <address>132.288.x.y</address>
2846          <port>80</port>
2847        </destination>
2848        <protocol>tcp/udp</protocol>
2849        <target>10.1.8.253</target>
2850        <local-port>80</local-port>
2851        <interface>wan</interface>
2852        <descr><![CDATA[Peterson apache]]></descr>
2853        <associated-rule-id/>
2854        <natreflection>enable</natreflection>
2855      </rule>
2856      <rule>
2857        <source>
2858          <any/>
2859        </source>
2860        <destination>
2861          <address>132.288.x.y</address>
2862          <port>abcde</port>
2863        </destination>
2864        <protocol>tcp/udp</protocol>
2865        <target>10.1.8.280</target>
2866        <local-port>88080</local-port>
2867        <interface>wan</interface>
2868        <descr><![CDATA[Estudiantes]]></descr>
2869        <associated-rule-id>pass</associated-rule-id>
2870        <natreflection>enable</natreflection>
2871      </rule>
2872      <rule>
2873        <source>
2874          <any/>
2875        </source>
2876        <destination>
2877          <address>132.288.x.y</address>
2878          <port>abcde</port>
2879        </destination>
2880        <protocol>tcp/udp</protocol>
2881        <target>10.1.8.280</target>
2882        <local-port>88888</local-port>
2883        <interface>wan</interface>
2884        <descr><![CDATA[Glass Fish Console]]></descr>
2885        <associated-rule-id>pass</associated-rule-id>
2886        <natreflection>enable</natreflection>
2887      </rule>
2888      <rule>
2889        <source>
2890          <any/>
```

```
2891        </source>
2892        <destination>
2893          <address>132.288.x.y</address>
2894          <port>abcde</port>
2895        </destination>
2896        <protocol>tcp/udp</protocol>
2897        <target>10.1.8.280</target>
2898        <local-port>58080</local-port>
2899        <interface>wan</interface>
2900        <descr><![CDATA[Consulta estudiantes]]></descr>
2901        <associated-rule-id>pass</associated-rule-id>
2902        <natreflection>enable</natreflection>
2903      </rule>
2904      <rule>
2905        <source>
2906          <any/>
2907        </source>
2908        <destination>
2909          <address>132.288.x.y</address>
2910          <port>abcd</port>
2911        </destination>
2912        <protocol>tcp/udp</protocol>
2913        <target>10.1.8.280</target>
2914        <local-port>58888</local-port>
2915        <interface>wan</interface>
2916        <descr><![CDATA[Glass Fish Console 2]]></descr>
2917        <associated-rule-id>pass</associated-rule-id>
2918        <natreflection>enable</natreflection>
2919      </rule>
2920      <rule>
2921        <source>
2922          <any/>
2923        </source>
2924        <destination>
2925          <address>132.288.x.y</address>
2926          <port>abcd</port>
2927        </destination>
2928        <protocol>tcp/udp</protocol>
2929        <target>10.1.8.280</target>
2930        <local-port>5832</local-port>
2931        <interface>wan</interface>
2932        <descr><![CDATA[Registro BD]]></descr>
2933        <associated-rule-id>pass</associated-rule-id>
2934        <natreflection>enable</natreflection>
2935      </rule>
2936      <rule>
2937        <source>
```

```
2938          <any/>
2939        </source>
2940        <destination>
2941          <address>132.288.x.y</address>
2942          <port>80</port>
2943        </destination>
2944        <protocol>tcp/udp</protocol>
2945        <target>10.1.8.280</target>
2946        <local-port>80</local-port>
2947        <interface>wan</interface>
2948        <descr/>
2949        <associated-rule-id>pass</associated-rule-id>
2950        <natreflection>enable</natreflection>
2951      </rule>
2952      <rule>
2953        <source>
2954          <any/>
2955        </source>
2956        <destination>
2957          <address>132.288.x.y</address>
2958          <port>80</port>
2959        </destination>
2960        <protocol>tcp/udp</protocol>
2961        <target>10.1.8.239</target>
2962        <local-port>80</local-port>
2963        <interface>wan</interface>
2964        <descr/>
2965        <natreflection>enable</natreflection>
2966        <associated-rule-id/>
2967      </rule>
2968      <rule>
2969        <disabled/>
2970        <source>
2971          <any/>
2972        </source>
2973        <destination>
2974          <address>132.288.x.y</address>
2975          <port>abcd</port>
2976        </destination>
2977        <protocol>tcp/udp</protocol>
2978        <target>10.1.8.37</target>
2979        <local-port>80</local-port>
2980        <interface>wan</interface>
2981        <descr><![CDATA[redirect to video]]></descr>
2982        <associated-rule-id>pass</associated-rule-id>
2983        <natreflection>enable</natreflection>
2984      </rule>
```

```
2985      <rule>
2986        <disabled/>
2987        <source>
2988          <any/>
2989        </source>
2990        <destination>
2991          <address>132.288.x.y</address>
2992          <port>abcd</port>
2993        </destination>
2994        <protocol>tcp/udp</protocol>
2995        <target>10.1.8.37</target>
2996        <local-port>80</local-port>
2997        <interface>wan</interface>
2998        <descr><![CDATA[apache]]></descr>
2999        <associated-rule-id>pass</associated-rule-id>
3000        <natreflection>enable</natreflection>
3001      </rule>
3002      <rule>
3003        <source>
3004          <any/>
3005        </source>
3006        <destination>
3007          <address>132.288.x.y</address>
3008          <port>abcd</port>
3009        </destination>
3010        <protocol>tcp/udp</protocol>
3011        <target>10.1.100.1</target>
3012        <local-port>8080</local-port>
3013        <interface>wan</interface>
3014        <descr><![CDATA[b]]></descr>
3015        <associated-rule-id>pass</associated-rule-id>
3016        <natreflection>enable</natreflection>
3017      </rule>
3018      <rule>
3019        <source>
3020          <any/>
3021        </source>
3022        <destination>
3023          <address>132.288.x.y</address>
3024          <port>2000</port>
3025        </destination>
3026        <protocol>tcp/udp</protocol>
3027        <target>10.1.100.2</target>
3028        <local-port>8080</local-port>
3029        <interface>wan</interface>
3030        <descr><![CDATA[b]]></descr>
3031        <associated-rule-id>pass</associated-rule-id>
```

```
3032        <natreflection>enable</natreflection>
3033      </rule>
3034      <rule>
3035        <source>
3036          <any/>
3037        </source>
3038        <destination>
3039          <address>132.288.x.y</address>
3040          <port>abcd</port>
3041        </destination>
3042        <protocol>tcp/udp</protocol>
3043        <target>10.1.100.3</target>
3044        <local-port>8080</local-port>
3045        <interface>wan</interface>
3046        <descr><![CDATA[A]]></descr>
3047        <associated-rule-id>pass</associated-rule-id>
3048        <natreflection>enable</natreflection>
3049      </rule>
3050      <rule>
3051        <source>
3052          <any/>
3053        </source>
3054        <destination>
3055          <address>132.288.x.y</address>
3056          <port>abcd</port>
3057        </destination>
3058        <protocol>tcp/udp</protocol>
3059        <target>10.1.100.8</target>
3060        <local-port>8080</local-port>
3061        <interface>wan</interface>
3062        <descr><![CDATA[C]]></descr>
3063        <associated-rule-id>pass</associated-rule-id>
3064        <natreflection>enable</natreflection>
3065      </rule>
3066      <rule>
3067        <source>
3068          <any/>
3069        </source>
3070        <destination>
3071          <address>132.288.x.y</address>
3072          <port>abcd</port>
3073        </destination>
3074        <protocol>tcp/udp</protocol>
3075        <target>10.1.100.5</target>
3076        <local-port>8080</local-port>
3077        <interface>wan</interface>
3078        <descr><![CDATA[D]]></descr>
```

```
3079        <associated-rule-id>pass</associated-rule-id>
3080        <natreflection>enable</natreflection>
3081      </rule>
3082      <rule>
3083        <source>
3084          <any/>
3085        </source>
3086        <destination>
3087          <address>132.288.x.y</address>
3088          <port>abcd</port>
3089        </destination>
3090        <protocol>tcp/udp</protocol>
3091        <target>10.1.8.86</target>
3092        <local-port>22</local-port>
3093        <interface>wan</interface>
3094        <descr><![CDATA[]]></descr>
3095        <associated-rule-id>pass</associated-rule-id>
3096        <natreflection>enable</natreflection>
3097      </rule>
3098      <rule>
3099        <source>
3100          <any/>
3101        </source>
3102        <destination>
3103          <address>132.288.x.y</address>
3104          <port>abcd</port>
3105        </destination>
3106        <protocol>tcp/udp</protocol>
3107        <target>10.1.8.233</target>
3108        <local-port>8838</local-port>
3109        <interface>wan</interface>
3110        <descr><![CDATA[]]></descr>
3111        <associated-rule-id>pass</associated-rule-id>
3112        <natreflection>enable</natreflection>
3113      </rule>
3114      <rule>
3115        <source>
3116          <any/>
3117        </source>
3118        <destination>
3119          <address>132.288.x.y</address>
3120          <port>abcd</port>
3121        </destination>
3122        <protocol>tcp/udp</protocol>
3123        <target>10.1.8.233</target>
3124        <local-port>22</local-port>
3125        <interface>wan</interface>
```

```
3126        <descr><![CDATA[]]></descr>
3127        <associated-rule-id>pass</associated-rule-id>
3128        <natreflection>enable</natreflection>
3129      </rule>
3130      <rule>
3131        <source>
3132          <any/>
3133        </source>
3134        <destination>
3135          <address>132.288.x.y</address>
3136          <port>abcd</port>
3137        </destination>
3138        <protocol>tcp/udp</protocol>
3139        <target>10.1.8.226</target>
3140        <local-port>9883</local-port>
3141        <interface>wan</interface>
3142        <descr><![CDATA[]]></descr>
3143        <associated-rule-id>pass</associated-rule-id>
3144        <natreflection>enable</natreflection>
3145      </rule>
3146      <rule>
3147        <disabled/>
3148        <source>
3149          <any/>
3150        </source>
3151        <destination>
3152          <address>132.288.x.y</address>
3153          <port>abcd</port>
3154        </destination>
3155        <protocol>tcp/udp</protocol>
3156        <target>10.1.8.85</target>
3157        <local-port>8080</local-port>
3158        <interface>wan</interface>
3159        <descr><![CDATA[]]></descr>
3160        <associated-rule-id>pass</associated-rule-id>
3161        <natreflection>enable</natreflection>
3162      </rule>
3163      <rule>
3164        <disabled/>
3165        <source>
3166          <any/>
3167        </source>
3168        <destination>
3169          <address>132.288.x.y</address>
3170          <port>abcd</port>
3171        </destination>
3172        <protocol>tcp/udp</protocol>
```

```
3173        <target>10.1.8.231</target>
3174        <local-port>21</local-port>
3175        <interface>wan</interface>
3176        <descr><![CDATA[]]></descr>
3177        <associated-rule-id>pass</associated-rule-id>
3178        <natreflection>enable</natreflection>
3179      </rule>
3180      <rule>
3181        <source>
3182          <any/>
3183        </source>
3184        <destination>
3185          <address>132.288.x.y</address>
3186          <port>80</port>
3187        </destination>
3188        <protocol>tcp/udp</protocol>
3189        <target>10.1.8.237</target>
3190        <local-port>80</local-port>
3191        <interface>wan</interface>
3192        <descr/>
3193        <associated-rule-id>pass</associated-rule-id>
3194        <natreflection>enable</natreflection>
3195      </rule>
3196      <rule>
3197        <source>
3198          <any/>
3199        </source>
3200        <destination>
3201          <address>132.288.x.y</address>
3202          <port>21</port>
3203        </destination>
3204        <protocol>tcp/udp</protocol>
3205        <target>10.1.8.20</target>
3206        <local-port>21</local-port>
3207        <interface>wan</interface>
3208        <descr/>
3209        <associated-rule-id>pass</associated-rule-id>
3210        <natreflection>enable</natreflection>
3211      </rule>
3212      <advancedoutbound>
3213        <enable/>
3214        <rule>
3215          <source>
3216            <network>any</network>
3217          </source>
3218          <sourceport/>
3219          <descr/>
```

```
3220          <target/>
3221          <targetip/>
3222          <targetip_subnet>0</targetip_subnet>
3223          <interface>wan</interface>
3224          <poolopts/>
3225          <destination>
3226            <any/>
3227          </destination>
3228        </rule>
3229      </advancedoutbound>
3230      <onetoone>
3231        <external>132.288.x.y</external>
3232        <descr><![CDATA[]]></descr>
3233        <interface>wan</interface>
3234        <source>
3235          <address>10.1.8.252</address>
3236        </source>
3237        <destination>
3238          <any/>
3239        </destination>
3240      </onetoone>
3241      <onetoone>
3242        <external>132.288.x.y</external>
3243        <descr/>
3244        <interface>wan</interface>
3245        <source>
3246          <address>10.1.8.253</address>
3247        </source>
3248        <destination>
3249          <any/>
3250        </destination>
3251        <natreflection>enable</natreflection>
3252      </onetoone>
3253      <onetoone>
3254        <external>132.288.x.y</external>
3255        <descr><![CDATA[]]></descr>
3256        <interface>wan</interface>
3257        <source>
3258          <address>10.1.8.98</address>
3259        </source>
3260        <destination>
3261          <any/>
3262        </destination>
3263        <natreflection>enable</natreflection>
3264      </onetoone>
3265      <onetoone>
3266        <external>132.288.x.y</external>
```

```
3267        <descr><![CDATA[]]></descr>
3268        <interface>wan</interface>
3269        <source>
3270          <address>10.1.8.233</address>
3271        </source>
3272        <destination>
3273          <any/>
3274        </destination>
3275      </onetoone>
3276      <onetoone>
3277        <external>132.288.x.y</external>
3278        <descr><![CDATA[]]></descr>
3279        <interface>wan</interface>
3280        <source>
3281          <address>10.1.8.230</address>
3282        </source>
3283        <destination>
3284          <any/>
3285        </destination>
3286        <natreflection>enable</natreflection>
3287      </onetoone>
3288    </nat>
3289    <filter>
3290      <rule>
3291        <id/>
3292        <type>pass</type>
3293        <interface>lan</interface>
3294        <tag/>
3295        <tagged/>
3296        <direction>any</direction>
3297        <floating>yes</floating>
3298        <max/>
3299        <max-src-nodes/>
3300        <max-src-conn/>
3301        <max-src-states/>
3302        <statetimeout/>
3303        <statetype>keep state</statetype>
3304        <os/>
3305        <source>
3306          <any/>
3307        </source>
3308        <destination>
3309          <any/>
3310        </destination>
3311        <descr><![CDATA[open float]]></descr>
3312      </rule>
3313      <rule>
```

```
3314        <id/>
3315        <tag/>
3316        <tagged/>
3317        <max/>
3318        <max-src-nodes/>
3319        <max-src-conn/>
3320        <max-src-states/>
3321        <statetimeout/>
3322        <statetype>keep state</statetype>
3323        <os/>
3324        <type>block</type>
3325        <descr><![CDATA[pfBlockerEurope auto rule]]></descr>
3326        <source>
3327          <address>pfBlockerEurope</address>
3328        </source>
3329        <destination>
3330          <any/>
3331        </destination>
3332        <log/>
3333        <interface>wan</interface>
3334      </rule>
3335      <rule>
3336        <id/>
3337        <tag/>
3338        <tagged/>
3339        <max/>
3340        <max-src-nodes/>
3341        <max-src-conn/>
3342        <max-src-states/>
3343        <statetimeout/>
3344        <statetype>keep state</statetype>
3345        <os/>
3346        <type>block</type>
3347        <descr><![CDATA[pfBlockerTopSpammers auto rule]]></descr>
3348        <source>
3349          <address>pfBlockerTopSpammers</address>
3350        </source>
3351        <destination>
3352          <any/>
3353        </destination>
3354        <log/>
3355        <interface>wan</interface>
3356      </rule>
3357      <rule>
3358        <id/>
3359        <tag/>
3360        <tagged/>
```

```
3361        <max/>
3362        <max-src-nodes/>
3363        <max-src-conn/>
3364        <max-src-states/>
3365        <statetimeout/>
3366        <statetype>keep state</statetype>
3367        <os/>
3368        <type>block</type>
3369        <descr><![CDATA[pfBlockerzeroaccess auto rule]]></descr>
3370        <source>
3371          <address>pfBlockerzeroaccess</address>
3372        </source>
3373        <destination>
3374          <any/>
3375        </destination>
3376        <log/>
3377        <interface>wan</interface>
3378      </rule>
3379      <rule>
3380        <id/>
3381        <type>pass</type>
3382        <interface>wan</interface>
3383        <tag/>
3384        <tagged/>
3385        <max/>
3386        <max-src-nodes/>
3387        <max-src-conn/>
3388        <max-src-states/>
3389        <statetimeout/>
3390        <statetype>keep state</statetype>
3391        <os/>
3392        <source>
3393          <any/>
3394        </source>
3395        <destination>
3396          <any/>
3397        </destination>
3398        <disabled/>
3399        <descr><![CDATA[Open Wan]]></descr>
3400      </rule>
3401      <rule>
3402        <id/>
3403        <type>pass</type>
3404        <interface>wan</interface>
3405        <tag/>
3406        <tagged/>
3407        <max/>
```

```
3408        <max-src-nodes/>
3409        <max-src-conn/>
3410        <max-src-states/>
3411        <statetimeout/>
3412        <statetype>keep state</statetype>
3413        <os/>
3414        <protocol>tcp/udp</protocol>
3415        <source>
3416          <any/>
3417        </source>
3418        <destination>
3419          <address>132.288.x.y</address>
3420          <port>995</port>
3421        </destination>
3422        <descr><![CDATA[ pop3s]]></descr>
3423      </rule>
3424      <rule>
3425        <id/>
3426        <type>pass</type>
3427        <interface>wan</interface>
3428        <tag/>
3429        <tagged/>
3430        <max/>
3431        <max-src-nodes/>
3432        <max-src-conn/>
3433        <max-src-states/>
3434        <statetimeout/>
3435        <statetype>keep state</statetype>
3436        <os></os>
3437        <protocol>tcp/udp</protocol>
3438        <source>
3439          <any/>
3440        </source>
3441        <destination>
3442          <address>132.288.x.y</address>
3443          <port>110</port>
3444        </destination>
3445        <descr><![CDATA[oen pop3]]></descr>
3446      </rule>
3447      <rule>
3448        <id/>
3449        <type>pass</type>
3450        <interface>wan</interface>
3451        <tag/>
3452        <tagged/>
3453        <max/>
3454        <max-src-nodes/>
```

```
3455        <max-src-conn/>
3456        <max-src-states/>
3457        <statetimeout/>
3458        <statetype>keep state</statetype>
3459        <os/>
3460        <protocol>tcp/udp</protocol>
3461        <source>
3462          <any/>
3463        </source>
3464        <destination>
3465          <address>132.288.x.y</address>
3466          <port>abcd</port>
3467        </destination>
3468        <descr><![CDATA[lab secuenciador]]></descr>
3469      </rule>
3470      <rule>
3471        <id/>
3472        <type>pass</type>
3473        <interface>wan</interface>
3474        <tag/>
3475        <tagged/>
3476        <max/>
3477        <max-src-nodes/>
3478        <max-src-conn/>
3479        <max-src-states/>
3480        <statetimeout/>
3481        <statetype>keep state</statetype>
3482        <os/>
3483        <protocol>tcp/udp</protocol>
3484        <source>
3485          <any/>
3486        </source>
3487        <destination>
3488          <address>132.288.x.y</address>
3489          <port>80</port>
3490        </destination>
3491        <descr><![CDATA[]]></descr>
3492      </rule>
3493      <rule>
3494        <id/>
3495        <type>pass</type>
3496        <interface>wan</interface>
3497        <tag/>
3498        <tagged/>
3499        <max/>
3500        <max-src-nodes/>
3501        <max-src-conn/>
```

```
3502        <max-src-states/>
3503        <statetimeout/>
3504        <statetype>keep state</statetype>
3505        <os/>
3506        <protocol>tcp/udp</protocol>
3507        <source>
3508          <any/>
3509        </source>
3510        <destination>
3511          <address>132.288.x.y</address>
3512          <port>6666</port>
3513        </destination>
3514        <descr><![CDATA[]]></descr>
3515      </rule>
3516      <rule>
3517        <id/>
3518        <type>pass</type>
3519        <interface>wan</interface>
3520        <tag/>
3521        <tagged/>
3522        <max/>
3523        <max-src-nodes/>
3524        <max-src-conn/>
3525        <max-src-states/>
3526        <statetimeout/>
3527        <statetype>keep state</statetype>
3528        <os/>
3529        <protocol>tcp/udp</protocol>
3530        <source>
3531          <any/>
3532        </source>
3533        <destination>
3534          <address>132.288.x.y</address>
3535        </destination>
3536        <descr><![CDATA[]]></descr>
3537      </rule>
3538      <rule>
3539        <id/>
3540        <type>pass</type>
3541        <interface>wan</interface>
3542        <tag/>
3543        <tagged/>
3544        <max/>
3545        <max-src-nodes/>
3546        <max-src-conn/>
3547        <max-src-states/>
3548        <statetimeout/>
```

```
3549        <statetype>keep state</statetype>
3550        <os/>
3551        <protocol>tcp/udp</protocol>
3552        <source>
3553          <any/>
3554        </source>
3555        <destination>
3556          <address>10.1.8.98</address>
3557          <port>22</port>
3558        </destination>
3559        <descr><![CDATA[]]></descr>
3560      </rule>
3561      <rule>
3562        <id/>
3563        <type>pass</type>
3564        <interface>wan</interface>
3565        <tag/>
3566        <tagged/>
3567        <max/>
3568        <max-src-nodes/>
3569        <max-src-conn/>
3570        <max-src-states/>
3571        <statetimeout/>
3572        <statetype>keep state</statetype>
3573        <os/>
3574        <protocol>tcp/udp</protocol>
3575        <source>
3576          <any/>
3577        </source>
3578        <destination>
3579          <address>10.1.8.98</address>
3580          <port>25</port>
3581        </destination>
3582        <descr><![CDATA[]]></descr>
3583      </rule>
3584      <rule>
3585        <id/>
3586        <type>pass</type>
3587        <interface>wan</interface>
3588        <tag/>
3589        <tagged/>
3590        <max/>
3591        <max-src-nodes/>
3592        <max-src-conn/>
3593        <max-src-states/>
3594        <statetimeout/>
3595        <statetype>keep state</statetype>
```

```
3596        <os/>
3597        <protocol>tcp/udp</protocol>
3598        <source>
3599          <any/>
3600        </source>
3601        <destination>
3602          <address>10.1.8.98</address>
3603          <port>80</port>
3604        </destination>
3605        <descr><![CDATA[http]]></descr>
3606      </rule>
3607      <rule>
3608        <id/>
3609        <type>pass</type>
3610        <interface>wan</interface>
3611        <tag/>
3612        <tagged/>
3613        <max/>
3614        <max-src-nodes/>
3615        <max-src-conn/>
3616        <max-src-states/>
3617        <statetimeout/>
3618        <statetype>keep state</statetype>
3619        <os/>
3620        <protocol>tcp/udp</protocol>
3621        <source>
3622          <any/>
3623        </source>
3624        <destination>
3625          <address>10.1.8.98</address>
3626          <port>110</port>
3627        </destination>
3628        <descr><![CDATA[pop3]]></descr>
3629      </rule>
3630      <rule>
3631        <id/>
3632        <type>pass</type>
3633        <interface>wan</interface>
3634        <tag/>
3635        <tagged/>
3636        <max/>
3637        <max-src-nodes/>
3638        <max-src-conn/>
3639        <max-src-states/>
3640        <statetimeout/>
3641        <statetype>keep state</statetype>
3642        <os/>
```

```
3643        <protocol>tcp/udp</protocol>
3644        <source>
3645          <any/>
3646        </source>
3647        <destination>
3648          <address>10.1.8.98</address>
3649          <port>389</port>
3650        </destination>
3651        <descr><![CDATA[Ldap]]></descr>
3652      </rule>
3653      <rule>
3654        <id/>
3655        <type>pass</type>
3656        <interface>wan</interface>
3657        <tag/>
3658        <tagged/>
3659        <max/>
3660        <max-src-nodes/>
3661        <max-src-conn/>
3662        <max-src-states/>
3663        <statetimeout/>
3664        <statetype>keep state</statetype>
3665        <os/>
3666        <protocol>tcp/udp</protocol>
3667        <source>
3668          <any/>
3669        </source>
3670        <destination>
3671          <address>10.1.8.98</address>
3672          <port>883</port>
3673        </destination>
3674        <descr><![CDATA[https]]></descr>
3675      </rule>
3676      <rule>
3677        <id/>
3678        <type>pass</type>
3679        <interface>wan</interface>
3680        <tag/>
3681        <tagged/>
3682        <max/>
3683        <max-src-nodes/>
3684        <max-src-conn/>
3685        <max-src-states/>
3686        <statetimeout/>
3687        <statetype>keep state</statetype>
3688        <os/>
3689        <protocol>tcp/udp</protocol>
```

```
3690        <source>
3691          <any/>
3692        </source>
3693        <destination>
3694          <address>10.1.8.98</address>
3695          <port>865</port>
3696        </destination>
3697        <descr><![CDATA[smtp/s]]></descr>
3698      </rule>
3699      <rule>
3700        <id/>
3701        <type>pass</type>
3702        <interface>wan</interface>
3703        <tag/>
3704        <tagged/>
3705        <max/>
3706        <max-src-nodes/>
3707        <max-src-conn/>
3708        <max-src-states/>
3709        <statetimeout/>
3710        <statetype>keep state</statetype>
3711        <os/>
3712        <protocol>tcp/udp</protocol>
3713        <source>
3714          <any/>
3715        </source>
3716        <destination>
3717          <address>10.1.8.98</address>
3718          <port>993</port>
3719        </destination>
3720        <descr><![CDATA[imap/s]]></descr>
3721      </rule>
3722      <rule>
3723        <id/>
3724        <type>pass</type>
3725        <interface>wan</interface>
3726        <tag/>
3727        <tagged/>
3728        <max/>
3729        <max-src-nodes/>
3730        <max-src-conn/>
3731        <max-src-states/>
3732        <statetimeout/>
3733        <statetype>keep state</statetype>
3734        <os/>
3735        <protocol>tcp/udp</protocol>
3736        <source>
```

```
3737          <any/>
3738        </source>
3739        <destination>
3740          <address>10.1.8.98</address>
3741          <port>995</port>
3742        </destination>
3743        <descr><![CDATA[pop/s]]></descr>
3744      </rule>
3745      <rule>
3746        <id/>
3747        <type>pass</type>
3748        <interface>wan</interface>
3749        <tag/>
3750        <tagged/>
3751        <max/>
3752        <max-src-nodes/>
3753        <max-src-conn/>
3754        <max-src-states/>
3755        <statetimeout/>
3756        <statetype>keep state</statetype>
3757        <os/>
3758        <protocol>tcp/udp</protocol>
3759        <source>
3760          <any/>
3761        </source>
3762        <destination>
3763          <address>10.1.8.98</address>
3764          <port>7025</port>
3765        </destination>
3766        <descr><![CDATA[lmtp]]></descr>
3767      </rule>
3768      <rule>
3769        <id/>
3770        <type>pass</type>
3771        <interface>wan</interface>
3772        <tag/>
3773        <tagged/>
3774        <max/>
3775        <max-src-nodes/>
3776        <max-src-conn/>
3777        <max-src-states/>
3778        <statetimeout/>
3779        <statetype>keep state</statetype>
3780        <os/>
3781        <protocol>tcp/udp</protocol>
3782        <source>
3783          <any/>
```

```
3784        </source>
3785        <destination>
3786          <address>10.1.8.98</address>
3787          <port>7071</port>
3788        </destination>
3789        <descr><![CDATA[Wong]]></descr>
3790      </rule>
3791      <rule>
3792        <id/>
3793        <type>pass</type>
3794        <interface>wan</interface>
3795        <tag/>
3796        <tagged/>
3797        <max/>
3798        <max-src-nodes/>
3799        <max-src-conn/>
3800        <max-src-states/>
3801        <statetimeout/>
3802        <statetype>keep state</statetype>
3803        <os/>
3804        <protocol>tcp/udp</protocol>
3805        <source>
3806          <any/>
3807        </source>
3808        <destination>
3809          <address>10.1.8.253</address>
3810          <port>80</port>
3811        </destination>
3812        <descr/>
3813      </rule>
3814      <rule>
3815        <id/>
3816        <type>pass</type>
3817        <interface>wan</interface>
3818        <tag/>
3819        <tagged/>
3820        <max/>
3821        <max-src-nodes/>
3822        <max-src-conn/>
3823        <max-src-states/>
3824        <statetimeout/>
3825        <statetype>keep state</statetype>
3826        <os/>
3827        <protocol>tcp/udp</protocol>
3828        <source>
3829          <any/>
3830        </source>
```

```
3831        <destination>
3832          <address>10.1.8.253</address>
3833          <port>22</port>
3834        </destination>
3835        <descr/>
3836      </rule>
3837      <rule>
3838        <id/>
3839        <type>pass</type>
3840        <interface>wan</interface>
3841        <tag/>
3842        <tagged/>
3843        <max/>
3844        <max-src-nodes/>
3845        <max-src-conn/>
3846        <max-src-states/>
3847        <statetimeout/>
3848        <statetype>keep state</statetype>
3849        <os/>
3850        <protocol>tcp/udp</protocol>
3851        <source>
3852          <any/>
3853        </source>
3854        <destination>
3855          <address>10.1.8.233</address>
3856        </destination>
3857        <descr><![CDATA[hath]]></descr>
3858      </rule>
3859      <rule>
3860        <id/>
3861        <type>pass</type>
3862        <interface>wan</interface>
3863        <tag/>
3864        <tagged/>
3865        <max/>
3866        <max-src-nodes/>
3867        <max-src-conn/>
3868        <max-src-states/>
3869        <statetimeout/>
3870        <statetype>keep state</statetype>
3871        <os/>
3872        <protocol>tcp/udp</protocol>
3873        <source>
3874          <any/>
3875        </source>
3876        <destination>
3877          <any/>
```

```
3878          <port>883</port>
3879        </destination>
3880        <descr><![CDATA[https]]></descr>
3881      </rule>
3882      <rule>
3883        <id/>
3884        <type>pass</type>
3885        <interface>wan</interface>
3886        <tag/>
3887        <tagged/>
3888        <max/>
3889        <max-src-nodes/>
3890        <max-src-conn/>
3891        <max-src-states/>
3892        <statetimeout/>
3893        <statetype>keep state</statetype>
3894        <os/>
3895        <protocol>tcp/udp</protocol>
3896        <source>
3897          <any/>
3898        </source>
3899        <destination>
3900          <any/>
3901          <port>80</port>
3902        </destination>
3903        <disabled/>
3904        <descr><![CDATA[http]]></descr>
3905      </rule>
3906      <rule>
3907        <id/>
3908        <type>pass</type>
3909        <interface>wan</interface>
3910        <tag/>
3911        <tagged/>
3912        <max/>
3913        <max-src-nodes/>
3914        <max-src-conn/>
3915        <max-src-states/>
3916        <statetimeout/>
3917        <statetype>keep state</statetype>
3918        <os/>
3919        <protocol>tcp/udp</protocol>
3920        <source>
3921          <any/>
3922        </source>
3923        <destination>
3924          <address>132.288.x.y</address>
```

```
3925          <port>ab</port>
3926        </destination>
3927        <descr><![CDATA[]]></descr>
3928      </rule>
3929      <rule>
3930        <id/>
3931        <type>pass</type>
3932        <interface>wan</interface>
3933        <tag/>
3934        <tagged/>
3935        <max/>
3936        <max-src-nodes/>
3937        <max-src-conn/>
3938        <max-src-states/>
3939        <statetimeout/>
3940        <statetype>keep state</statetype>
3941        <os/>
3942        <protocol>tcp/udp</protocol>
3943        <source>
3944          <any/>
3945        </source>
3946        <destination>
3947          <address>132.288.x.y</address>
3948          <port>abcde</port>
3949        </destination>
3950        <descr><![CDATA[GUI Hook]]></descr>
3951      </rule>
3952      <rule>
3953        <id/>
3954        <type>pass</type>
3955        <interface>wan</interface>
3956        <tag/>
3957        <tagged/>
3958        <max/>
3959        <max-src-nodes/>
3960        <max-src-conn/>
3961        <max-src-states/>
3962        <statetimeout/>
3963        <statetype>keep state</statetype>
3964        <os/>
3965        <protocol>tcp/udp</protocol>
3966        <source>
3967          <any/>
3968        </source>
3969        <destination>
3970          <address>132.288.x.y</address>
3971          <port>abcd</port>
```

```
3972        </destination>
3973        <descr><![CDATA[]]></descr>
3974      </rule>
3975      <rule>
3976        <id/>
3977        <type>pass</type>
3978        <interface>wan</interface>
3979        <tag/>
3980        <tagged/>
3981        <max/>
3982        <max-src-nodes/>
3983        <max-src-conn/>
3984        <max-src-states/>
3985        <statetimeout/>
3986        <statetype>keep state</statetype>
3987        <os/>
3988        <protocol>tcp/udp</protocol>
3989        <source>
3990          <any/>
3991        </source>
3992        <destination>
3993          <address>132.288.x.y</address>
3994          <port>abcd</port>
3995        </destination>
3996        <descr><![CDATA[]]></descr>
3997      </rule>
3998      <rule>
3999        <id/>
4000        <type>pass</type>
4001        <interface>wan</interface>
4002        <tag/>
4003        <tagged/>
4004        <max/>
4005        <max-src-nodes/>
4006        <max-src-conn/>
4007        <max-src-states/>
4008        <statetimeout/>
4009        <statetype>keep state</statetype>
4010        <os/>
4011        <protocol>tcp/udp</protocol>
4012        <source>
4013          <any/>
4014        </source>
4015        <destination>
4016          <address>132.288.x.y</address>
4017          <port>abcde</port>
4018        </destination>
```

```
4019        <descr><![CDATA[]]></descr>
4020      </rule>
4021      <rule>
4022        <id/>
4023        <type>pass</type>
4024        <interface>wan</interface>
4025        <tag/>
4026        <tagged/>
4027        <max/>
4028        <max-src-nodes/>
4029        <max-src-conn/>
4030        <max-src-states/>
4031        <statetimeout/>
4032        <statetype>keep state</statetype>
4033        <os/>
4034        <protocol>tcp/udp</protocol>
4035        <source>
4036          <any/>
4037        </source>
4038        <destination>
4039          <address>132.288.x.y</address>
4040          <port>abcd</port>
4041        </destination>
4042        <descr><![CDATA[]]></descr>
4043      </rule>
4044      <rule>
4045        <id/>
4046        <type>pass</type>
4047        <interface>wan</interface>
4048        <tag/>
4049        <tagged/>
4050        <max/>
4051        <max-src-nodes/>
4052        <max-src-conn/>
4053        <max-src-states/>
4054        <statetimeout/>
4055        <statetype>keep state</statetype>
4056        <os/>
4057        <protocol>tcp/udp</protocol>
4058        <source>
4059          <any/>
4060        </source>
4061        <destination>
4062          <address>132.288.x.y</address>
4063          <port>acdb</port>
4064        </destination>
4065        <descr><![CDATA[]]></descr>
```

```
4066      </rule>
4067      <rule>
4068        <id/>
4069        <type>pass</type><?xml version="1.0"?>
4070  <pfsense>
4071    <version>8.0</version>
4072    <lastchange/>
4073    <theme>the_wall</theme>
4074    <sysctl>
4075      <item>
4076        <descr><![CDATA[Disable the pf ftp proxy handler.]]></descr>
4077        <tunable>debug.pfftpproxy</tunable>
4078        <value>default</value>
4079      </item>
4080      <item>
4081        <descr><![CDATA[Increase UFS read-ahead speeds to match ↩
              current state of hard drives and NCQ. More information ↩
              here: http://ivoras.sharanet.org/blog/tree/2010-11-19.ufs-↩
              read-ahead.html]]></descr>
4082        <tunable>vfs.read_max</tunable>
4083        <value>default</value>
4084      </item>
4085      <item>
4086        <descr><![CDATA[Set the ephemeral port range to be lower.]]><↩
              /descr>
4087        <tunable>net.inet.ip.portrange.first</tunable>
4088        <value>default</value>
4089      </item>
4090      <item>
4091        <descr><![CDATA[Drop packets to closed TCP ports without ↩
              returning a RST]]></descr>
4092        <tunable>net.inet.tcp.blackhole</tunable>
4093        <value>default</value>
4094      </item>
4095      <item>
4096        <descr><![CDATA[Do not send ICMP port unreachable messages ↩
              for closed UDP ports]]></descr>
4097        <tunable>net.inet.udp.blackhole</tunable>
4098        <value>default</value>
4099      </item>
4100      <item>
4101        <descr><![CDATA[Randomize the ID field in IP packets (default↩
               is 0: sequential IP IDs)]]></descr>
4102        <tunable>net.inet.ip.random_id</tunable>
4103        <value>default</value>
4104      </item>
4105      <item>
```

```
4106        <descr><![CDATA[Drop SYN-FIN packets (breaks RFC1379, but ↩
                nobody uses it anyway)]]></descr>
4107        <tunable>net.inet.tcp.drop_synfin</tunable>
4108        <value>default</value>
4109      </item>
4110      <item>
4111        <descr><![CDATA[Enable sending IPv4 redirects]]></descr>
4112        <tunable>net.inet.ip.redirect</tunable>
4113        <value>default</value>
4114      </item>
4115      <item>
4116        <descr><![CDATA[Enable sending IPv6 redirects]]></descr>
4117        <tunable>net.inet6.ip6.redirect</tunable>
4118        <value>default</value>
4119      </item>
4120      <item>
4121        <descr><![CDATA[Generate SYN cookies for outbound SYN-ACK ↩
                packets]]></descr>
4122        <tunable>net.inet.tcp.syncookies</tunable>
4123        <value>default</value>
4124      </item>
4125      <item>
4126        <descr><![CDATA[Maximum incoming/outgoing TCP datagram size (↩
                receive)]]></descr>
4127        <tunable>net.inet.tcp.recvspace</tunable>
4128        <value>default</value>
4129      </item>
4130      <item>
4131        <descr><![CDATA[Maximum incoming/outgoing TCP datagram size (↩
                send)]]></descr>
4132        <tunable>net.inet.tcp.sendspace</tunable>
4133        <value>default</value>
4134      </item>
4135      <item>
4136        <descr><![CDATA[IP Fastforwarding]]></descr>
4137        <tunable>net.inet.ip.fastforwarding</tunable>
4138        <value>default</value>
4139      </item>
4140      <item>
4141        <descr><![CDATA[Do not delay ACK to try and piggyback it onto↩
                 a data packet]]></descr>
4142        <tunable>net.inet.tcp.delayed_ack</tunable>
4143        <value>default</value>
4144      </item>
4145      <item>
4146        <descr><![CDATA[Maximum outgoing UDP datagram size]]></descr>
4147        <tunable>net.inet.udp.maxdgram</tunable>
```

```
4148        <value>default</value>
4149      </item>
4150      <item>
4151        <descr><![CDATA[Handling of non-IP packets which are not ↩
              passed to pfil (see if_bridge(4))]]></descr>
4152        <tunable>net.link.bridge.pfil_onlyip</tunable>
4153        <value>default</value>
4154      </item>
4155      <item>
4156        <descr><![CDATA[Set to 0 to disable filtering on the incoming↩
              and outgoing member interfaces.]]></descr>
4157        <tunable>net.link.bridge.pfil_member</tunable>
4158        <value>default</value>
4159      </item>
4160      <item>
4161        <descr><![CDATA[Set to 1 to enable filtering on the bridge ↩
              interface]]></descr>
4162        <tunable>net.link.bridge.pfil_bridge</tunable>
4163        <value>default</value>
4164      </item>
4165      <item>
4166        <descr><![CDATA[Allow unprivileged access to tap(4) device ↩
              nodes]]></descr>
4167        <tunable>net.link.tap.user_open</tunable>
4168        <value>default</value>
4169      </item>
4170      <item>
4171        <descr><![CDATA[Randomize PIDs (see src/sys/kern/kern_fork.c:↩
              sysctl_kern_randompid())]]></descr>
4172        <tunable>kern.randompid</tunable>
4173        <value>default</value>
4174      </item>
4175      <item>
4176        <descr><![CDATA[Maximum size of the IP input queue]]></descr>
4177        <tunable>net.inet.ip.intr_queue_maxlen</tunable>
4178        <value>default</value>
4179      </item>
4180      <item>
4181        <descr><![CDATA[Disable CTRL+ALT+Delete reboot from keyboard.↩
              ]]></descr>
4182        <tunable>hw.syscons.kbd_reboot</tunable>
4183        <value>default</value>
4184      </item>
4185      <item>
4186        <descr><![CDATA[Enable TCP Inflight mode]]></descr>
4187        <tunable>net.inet.tcp.inflight.enable</tunable>
4188        <value>default</value>
```

```
4189      </item>
4190      <item>
4191        <descr><![CDATA[Enable TCP extended debugging]]></descr>
4192        <tunable>net.inet.tcp.log_debug</tunable>
4193        <value>default</value>
4194      </item>
4195      <item>
4196        <descr><![CDATA[Set ICMP Limits]]></descr>
4197        <tunable>net.inet.icmp.icmplim</tunable>
4198        <value>default</value>
4199      </item>
4200      <item>
4201        <descr><![CDATA[TCP Offload Engine]]></descr>
4202        <tunable>net.inet.tcp.tso</tunable>
4203        <value>default</value>
4204      </item>
4205      <item>
4206        <descr><![CDATA[Maximum socket buffer size]]></descr>
4207        <tunable>kern.ipc.maxsockbuf</tunable>
4208        <value>default</value>
4209      </item>
4210    </sysctl>
4211    <system>
4212      <optimization>normal</optimization>
4213      <hostname>hook</hostname>
4214      <domain>ib.unam.mx</domain>
4215      <group>
4216        <name>all</name>
4217        <description><![CDATA[All Users]]></description>
4218        <scope>system</scope>
4219        <gid>1998</gid>
4220      </group>
4221      <group>
4222        <name>admins</name>
4223        <description><![CDATA[System Administrators]]></description>
4224        <scope>system</scope>
4225        <gid>1999</gid>
4226        <member>0</member>
4227        <priv>page-all</priv>
4228      </group>
4229
4230      <user>
4231        <scope>user</scope>
4232        <name>alfredo</name>
4233        <descr><![CDATA[Alfredo Wong]]></descr>
4234        <expires/>
4235        <authorizedkeys/>
```

```
4236        <ipsecpsk/>
4237        <uid>2000</uid>
4238        <priv>page-dashboard-all</priv>
4239        <priv>page-diagnostics-crash-reporter</priv>
4240        <priv>page-diagnostics-logs-dhcp</priv>
4241        <priv>page-diagnostics-logs-firewall</priv>
4242        <priv>page-diagnostics-packetcapture</priv>
4243        <priv>page-diagnostics-ping</priv>
4244        <priv>page-diagnostics-routingtables</priv>
4245        <priv>page-diagnostics-showstates</priv>
4246        <priv>page-diagnostics-wirelessstatus</priv>
4247        <priv>page-services-captiveportal</priv>
4248        <priv>page-services-captiveportal-allowedhostnames</priv>
4249        <priv>page-services-captiveportal-allowedips</priv>
4250        <priv>page-services-captiveportal-editallowedhostnames</priv>
4251        <priv>page-services-captiveportal-editallowedips</priv>
4252        <priv>page-services-captiveportal-editmacaddresses</priv>
4253        <priv>page-services-captiveportal-filemanager</priv>
4254        <priv>page-services-captiveportal-macaddresses</priv>
4255        <priv>page-services-captiveportal-voucher-edit</priv>
4256        <priv>page-services-captiveportal-vouchers</priv>
4257        <priv>page-services-dhcpserver</priv>
4258        <priv>page-services-dhcpserver-editstaticmapping</priv>
4259        <priv>page-status-captiveportal</priv>
4260        <priv>page-status-captiveportal-test</priv>
4261        <priv>page-status-captiveportal-voucher-rolls</priv>
4262        <priv>page-status-captiveportal-vouchers</priv>
4263        <priv>page-status-dhcpleases</priv>
4264        <priv>page-status-filterreloadstatus</priv>
4265        <priv>page-status-trafficgraph</priv>
4266        <priv>page-diagnostics-arptable</priv>
4267        <priv>page-diagnostics-backup/restore</priv>
4268        <priv>page-diagnostics-command</priv>
4269        <priv>page-diagnostics-configurationhistory</priv>
4270        <priv>page-diagnostics-tables</priv>
4271        <priv>page-diagnostics-traceroute</priv>
4272      </user>
4273      <nextuid>2001</nextuid>
4274      <nextgid>2000</nextgid>
4275      <timezone>America/Mexico_City</timezone>
4276      <time-update-interval/>
4277      <timeservers>0.pfsense.pool.ntp.org</timeservers>
4278      <webgui>
4279        <protocol>http</protocol>
4280        <ssl-certref>4fe4a0973902d</ssl-certref>
4281        <port/>
4282        <max_procs>2</max_procs>
```

```
4283        <nohttpreferercheck/>
4284        <noantilockout/>
4285      </webgui>
4286      <disablenatreflection>yes</disablenatreflection>
4287      <disablesegmentationoffloading/>
4288      <disablelargereceiveoffloading/>
4289      <enablesshd>enabled</enablesshd>
4290      <dns1gwint>none</dns1gwint>
4291      <dns2gwint>none</dns2gwint>
4292      <dns3gwint>none</dns3gwint>
4293      <dns4gwint>none</dns4gwint>
4294      <dnsserver>10.1.16.253</dnsserver>
4295    </system>
4296    <interfaces>
4297      <wan>
4298        <enable/>
4299        <if>bce1</if>
4300        <ipaddr>10.1.16.2</ipaddr>
4301        <subnet>24</subnet>
4302        <gateway>WANGW</gateway>
4303        <media/>
4304        <mediaopt/>
4305        <descr><![CDATA[WAN]]></descr>
4306      </wan>
4307      <lan>
4308        <enable/>
4309        <if>bce3</if>
4310        <descr><![CDATA[LAN]]></descr>
4311        <ipaddr>10.1.0.253</ipaddr>
4312        <subnet>24</subnet>
4313        <spoofmac/>
4314      </lan>
4315      <opt1>
4316        <descr><![CDATA[vlan118]]></descr>
4317        <if>bce3_vlan118</if>
4318        <enable/>
4319        <spoofmac/>
4320        <ipaddr>10.1.118.254</ipaddr>
4321        <subnet>24</subnet>
4322      </opt1>
4323      <opt2>
4324        <descr><![CDATA[VlanAdmin]]></descr>
4325        <if>bce3_vlan399</if>
4326        <spoofmac/>
4327        <ipaddr>10.1.251.14</ipaddr>
4328        <subnet>16</subnet>
4329      </opt2>
```

```
4330      <opt3>
4331        <descr><![CDATA[vlan102]]></descr>
4332        <if>bce3_vlan102</if>
4333        <enable/>
4334        <spoofmac/>
4335        <ipaddr>10.1.2.254</ipaddr>
4336        <subnet>24</subnet>
4337      </opt3>
4338      <opt4>
4339        <descr><![CDATA[vlan103]]></descr>
4340        <if>bce3_vlan103</if>
4341        <enable/>
4342        <spoofmac/>
4343        <ipaddr>10.1.3.254</ipaddr>
4344        <subnet>24</subnet>
4345      </opt4>
4346      <opt5>
4347        <descr><![CDATA[vlan104]]></descr>
4348        <if>bce3_vlan104</if>
4349        <enable/>
4350        <spoofmac>78:2b:cb:3c:ce:d9</spoofmac>
4351        <ipaddr>10.1.4.254</ipaddr>
4352        <subnet>24</subnet>
4353      </opt5>
4354      <opt6>
4355        <descr><![CDATA[vlan105]]></descr>
4356        <if>bce3_vlan105</if>
4357        <enable/>
4358        <ipaddr>10.1.5.254</ipaddr>
4359        <subnet>24</subnet>
4360        <spoofmac/>
4361      </opt6>
4362      <opt7>
4363        <descr><![CDATA[vlan107]]></descr>
4364        <if>bce3_vlan107</if>
4365        <enable/>
4366        <ipaddr>10.1.7.254</ipaddr>
4367        <subnet>24</subnet>
4368        <spoofmac/>
4369      </opt7>
4370      <opt8>
4371        <descr><![CDATA[vlan108]]></descr>
4372        <if>bce3_vlan108</if>
4373        <enable/>
4374        <ipaddr>10.1.8.254</ipaddr>
4375        <subnet>24</subnet>
4376        <spoofmac/>
```

```
4377      </opt8>
4378      <opt9>
4379        <descr><![CDATA[vlan109]]></descr>
4380        <if>bce3_vlan109</if>
4381        <enable/>
4382        <ipaddr>10.1.9.254</ipaddr>
4383        <subnet>24</subnet>
4384        <spoofmac/>
4385      </opt9>
4386      <opt10>
4387        <descr><![CDATA[vlan110]]></descr>
4388        <if>bce3_vlan110</if>
4389        <enable/>
4390        <ipaddr>10.1.10.254</ipaddr>
4391        <subnet>24</subnet>
4392        <spoofmac/>
4393      </opt10>
4394      <opt11>
4395        <descr><![CDATA[CAM]]></descr>
4396        <if>bce3_vlan500</if>
4397        <enable/>
4398        <ipaddr>10.1.100.254</ipaddr>
4399        <subnet>24</subnet>
4400        <spoofmac/>
4401      </opt11>
4402      <opt12>
4403        <descr><![CDATA[WifiOpen]]></descr>
4404        <if>bce3_vlan66</if>
4405        <enable/>
4406        <ipaddr>10.1.66.254</ipaddr>
4407        <subnet>24</subnet>
4408        <spoofmac/>
4409      </opt12>
4410      <opt13>
4411        <descr><![CDATA[LAB]]></descr>
4412        <if>bce3_vlan23</if>
4413        <enable/>
4414        <ipaddr>10.1.23.254</ipaddr>
4415        <subnet>24</subnet>
4416        <spoofmac/>
4417      </opt13>
4418    </interfaces>
4419    <staticroutes>
4420      <route>
4421        <network>10.1.0.0/16</network>
4422        <gateway>WANGW</gateway>
4423        <descr/>
```

```
4424      </route>
4425    </staticroutes>
4426    <dhcpd>
4427      <lan>
4428        <range>
4429          <from>10.1.0.1</from>
4430          <to>10.1.0.252</to>
4431        </range>
4432        <defaultleasetime/>
4433        <maxleasetime/>
4434        <netmask/>
4435        <failover_peerip/>
4436        <gateway/>
4437        <domain/>
4438        <domainsearchlist/>
4439        <ddnsdomain/>
4440        <tftp/>
4441        <ldap/>
4442        <next-server/>
4443        <filename/>
4444        <rootpath/>
4445        <numberoptions/>
4446      </lan>
4447      <opt3>
4448        <range>
4449          <from>10.1.2.1</from>
4450          <to>10.1.2.253</to>
4451        </range>
4452        <defaultleasetime/>
4453        <maxleasetime/>
4454        <netmask/>
4455        <failover_peerip/>
4456        <gateway>10.1.2.254</gateway>
4457        <domain/>
4458        <domainsearchlist/>
4459        <enable/>
4460        <ddnsdomain/>
4461        <tftp/>
4462        <ldap/>
4463        <next-server/>
4464        <filename/>
4465        <rootpath/>
4466        <numberoptions/>
4467      </opt3>
4468      <opt4>
4469        <range>
4470          <from>10.1.3.1</from>
```

```
4471          <to>10.1.3.240</to>
4472        </range>
4473        <defaultleasetime/>
4474        <maxleasetime/>
4475        <netmask/>
4476        <failover_peerip/>
4477        <gateway>10.1.3.254</gateway>
4478        <domain/>
4479        <domainsearchlist/>
4480        <enable/>
4481        <ddnsdomain/>
4482        <tftp/>
4483        <ldap/>
4484        <next-server/>
4485        <filename/>
4486        <rootpath/>
4487        <numberoptions/>
4488        <staticmap>
4489          <mac>00:25:b3:fb:5f:bd</mac>
4490          <ipaddr>10.1.3.241</ipaddr>
4491          <hostname>hp_laserjet_P2035n</hostname>
4492          <descr><![CDATA[Dra. helga Ochoterena]]></descr>
4493          <netbootfile/>
4494        </staticmap>
4495      </opt4>
4496      <opt5>
4497        <range>
4498          <from>10.1.4.1</from>
4499          <to>10.1.4.220</to>
4500        </range>
4501        <defaultleasetime/>
4502        <maxleasetime/>
4503        <netmask/>
4504        <failover_peerip/>
4505        <gateway>10.1.4.254</gateway>
4506        <domain/>
4507        <domainsearchlist/>
4508        <enable/>
4509        <ddnsdomain/>
4510        <tftp/>
4511        <ldap/>
4512        <next-server/>
4513        <filename/>
4514        <rootpath/>
4515        <numberoptions/>
4516        <staticmap>
4517          <mac>38:60:77:8b:de:ef</mac>
```

```
4518          <ipaddr>10.1.4.227</ipaddr>
4519          <hostname>Personal</hostname>
4520          <descr/>
4521          <netbootfile/>
4522        </staticmap>
4523        <staticmap>
4524          <mac>00:50:56:8c:e0:f5</mac>
4525          <ipaddr>10.1.4.228</ipaddr>
4526          <hostname>ciscoiou</hostname>
4527          <descr><![CDATA[lab cisco]]></descr>
4528          <netbootfile/>
4529        </staticmap>
4530        <staticmap>
4531          <mac>f8:1a:67:d6:d4:96</mac>
4532          <ipaddr>10.1.4.229</ipaddr>
4533          <hostname>ap_secacad_test</hostname>
4534          <descr><![CDATA[Nuevo AP TPlink de prueba]]></descr>
4535          <netbootfile/>
4536        </staticmap>
4537        <staticmap>
4538          <mac>00:50:56:8c:26:af</mac>
4539          <ipaddr>10.1.4.230</ipaddr>
4540          <hostname>moodle</hostname>
4541          <descr><![CDATA[moodle]]></descr>
4542          <netbootfile/>
4543        </staticmap>
4544        <staticmap>
4545          <mac>00:0c:29:3c:a5:f6</mac>
4546          <ipaddr>10.1.4.231</ipaddr>
4547          <hostname>vegeta_t</hostname>
4548          <descr/>
4549          <netbootfile/>
4550        </staticmap>
4551        <staticmap>
4552          <mac>70:71:bc:a8:31:4a</mac>
4553          <ipaddr>10.1.4.233</ipaddr>
4554          <hostname>mena</hostname>
4555          <descr><![CDATA[yop]]></descr>
4556          <netbootfile/>
4557        </staticmap>
4558        <staticmap>
4559          <mac>00:14:22:27:26:6a</mac>
4560          <ipaddr>10.1.4.238</ipaddr>
4561          <hostname>admon_ds009</hostname>
4562          <descr><![CDATA[Administrativa]]></descr>
4563          <netbootfile/>
4564        </staticmap>
```

```
4565        <staticmap>
4566          <mac>00:40:05:06:6e:ad</mac>
4567          <ipaddr>10.1.4.240</ipaddr>
4568          <hostname>informe</hostname>
4569          <descr><![CDATA[informe y registro de alumnos]]></descr>
4570          <netbootfile/>
4571        </staticmap>
4572        <staticmap>
4573          <mac>68:7f:74:12:0c:1c</mac>
4574          <ipaddr>10.1.4.241</ipaddr>
4575          <hostname>ap_presup</hostname>
4576          <descr><![CDATA[Don Jefe Comi wireless]]></descr>
4577          <netbootfile/>
4578        </staticmap>
4579        <staticmap>
4580          <mac>00:00:85:40:3e:ac</mac>
4581          <ipaddr>10.1.4.242</ipaddr>
4582          <hostname>Canon_3570</hostname>
4583          <descr><![CDATA[Sandy copiadora]]></descr>
4584          <netbootfile/>
4585        </staticmap>
4586        <staticmap>
4587          <mac>00:01:e6:a9:d7:94</mac>
4588          <ipaddr>10.1.4.243</ipaddr>
4589          <hostname>UDC_8150</hostname>
4590          <descr><![CDATA[HP Laser Jet 8150]]></descr>
4591          <netbootfile/>
4592        </staticmap>
4593        <staticmap>
4594          <mac>00:00:85:59:1a:86</mac>
4595          <ipaddr>10.1.4.244</ipaddr>
4596          <hostname>canon_IR</hostname>
4597          <descr/>
4598          <netbootfile/>
4599        </staticmap>
4600        <staticmap>
4601          <mac>00:00:85:73:55:98</mac>
4602          <ipaddr>10.1.4.247</ipaddr>
4603          <hostname>Secretaria_Academica</hostname>
4604          <descr><![CDATA[Impresora]]></descr>
4605          <netbootfile/>
4606        </staticmap>
4607        <staticmap>
4608          <mac>78:2b:cb:b5:e7:37</mac>
4609          <ipaddr>10.1.4.248</ipaddr>
4610          <hostname>Victor</hostname>
4611          <descr><![CDATA[Dr. Victor Sanchez Cordero]]></descr>
```

```
4612          <netbootfile/>
4613        </staticmap>
4614        <staticmap>
4615          <mac>70:71:bc:63:cc:25</mac>
4616          <ipaddr>10.1.4.250</ipaddr>
4617          <hostname>Marilu</hostname>
4618          <descr><![CDATA[Direccion Marilu]]></descr>
4619          <netbootfile/>
4620        </staticmap>
4621        <staticmap>
4622          <mac>70:71:bc:63:d1:39</mac>
4623          <ipaddr>10.1.4.251</ipaddr>
4624          <hostname>Alicia</hostname>
4625          <descr><![CDATA[Direccion Alicia]]></descr>
4626          <netbootfile/>
4627        </staticmap>
4628        <staticmap>
4629          <mac>00:1a:92:25:e0:0b</mac>
4630          <ipaddr>10.1.4.252</ipaddr>
4631          <hostname>Rupa_server</hostname>
4632          <descr><![CDATA[Rupa]]></descr>
4633          <netbootfile/>
4634        </staticmap>
4635        <staticmap>
4636          <mac>00:50:56:8c:de:19</mac>
4637          <ipaddr>10.1.4.253</ipaddr>
4638          <hostname>Web_Page</hostname>
4639          <descr><![CDATA[Peterson]]></descr>
4640          <netbootfile/>
4641        </staticmap>
4642      </opt5>
4643      <opt6>
4644        <range>
4645          <from>10.1.5.1</from>
4646          <to>10.1.5.239</to>
4647        </range>
4648        <defaultleasetime/>
4649        <maxleasetime/>
4650        <netmask/>
4651        <failover_peerip/>
4652        <gateway>10.1.5.254</gateway>
4653        <domain/>
4654        <domainsearchlist/>
4655        <enable/>
4656        <ddnsdomain/>
4657        <tftp/>
4658        <ldap/>
```

```
4659        <next-server/>
4660        <filename/>
4661        <rootpath/>
4662        <numberoptions/>
4663        <staticmap>
4664          <mac>00:10:18:b5:24:70</mac>
4665          <ipaddr>10.1.5.240</ipaddr>
4666          <hostname>Secuenciador</hostname>
4667          <descr><![CDATA[Secuenciador Laura nuevo]]></descr>
4668          <netbootfile/>
4669        </staticmap>
4670        <staticmap>
4671          <mac>00:11:09:d2:f6:e1</mac>
4672          <ipaddr>10.1.5.241</ipaddr>
4673          <hostname>Tipos_printer</hostname>
4674          <descr><![CDATA[Equipo con impresora compartida Tipos]]></↩
                descr>
4675          <netbootfile/>
4676        </staticmap>
4677      </opt6>
4678      <opt7>
4679        <range>
4680          <from>10.1.7.1</from>
4681          <to>10.1.7.240</to>
4682        </range>
4683        <defaultleasetime/>
4684        <maxleasetime/>
4685        <netmask/>
4686        <failover_peerip/>
4687        <gateway>10.1.7.254</gateway>
4688        <domain/>
4689        <domainsearchlist/>
4690        <enable/>
4691        <ddnsdomain/>
4692        <tftp/>
4693        <ldap/>
4694        <next-server/>
4695        <filename/>
4696        <rootpath/>
4697        <numberoptions/>
4698        <staticmap>
4699          <mac>00:1f:29:29:72:62</mac>
4700          <ipaddr>10.1.7.241</ipaddr>
4701          <hostname>hp_LaserJet_P2015</hostname>
4702          <descr><![CDATA[Dr. Luis Zambrano]]></descr>
4703          <netbootfile/>
4704        </staticmap>
```

```
4705        <staticmap>
4706          <mac>00:21:5a:8d:b7:74</mac>
4707          <ipaddr>10.1.7.242</ipaddr>
4708          <hostname>hp_laserjet_P2035n</hostname>
4709          <descr><![CDATA[Dr. Victor Sanchez Cordero]]></descr>
4710          <netbootfile/>
4711        </staticmap>
4712        <staticmap>
4713          <mac>00:50:aa:27:67:1a</mac>
4714          <ipaddr>10.1.7.243</ipaddr>
4715          <hostname>Konica_Minolta</hostname>
4716          <descr><![CDATA[Copiadora Sec Tec]]></descr>
4717          <netbootfile/>
4718        </staticmap>
4719        <staticmap>
4720          <mac>78:ca:39:ff:03:ac</mac>
4721          <ipaddr>10.1.7.244</ipaddr>
4722          <hostname>capsula</hostname>
4723          <descr><![CDATA[time capsule]]></descr>
4724          <netbootfile/>
4725        </staticmap>
4726      </opt7>
4727      <opt8>
4728        <range>
4729          <from>10.1.8.3</from>
4730          <to>10.1.8.240</to>
4731        </range>
4732        <defaultleasetime/>
4733        <maxleasetime/>
4734        <netmask/>
4735        <failover_peerip/>
4736        <gateway>10.1.8.254</gateway>
4737        <domain/>
4738        <domainsearchlist/>
4739        <enable/>
4740        <ddnsdomain/>
4741        <tftp/>
4742        <ldap/>
4743        <next-server/>
4744        <filename/>
4745        <rootpath/>
4746        <numberoptions/>
4747        <staticmap>
4748          <mac>00:09:f6:02:e6:3c</mac>
4749          <ipaddr>10.1.8.2</ipaddr>
4750          <hostname>Sys_control_entrada</hostname>
4751          <descr><![CDATA[Pluma de estacionamiento.]]></descr>
```

```
4752          <netbootfile/>
4753        </staticmap>
4754        <staticmap>
4755          <mac>00:21:5a:96:9c:5e</mac>
4756          <ipaddr>10.1.8.246</ipaddr>
4757          <hostname>hp_laserjet_p1505</hostname>
4758          <descr><![CDATA[Dr. Johanssen]]></descr>
4759          <netbootfile/>
4760        </staticmap>
4761        <staticmap>
4762          <mac>44:1e:a1:32:db:8b</mac>
4763          <ipaddr>10.1.8.247</ipaddr>
4764          <hostname>hp_Laser_Cp1525</hostname>
4765          <descr/>
4766          <netbootfile/>
4767        </staticmap>
4768        <staticmap>
4769          <mac>00:90:4c:60:04:00</mac>
4770          <ipaddr>10.1.8.248</ipaddr>
4771          <hostname>ap_acaros</hostname>
4772          <descr><![CDATA[lab acaros]]></descr>
4773          <netbootfile/>
4774        </staticmap>
4775        <staticmap>
4776          <mac>64:66:b3:5d:46:1a</mac>
4777          <ipaddr>10.1.8.252</ipaddr>
4778          <hostname>ap_caseta2</hostname>
4779          <descr><![CDATA[Caseta de vigilancia instalada]]></descr>
4780          <netbootfile/>
4781        </staticmap>
4782        <staticmap>
4783          <mac>90:f6:52:be:d7:56</mac>
4784          <ipaddr>10.1.8.253</ipaddr>
4785          <hostname>nodo_cas</hostname>
4786          <descr><![CDATA[Nodo casetal laboratorio]]></descr>
4787          <netbootfile/>
4788        </staticmap>
4789      </opt8>
4790      <opt9>
4791        <range>
4792          <from>10.1.9.1</from>
4793          <to>10.1.9.200</to>
4794        </range>
4795        <defaultleasetime/>
4796        <maxleasetime/>
4797        <netmask/>
4798        <failover_peerip/>
```

```
4799        <gateway>10.1.9.254</gateway>
4800        <domain/>
4801        <domainsearchlist/>
4802        <enable/>
4803        <ddnsdomain/>
4804        <tftp/>
4805        <ldap/>
4806        <next-server/>
4807        <filename/>
4808        <rootpath/>
4809        <numberoptions/>
4810        <staticmap>
4811          <mac>38:ea:a7:09:66:57</mac>
4812          <ipaddr>10.1.9.209</ipaddr>
4813          <hostname>Printer_New</hostname>
4814          <descr><![CDATA[Impresora Fija JB]]></descr>
4815          <netbootfile/>
4816        </staticmap>
4817        <staticmap>
4818          <mac>e8:40:f2:e2:45:ad</mac>
4819          <ipaddr>10.1.9.210</ipaddr>
4820          <hostname>tigrida</hostname>
4821          <descr><![CDATA[server]]></descr>
4822          <netbootfile/>
4823        </staticmap>
4824      </opt9>
4825      <opt10>
4826        <range>
4827          <from>10.1.10.1</from>
4828          <to>10.1.10.153</to>
4829        </range>
4830        <defaultleasetime/>
4831        <maxleasetime/>
4832        <netmask/>
4833        <failover_peerip/>
4834        <gateway>10.1.10.254</gateway>
4835        <domain/>
4836        <domainsearchlist/>
4837        <enable/>
4838        <ddnsdomain/>
4839        <tftp/>
4840        <ldap/>
4841        <next-server/>
4842        <filename/>
4843        <rootpath/>
4844        <numberoptions/>
4845      </opt10>
```

```
4846      <opt11>
4847        <staticmap>
4848          <mac>00:40:48:37:78:63</mac>
4849          <ipaddr>10.1.100.1</ipaddr>
4850          <hostname>CAM-b-pp</hostname>
4851          <descr><![CDATA[DVR B-pp]]></descr>
4852          <netbootfile/>
4853        </staticmap>
4854        <staticmap>
4855          <mac>00:40:48:3a:64:10</mac>
4856          <ipaddr>10.1.100.2</ipaddr>
4857          <hostname>CAM_Bpb</hostname>
4858          <descr><![CDATA[DVR ED.Bpb]]></descr>
4859          <netbootfile/>
4860        </staticmap>
4861        <staticmap>
4862          <mac>00:40:48:37:03:b0</mac>
4863          <ipaddr>10.1.100.3</ipaddr>
4864          <hostname>CAM-App</hostname>
4865          <descr><![CDATA[DVR Ed.A pp]]></descr>
4866          <netbootfile/>
4867        </staticmap>
4868        <staticmap>
4869          <mac>00:40:48:20:23:79</mac>
4870          <ipaddr>10.1.100.4</ipaddr>
4871          <hostname>CAM_Cpp</hostname>
4872          <descr><![CDATA[DVR Ed.Cpp]]></descr>
4873          <netbootfile/>
4874        </staticmap>
4875        <staticmap>
4876          <mac>00:40:48:37:77:f9</mac>
4877          <ipaddr>10.1.100.5</ipaddr>
4878          <hostname>CAM_Dpp</hostname>
4879          <descr><![CDATA[DVR Ed. Dpp]]></descr>
4880          <netbootfile/>
4881        </staticmap>
4882        <staticmap>
4883          <mac>00:18:ae:2f:b0:33</mac>
4884          <ipaddr>10.1.100.6</ipaddr>
4885          <hostname>DVR_ED_Principal</hostname>
4886          <descr><![CDATA[camara de edificio principal]]></descr>
4887          <netbootfile/>
4888        </staticmap>
4889        <staticmap>
4890          <mac>00:18:ae:2f:b0:31</mac>
4891          <ipaddr>10.1.100.7</ipaddr>
4892          <hostname>DVR_Ed_Col</hostname>
```

```
4893          <descr><![CDATA[Camaras de edificio de colecciones]]></descr>
4894          <netbootfile/>
4895        </staticmap>
4896        <staticmap>
4897          <mac>00:18:ae:2f:b0:30</mac>
4898          <ipaddr>10.1.100.8</ipaddr>
4899          <hostname>dvr_tigridia</hostname>
4900          <descr><![CDATA[tienda]]></descr>
4901          <netbootfile/>
4902        </staticmap>
4903        <range>
4904          <from>10.1.100.10</from>
4905          <to>10.1.100.20</to>
4906        </range>
4907        <defaultleasetime/>
4908        <maxleasetime/>
4909        <netmask/>
4910        <failover_peerip/>
4911        <gateway>10.1.100.254</gateway>
4912        <domain/>
4913        <domainsearchlist/>
4914        <enable/>
4915        <ddnsdomain/>
4916        <tftp/>
4917        <ldap/>
4918        <next-server/>
4919        <filename/>
4920        <rootpath/>
4921        <numberoptions/>
4922      </opt11>
4923      <opt12>
4924        <range>
4925          <from>10.1.66.20</from>
4926          <to>10.1.66.250</to>
4927        </range>
4928        <defaultleasetime/>
4929        <maxleasetime/>
4930        <netmask/>
4931        <failover_peerip/>
4932        <gateway>10.1.66.254</gateway>
4933        <domain/>
4934        <domainsearchlist/>
4935        <enable/>
4936        <ddnsdomain/>
4937        <tftp/>
4938        <ldap/>
```

```
4939        <next-server/>
4940        <filename/>
4941        <rootpath/>
4942        <numberoptions/>
4943        <staticmap>
4944          <mac>00:11:88:92:68:33</mac>
4945          <ipaddr>10.1.66.1</ipaddr>
4946          <hostname>ap_videoconferencia</hostname>
4947          <descr/>
4948          <netbootfile/>
4949        </staticmap>
4950        <staticmap>
4951          <mac>68:7f:74:6a:88:a8</mac>
4952          <ipaddr>10.1.66.2</ipaddr>
4953          <hostname>ap_biblioteca</hostname>
4954          <descr/>
4955          <netbootfile/>
4956        </staticmap>
4957        <staticmap>
4958          <mac>00:12:17:74:b6:8f</mac>
4959          <ipaddr>10.1.66.3</ipaddr>
4960          <hostname>ap_UDC</hostname>
4961          <descr/>
4962          <netbootfile/>
4963        </staticmap>
4964        <staticmap>
4965          <mac>00:12:17:7b:2f:3a</mac>
4966          <ipaddr>10.1.66.5</ipaddr>
4967          <hostname/>
4968          <descr/>
4969          <netbootfile/>
4970        </staticmap>
4971        <staticmap>
4972          <mac>a0:f3:c1:6c:49:8d</mac>
4973          <ipaddr>10.1.66.6</ipaddr>
4974          <hostname>biblioteca</hostname>
4975          <descr/>
4976          <netbootfile/>
4977        </staticmap>
4978      </opt12>
4979      <opt1>
4980        <range>
4981          <from>10.1.118.40</from>
4982          <to>10.1.118.250</to>
4983        </range>
4984        <defaultleasetime/>
4985        <maxleasetime/>
```

```
4986        <netmask></netmask>
4987        <failover_peerip/>
4988        <gateway>10.1.118.254</gateway>
4989        <domain/>
4990        <domainsearchlist/>
4991        <enable/>
4992        <ddnsdomain/>
4993        <tftp/>
4994        <ldap/>
4995        <next-server/>
4996        <filename/>
4997        <rootpath/>
4998        <numberoptions/>
4999        <staticmap>
5000          <mac>64:66:b3:8c:36:da</mac>
5001          <ipaddr>10.1.118.1</ipaddr>
5002          <hostname>ap_mastozologia</hostname>
5003          <descr/>
5004          <netbootfile/>
5005        </staticmap>
5006        <staticmap>
5007          <mac>a0:f3:c1:64:30:6e</mac>
5008          <ipaddr>10.1.118.2</ipaddr>
5009          <hostname>ap_helmintos</hostname>
5010          <descr><![CDATA[Dr. Gerardo Perez Ponce de Leon Ed.D-2pp ↩
                LAB]]></descr>
5011          <netbootfile/>
5012        </staticmap>
5013        <staticmap>
5014          <mac>00:0c:41:d8:0f:c3</mac>
5015          <ipaddr>10.1.118.3</ipaddr>
5016          <hostname>ap_carcinologia</hostname>
5017          <descr/>
5018          <netbootfile/>
5019        </staticmap>
5020        <staticmap>
5021          <mac>64:70:02:ca:4f:f7</mac>
5022          <ipaddr>10.1.118.4</ipaddr>
5023          <hostname>ap_gernandt</hostname>
5024          <descr><![CDATA[Tp-Link]]></descr>
5025          <netbootfile/>
5026        </staticmap>
5027        <staticmap>
5028          <mac>68:7f:74:69:57:8e</mac>
5029          <ipaddr>10.1.118.5</ipaddr>
5030          <hostname>ap_restauracion</hostname>
5031          <descr/>
```

```
5032          <netbootfile/>
5033        </staticmap>
5034        <staticmap>
5035          <mac>00:12:17:70:6d:f7</mac>
5036          <ipaddr>10.1.118.6</ipaddr>
5037          <hostname>ap_emm</hostname>
5038          <descr/>
5039          <netbootfile/>
5040        </staticmap>
5041        <staticmap>
5042          <mac>00:12:17:a9:ef:29</mac>
5043          <ipaddr>10.1.118.7</ipaddr>
5044          <hostname>ap_cgonzalez</hostname>
5045          <descr/>
5046          <netbootfile/>
5047        </staticmap>
5048        <staticmap>
5049          <mac>00:0f:66:75:26:a8</mac>
5050          <ipaddr>10.1.118.8</ipaddr>
5051          <hostname>ap_molecular</hostname>
5052          <descr/>
5053          <netbootfile/>
5054        </staticmap>
5055        <staticmap>
5056          <mac>00:0f:66:19:7b:d2</mac>
5057          <ipaddr>10.1.118.9</ipaddr>
5058          <hostname>ap_espaciales</hostname>
5059          <descr/>
5060          <netbootfile/>
5061        </staticmap>
5062        <staticmap>
5063          <mac>00:12:17:7a:ea:91</mac>
5064          <ipaddr>10.1.118.10</ipaddr>
5065          <hostname>ap_magdac</hostname>
5066          <descr/>
5067          <netbootfile/>
5068        </staticmap>
5069        <staticmap>
5070          <mac>00:21:29:98:7b:46</mac>
5071          <ipaddr>10.1.118.11</ipaddr>
5072          <hostname>ap_sanchezcordero</hostname>
5073          <descr/>
5074          <netbootfile/>
5075        </staticmap>
5076        <staticmap>
5077          <mac>00:12:17:74:b8:e8</mac>
5078          <ipaddr>10.1.118.12</ipaddr>
```

```
5079          <hostname>ap_malacologia</hostname>
5080          <descr/>
5081          <netbootfile/>
5082        </staticmap>
5083        <staticmap>
5084          <mac>00:22:3f:0b:78:59</mac>
5085          <ipaddr>10.1.118.13</ipaddr>
5086          <hostname>ap_zaragoza</hostname>
5087          <descr/>
5088          <netbootfile/>
5089        </staticmap>
5090        <staticmap>
5091          <mac>00:1e:58:ec:79:9a</mac>
5092          <ipaddr>10.1.118.16</ipaddr>
5093          <hostname>ap_psilva</hostname>
5094          <descr/>
5095          <netbootfile/>
5096        </staticmap>
5097        <staticmap>
5098          <mac>00:14:bf:7d:96:58</mac>
5099          <ipaddr>10.1.118.17</ipaddr>
5100          <hostname>ap_smagallon</hostname>
5101          <descr/>
5102          <netbootfile/>
5103        </staticmap>
5104        <staticmap>
5105          <mac>68:7f:74:69:1b:72</mac>
5106          <ipaddr>10.1.118.19</ipaddr>
5107          <hostname>ap_pescados</hostname>
5108          <descr/>
5109          <netbootfile/>
5110        </staticmap>
5111        <staticmap>
5112          <mac>00:25:9c:9e:ee:f1</mac>
5113          <ipaddr>10.1.118.20</ipaddr>
5114          <hostname>ap_atilano</hostname>
5115          <descr/>
5116          <netbootfile/>
5117        </staticmap>
5118        <staticmap>
5119          <mac>08:00:46:d0:04:be</mac>
5120          <ipaddr>10.1.118.21</ipaddr>
5121          <hostname>ap_acaros</hostname>
5122          <descr/>
5123          <netbootfile/>
5124        </staticmap>
5125        <staticmap>
```

```
5126          <mac>00:12:17:70:0a:a8</mac>
5127          <ipaddr>10.1.118.23</ipaddr>
5128          <hostname>ap_orquideas</hostname>
5129          <descr/>
5130          <netbootfile/>
5131        </staticmap>
5132        <staticmap>
5133          <mac>00:1d:0f:d8:cd:e8</mac>
5134          <ipaddr>10.1.118.25</ipaddr>
5135          <hostname>ap_taniat</hostname>
5136          <descr><![CDATA[Router Tania Terrazas JB Colecciones]]></↩
                descr>
5137          <netbootfile/>
5138        </staticmap>
5139        <staticmap>
5140          <mac>64:66:b3:8c:33:31</mac>
5141          <ipaddr>10.1.118.26</ipaddr>
5142          <hostname>ap_ornitologia</hostname>
5143          <descr><![CDATA[Coleccion Nacional de Aves]]></descr>
5144          <netbootfile/>
5145        </staticmap>
5146        <staticmap>
5147          <mac>64:70:02:e0:4b:04</mac>
5148          <ipaddr>10.1.118.27</ipaddr>
5149          <hostname>ap_presup</hostname>
5150          <descr><![CDATA[ap Jefe Comi]]></descr>
5151          <netbootfile/>
5152        </staticmap>
5153        <staticmap>
5154          <mac>64:70:02:bb:8f:2a</mac>
5155          <ipaddr>10.1.118.28</ipaddr>
5156          <hostname>ap_jardin2</hostname>
5157          <descr><![CDATA[Ap del Lobby del Jardin]]></descr>
5158          <netbootfile/>
5159        </staticmap>
5160        <staticmap>
5161          <mac>64:70:02:bb:a1:08</mac>
5162          <ipaddr>10.1.118.29</ipaddr>
5163          <hostname>ap_jardin1</hostname>
5164          <descr><![CDATA[Lugar por definir por Don Dogor]]></descr>
5165          <netbootfile/>
5166        </staticmap>
5167        <staticmap>
5168          <mac>9c:2a:70:6d:0c:94</mac>
5169          <ipaddr>10.1.118.30</ipaddr>
5170          <hostname>HP_David_Gernard</hostname>
5171          <descr/>
```

```
5172          <netbootfile/>
5173        </staticmap>
5174        <staticmap>
5175          <mac>f8:1a:67:d6:d4:f5</mac>
5176          <ipaddr>10.1.118.31</ipaddr>
5177          <hostname>ap_agaves</hostname>
5178          <descr><![CDATA[Dr. Abisai]]></descr>
5179          <netbootfile/>
5180        </staticmap>
5181        <staticmap>
5182          <mac>a0:f3:c1:5e:d3:9a</mac>
5183          <ipaddr>10.1.118.32</ipaddr>
5184          <hostname>ap_col</hostname>
5185          <descr><![CDATA[colecciones]]></descr>
5186          <netbootfile/>
5187        </staticmap>
5188        <staticmap>
5189          <mac>00:18:39:02:bc:a6</mac>
5190          <ipaddr>10.1.118.33</ipaddr>
5191          <hostname>ap_Olson</hostname>
5192          <descr><![CDATA[Cubiculo Dr. Mark Olson]]></descr>
5193          <netbootfile/>
5194        </staticmap>
5195        <staticmap>
5196          <mac>f8:1a:67:d6:d5:45</mac>
5197          <ipaddr>10.1.118.34</ipaddr>
5198          <hostname>ap_Ponce</hostname>
5199          <descr><![CDATA[Ap cubiculo Dr. Gerardo Perez Ponce de Leon↩
                ]]></descr>
5200          <netbootfile/>
5201        </staticmap>
5202      </opt1>
5203      <wan>
5204        <range>
5205          <from/>
5206          <to/>
5207        </range>
5208        <defaultleasetime/>
5209        <maxleasetime/>
5210        <netmask/>
5211        <failover_peerip/>
5212        <gateway/>
5213        <domain/>
5214        <domainsearchlist/>
5215        <ddnsdomain/>
5216        <tftp/>
5217        <ldap/>
```

```
5218        <next-server/>
5219        <filename/>
5220        <rootpath/>
5221        <numberoptions/>
5222      </wan>
5223    </dhcpd>
5224    <pptpd>
5225      <mode/>
5226      <redir/>
5227      <localip/>
5228      <remoteip/>
5229    </pptpd>
5230    <dnsmasq>
5231      <enable/>
5232      <custom_options/>
5233      <hosts>
5234        <host>app</host>
5235        <domain>ib.unam.mx</domain>
5236        <ip>10.1.100.3</ip>
5237        <descr><![CDATA[Ed A primer piso]]></descr>
5238      </hosts>
5239      <hosts>
5240        <host>colecciones</host>
5241        <domain>ib.unam.mx</domain>
5242        <ip>10.1.100.7</ip>
5243        <descr><![CDATA[col]]></descr>
5244      </hosts>
5245      <hosts>
5246        <host>congresoslccs</host>
5247        <domain>unam.mx</domain>
5248        <ip>10.1.4.239</ip>
5249        <descr><![CDATA[Congreso cactaceas]]></descr>
5250      </hosts>
5251      <hosts>
5252        <host>correo</host>
5253        <domain>ib.unam.mx</domain>
5254        <ip>10.1.4.98</ip>
5255        <descr/>
5256      </hosts>
5257      <hosts>
5258        <host>jb</host>
5259        <domain>ib.unam.mx</domain>
5260        <ip>10.1.100.6</ip>
5261        <descr><![CDATA[dvr jb]]></descr>
5262      </hosts>
5263      <hosts>
5264        <host>secuenciador</host>
```

```
5265        <domain>ib.unam.mx</domain>
5266        <ip>10.1.5.240</ip>
5267        <descr><![CDATA[hacia secuenciador]]></descr>
5268      </hosts>
5269    </dnsmasq>
5270    <snmpd>
5271      <syslocation/>
5272      <syscontact/>
5273      <rocommunity>public</rocommunity>
5274    </snmpd>
5275    <diag>
5276      <ipv6nat>
5277        <ipaddr/>
5278      </ipv6nat>
5279    </diag>
5280    <bridge/>
5281    <syslog>
5282      <reverse/>
5283      <nentries>100</nentries>
5284      <filter/>
5285      <system/>
5286      <remoteserver>10.1.4.20</remoteserver>
5287      <remoteserver2/>
5288      <remoteserver3/>
5289      <dhcp/>
5290      <enable/>
5291    </syslog>
5292    <nat>
5293      <ipsecpassthru>
5294        <enable/>
5295      </ipsecpassthru>
5296      <advancedoutbound>
5297        <enable/>
5298      </advancedoutbound>
5299    </nat>
5300    <filter>
5301      <rule>
5302        <id/>
5303        <type>pass</type>
5304        <interface>lan,opt1</interface>
5305        <tag/>
5306        <tagged/>
5307        <direction>any</direction>
5308        <floating>yes</floating>
5309        <max/>
5310        <max-src-nodes/>
5311        <max-src-conn/>
```

```
5312        <max-src-states/>
5313        <statetimeout/>
5314        <statetype>keep state</statetype>
5315        <os/>
5316        <source>
5317          <any/>
5318        </source>
5319        <destination>
5320          <any/>
5321        </destination>
5322        <descr/>
5323      </rule>
5324      <rule>
5325        <id/>
5326        <type>pass</type>
5327        <interface>wan</interface>
5328        <tag/>
5329        <tagged/>
5330        <max/>
5331        <max-src-nodes/>
5332        <max-src-conn/>
5333        <max-src-states/>
5334        <statetimeout/>
5335        <statetype>keep state</statetype>
5336        <os/>
5337        <source>
5338          <any/>
5339        </source>
5340        <destination>
5341          <any/>
5342        </destination>
5343        <log/>
5344        <descr><![CDATA[Open Wan]]></descr>
5345      </rule>
5346      <rule>
5347        <id/>
5348        <type>pass</type>
5349        <interface>lan</interface>
5350        <tag/>
5351        <tagged/>
5352        <max/>
5353        <max-src-nodes/>
5354        <max-src-conn/>
5355        <max-src-states/>
5356        <statetimeout/>
5357        <statetype>keep state</statetype>
5358        <os/>
```

```
5359        <source>
5360          <any/>
5361        </source>
5362        <destination>
5363          <any/>
5364        </destination>
5365        <descr><![CDATA[Default allow LAN to any rule]]></descr>
5366      </rule>
5367      <rule>
5368        <id/>
5369        <type>pass</type>
5370        <interface>opt1</interface>
5371        <tag/>
5372        <tagged/>
5373        <max/>
5374        <max-src-nodes/>
5375        <max-src-conn/>
5376        <max-src-states/>
5377        <statetimeout/>
5378        <statetype>keep state</statetype>
5379        <os/>
5380        <source>
5381          <any/>
5382        </source>
5383        <destination>
5384          <any/>
5385        </destination>
5386        <descr/>
5387      </rule>
5388      <rule>
5389        <id/>
5390        <type>pass</type>
5391        <interface>opt2</interface>
5392        <tag/>
5393        <tagged/>
5394        <max/>
5395        <max-src-nodes/>
5396        <max-src-conn/>
5397        <max-src-states/>
5398        <statetimeout/>
5399        <statetype>keep state</statetype>
5400        <os/>
5401        <source>
5402          <any/>
5403        </source>
5404        <destination>
5405          <any/>
```

```
5406        </destination>
5407        <descr><![CDATA[Trafico administrativo]]></descr>
5408      </rule>
5409      <rule>
5410        <id/>
5411        <type>pass</type>
5412        <interface>opt3</interface>
5413        <tag/>
5414        <tagged/>
5415        <max/>
5416        <max-src-nodes/>
5417        <max-src-conn/>
5418        <max-src-states/>
5419        <statetimeout/>
5420        <statetype>keep state</statetype>
5421        <os/>
5422        <source>
5423          <any/>
5424        </source>
5425        <destination>
5426          <any/>
5427        </destination>
5428        <descr/>
5429        <dnpipe>1</dnpipe>
5430        <pdnpipe>2</pdnpipe>
5431      </rule>
5432      <rule>
5433        <id/>
5434        <type>pass</type>
5435        <interface>opt4</interface>
5436        <tag/>
5437        <tagged/>
5438        <max/>
5439        <max-src-nodes/>
5440        <max-src-conn/>
5441        <max-src-states/>
5442        <statetimeout/>
5443        <statetype>keep state</statetype>
5444        <os/>
5445        <source>
5446          <any/>
5447        </source>
5448        <destination>
5449          <any/>
5450        </destination>
5451        <descr/>
5452      </rule>
```

```
5453      <rule>
5454        <id/>
5455        <type>block</type>
5456        <interface>opt5</interface>
5457        <tag/>
5458        <tagged/>
5459        <max/>
5460        <max-src-nodes/>
5461        <max-src-conn/>
5462        <max-src-states/>
5463        <statetimeout/>
5464        <statetype>keep state</statetype>
5465        <os/>
5466        <protocol>tcp/udp</protocol>
5467        <source>
5468          <address>10.1.4.238</address>
5469        </source>
5470        <destination>
5471          <any/>
5472        </destination>
5473        <log/>
5474        <descr><![CDATA[block internet]]></descr>
5475      </rule>
5476      <rule>
5477        <id/>
5478        <type>pass</type>
5479        <interface>opt5</interface>
5480        <tag/>
5481        <tagged/>
5482        <max/>
5483        <max-src-nodes/>
5484        <max-src-conn/>
5485        <max-src-states/>
5486        <statetimeout/>
5487        <statetype>keep state</statetype>
5488        <os/>
5489        <source>
5490          <any/>
5491        </source>
5492        <destination>
5493          <any/>
5494        </destination>
5495        <descr/>
5496      </rule>
5497      <rule>
5498        <id/>
5499        <type>pass</type>
```

```
5500        <interface>opt6</interface>
5501        <tag/>
5502        <tagged/>
5503        <max/>
5504        <max-src-nodes/>
5505        <max-src-conn/>
5506        <max-src-states/>
5507        <statetimeout/>
5508        <statetype>keep state</statetype>
5509        <os/>
5510        <source>
5511          <any/>
5512        </source>
5513        <destination>
5514          <any/>
5515        </destination>
5516        <descr/>
5517        <dnpipe>1</dnpipe>
5518        <pdnpipe>2</pdnpipe>
5519      </rule>
5520      <rule>
5521        <id/>
5522        <type>pass</type>
5523        <interface>opt7</interface>
5524        <tag/>
5525        <tagged/>
5526        <max/>
5527        <max-src-nodes/>
5528        <max-src-conn/>
5529        <max-src-states/>
5530        <statetimeout/>
5531        <statetype>keep state</statetype>
5532        <os/>
5533        <source>
5534          <any/>
5535        </source>
5536        <destination>
5537          <any/>
5538        </destination>
5539        <descr/>
5540      </rule>
5541      <rule>
5542        <id/>
5543        <type>pass</type>
5544        <interface>opt8</interface>
5545        <tag/>
5546        <tagged/>
```

```
5547        <max/>
5548        <max-src-nodes/>
5549        <max-src-conn/>
5550        <max-src-states/>
5551        <statetimeout/>
5552        <statetype>keep state</statetype>
5553        <os/>
5554        <source>
5555          <any/>
5556        </source>
5557        <destination>
5558          <any/>
5559        </destination>
5560        <descr/>
5561      </rule>
5562      <rule>
5563        <id/>
5564        <type>pass</type>
5565        <interface>opt9</interface>
5566        <tag/>
5567        <tagged/>
5568        <max/>
5569        <max-src-nodes/>
5570        <max-src-conn/>
5571        <max-src-states/>
5572        <statetimeout/>
5573        <statetype>keep state</statetype>
5574        <os/>
5575        <source>
5576          <any/>
5577        </source>
5578        <destination>
5579          <any/>
5580        </destination>
5581        <descr/>
5582        <dnpipe>1</dnpipe>
5583        <pdnpipe>2</pdnpipe>
5584      </rule>
5585      <rule>
5586        <id/>
5587        <type>pass</type>
5588        <interface>opt9</interface>
5589        <tag/>
5590        <tagged/>
5591        <max/>
5592        <max-src-nodes/>
5593        <max-src-conn/>
```

```
5594        <max-src-states/>
5595        <statetimeout/>
5596        <statetype>keep state</statetype>
5597        <os/>
5598        <protocol>tcp/udp</protocol>
5599        <source>
5600          <any/>
5601        </source>
5602        <destination>
5603          <any/>
5604          <port>3050</port>
5605        </destination>
5606        <descr/>
5607      </rule>
5608      <rule>
5609        <id/>
5610        <type>pass</type>
5611        <interface>opt10</interface>
5612        <tag/>
5613        <tagged/>
5614        <max/>
5615        <max-src-nodes/>
5616        <max-src-conn/>
5617        <max-src-states/>
5618        <statetimeout/>
5619        <statetype>keep state</statetype>
5620        <os/>
5621        <source>
5622          <any/>
5623        </source>
5624        <destination>
5625          <any/>
5626        </destination>
5627        <descr/>
5628        <dnpipe>1</dnpipe>
5629        <pdnpipe>2</pdnpipe>
5630      </rule>
5631      <rule>
5632        <id/>
5633        <type>pass</type>
5634        <interface>opt11</interface>
5635        <tag/>
5636        <tagged/>
5637        <max/>
5638        <max-src-nodes/>
5639        <max-src-conn/>
5640        <max-src-states/>
```

```
5641        <statetimeout/>
5642        <statetype>keep state</statetype>
5643        <os/>
5644        <source>
5645          <any/>
5646        </source>
5647        <destination>
5648          <any/>
5649        </destination>
5650        <descr/>
5651      </rule>
5652      <rule>
5653        <id/>
5654        <type>pass</type>
5655        <interface>opt12</interface>
5656        <tag/>
5657        <tagged/>
5658        <max/>
5659        <max-src-nodes/>
5660        <max-src-conn/>
5661        <max-src-states/>
5662        <statetimeout/>
5663        <statetype>keep state</statetype>
5664        <os/>
5665        <source>
5666          <any/>
5667        </source>
5668        <destination>
5669          <any/>
5670        </destination>
5671        <descr/>
5672        <dnpipe>1</dnpipe>
5673        <pdnpipe>2</pdnpipe>
5674      </rule>
5675      <rule>
5676        <id/>
5677        <type>pass</type>
5678        <interface>opt13</interface>
5679        <tag/>
5680        <tagged/>
5681        <max/>
5682        <max-src-nodes/>
5683        <max-src-conn/>
5684        <max-src-states/>
5685        <statetimeout/>
5686        <statetype>keep state</statetype>
5687        <os/>
```

```
5688        <source>
5689          <any/>
5690        </source>
5691        <destination>
5692          <any/>
5693        </destination>
5694        <descr><![CDATA[Open cisco]]></descr>
5695      </rule>
5696    </filter>
5697    <shaper/>
5698    <ipsec>
5699      <preferoldsa/>
5700    </ipsec>
5701    <aliases/>
5702    <proxyarp/>
5703    <cron>
5704      <item>
5705        <minute>0</minute>
5706        <hour>*</hour>
5707        <mday>*</mday>
5708        <month>*</month>
5709        <wday>*</wday>
5710        <who>root</who>
5711        <command>/usr/bin/nice -n20 newsyslog</command>
5712      </item>
5713      <item>
5714        <minute>1,31</minute>
5715        <hour>0-5</hour>
5716        <mday>*</mday>
5717        <month>*</month>
5718        <wday>*</wday>
5719        <who>root</who>
5720        <command>/usr/bin/nice -n20 adjkerntz -a</command>
5721      </item>
5722      <item>
5723        <minute>1</minute>
5724        <hour>3</hour>
5725        <mday>1</mday>
5726        <month>*</month>
5727        <wday>*</wday>
5728        <who>root</who>
5729        <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command↩
             >
5730      </item>
5731      <item>
5732        <minute>*/60</minute>
5733        <hour>*</hour>
```

```
5734        <mday>*</mday>
5735        <month>*</month>
5736        <wday>*</wday>
5737        <who>root</who>
5738        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t↩
                3600 sshlockout</command>
5739      </item>
5740      <item>
5741        <minute>1</minute>
5742        <hour>1</hour>
5743        <mday>*</mday>
5744        <month>*</month>
5745        <wday>*</wday>
5746        <who>root</who>
5747        <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
5748      </item>
5749      <item>
5750        <minute>*/60</minute>
5751        <hour>*</hour>
5752        <mday>*</mday>
5753        <month>*</month>
5754        <wday>*</wday>
5755        <who>root</who>
5756        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t↩
                3600 virusprot</command>
5757      </item>
5758      <item>
5759        <minute>30</minute>
5760        <hour>12</hour>
5761        <mday>*</mday>
5762        <month>*</month>
5763        <wday>*</wday>
5764        <who>root</who>
5765        <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command↩
              >
5766      </item>
5767      <item>
5768        <task_name>squid_rotate_logs</task_name>
5769        <minute>0</minute>
5770        <hour>0</hour>
5771        <mday>*</mday>
5772        <month>*</month>
5773        <wday>*</wday>
5774        <who>root</who>
5775        <command>/bin/rm /var/squid/cache/swap.state; /usr/local/sbin↩
              /squid -k rotate</command>
5776      </item>
```

```
5777      <item>
5778        <task_name>squid_check_swapstate</task_name>
5779        <minute>*/15</minute>
5780        <hour>*</hour>
5781        <mday>*</mday>
5782        <month>*</month>
5783        <wday>*</wday>
5784        <who>root</who>
5785        <command>/usr/local/pkg/swapstate_check.php</command>
5786      </item>
5787    </cron>
5788    <wol>
5789      <wolentry>
5790        <interface>opt12</interface>
5791        <mac>00:12:17:7b:2f:3a</mac>
5792        <descr/>
5793      </wolentry>
5794      <wolentry>
5795        <interface>opt5</interface>
5796        <mac>00:10:b5:72:8d:54</mac>
5797        <descr><![CDATA[Pfsense_UDC]]></descr>
5798      </wolentry>
5799      <wolentry>
5800        <interface>opt5</interface>
5801        <mac>00:14:22:27:26:6a</mac>
5802        <descr><![CDATA[admon_ds009]]></descr>
5803      </wolentry>
5804      <wolentry>
5805        <interface>opt8</interface>
5806        <mac>64:66:b3:5d:46:1a</mac>
5807        <descr><![CDATA[ap_caseta2]]></descr>
5808      </wolentry>
5809      <wolentry>
5810        <interface>opt1</interface>
5811        <mac>68:7f:74:12:0c:1c</mac>
5812        <descr><![CDATA[ap_presup]]></descr>
5813      </wolentry>
5814    </wol>
5815    <rrd>
5816      <enable/>
5817    </rrd>
5818    <load_balancer>
5819      <monitor_type>
5820        <name>ICMP</name>
5821        <type>icmp</type>
5822        <descr><![CDATA[ICMP]]></descr>
5823        <options/>
```

```
5824      </monitor_type>
5825      <monitor_type>
5826        <name>TCP</name>
5827        <type>tcp</type>
5828        <descr><![CDATA[Generic TCP]]></descr>
5829        <options/>
5830      </monitor_type>
5831      <monitor_type>
5832        <name>HTTP</name>
5833        <type>http</type>
5834        <descr><![CDATA[Generic HTTP]]></descr>
5835        <options>
5836          <path>/</path>
5837          <host/>
5838          <code>200</code>
5839        </options>
5840      </monitor_type>
5841      <monitor_type>
5842        <name>HTTPS</name>
5843        <type>https</type>
5844        <descr><![CDATA[Generic HTTPS]]></descr>
5845        <options>
5846          <path>/</path>
5847          <host/>
5848          <code>200</code>
5849        </options>
5850      </monitor_type>
5851      <monitor_type>
5852        <name>SMTP</name>
5853        <type>send</type>
5854        <descr><![CDATA[Generic SMTP]]></descr>
5855        <options>
5856          <send>EHLO nosuchhost</send>
5857          <expect>250-</expect>
5858        </options>
5859      </monitor_type>
5860    </load_balancer>
5861    <widgets>
5862      <sequence>gateways-container:col1:show,system_information-↩
          container:col1:show,captive_portal_status-↩
          container:col1:close,carp_status-container:col1:close,↩
          cpu_graphs-container:col1:close,gmirror_status-↩
          container:col1:close,installed_packages-container:col1:close↩
          ,interface_statistics-container:col1:close,picture-↩
          container:col2:show,interfaces-container:col2:show,ipsec-↩
          container:col2:close,load_balancer_status-↩
          container:col2:close,log-container:col2:close,rss-↩
```

```
        container:col2:close,services_status-container:col2:close,↩
        traffic_graphs-container:col2:close,openvpn-↩
        container:col2:none,wake_on_lan-container:col2:none</↩
        sequence>
5863
5864    <revision>
5865      <time>1381165008</time>
5866      <description><![CDATA[admin@10.1.4.233: /services_dhcp.php made↩
            unknown change]]></description>
5867      <username>admin@10.1.4.233</username>
5868    </revision>
5869    <openvpn/>
5870    <l7shaper>
5871      <container/>
5872    </l7shaper>
5873    <dnshaper>
5874      <queue>
5875        <name>2MbS</name>
5876        <number/>
5877        <qlimit/>
5878        <plr/>
5879        <description><![CDATA[Para Evento LB]]></description>
5880        <bandwidth>2</bandwidth>
5881        <bandwidthtype>Mb</bandwidthtype>
5882        <enabled>on</enabled>
5883        <buckets/>
5884        <mask>srcaddress</mask>
5885        <delay>0</delay>
5886      </queue>
5887      <queue>
5888        <name>2MBD</name>
5889        <number/>
5890        <qlimit/>
5891        <plr/>
5892        <description/>
5893        <bandwidth>2</bandwidth>
5894        <bandwidthtype>Mb</bandwidthtype>
5895        <enabled>on</enabled>
5896        <buckets/>
5897        <mask>dstaddress</mask>
5898        <delay>0</delay>
5899      </queue>
5900    </dnshaper>
5901    <cert>
5902      <refid>4fe4a0973902d</refid>
5903      <descr><![CDATA[webConfigurator default]]></descr>
5904
```

```
5905    <ppps/>
5906    <gateways>
5907      <gateway_item>
5908        <interface>wan</interface>
5909        <gateway>10.1.10.253</gateway>
5910        <name>WANGW</name>
5911        <weight>1</weight>
5912        <descr><![CDATA[WAN Gateway]]></descr>
5913        <defaultgw/>
5914      </gateway_item>
5915      <gateway_item>
5916        <interface>opt3</interface>
5917        <gateway>10.1.2.254</gateway>
5918        <name>102gw</name>
5919        <weight>1</weight>
5920        <interval/>
5921        <descr/>
5922      </gateway_item>
5923      <gateway_item>
5924        <interface>opt4</interface>
5925        <gateway>10.1.3.254</gateway>
5926        <name>103gw</name>
5927        <weight>1</weight>
5928        <interval/>
5929        <descr/>
5930      </gateway_item>
5931      <gateway_item>
5932        <interface>opt5</interface>
5933        <gateway>10.1.4.254</gateway>
5934        <name>104gw</name>
5935        <weight>1</weight>
5936        <interval/>
5937        <descr/>
5938      </gateway_item>
5939      <gateway_item>
5940        <interface>opt6</interface>
5941        <gateway>10.1.5.254</gateway>
5942        <name>105gw</name>
5943        <weight>1</weight>
5944        <interval/>
5945        <descr/>
5946      </gateway_item>
5947      <gateway_item>
5948        <interface>opt7</interface>
5949        <gateway>10.1.7.254</gateway>
5950        <name>107gw</name>
5951        <weight>1</weight>
```

```
5952        <interval/>
5953        <descr/>
5954      </gateway_item>
5955      <gateway_item>
5956        <interface>opt8</interface>
5957        <gateway>10.1.8.254</gateway>
5958        <name>108gw</name>
5959        <weight>1</weight>
5960        <interval/>
5961        <descr/>
5962      </gateway_item>
5963      <gateway_item>
5964        <interface>opt9</interface>
5965        <gateway>10.1.9.254</gateway>
5966        <name>109gw</name>
5967        <weight>1</weight>
5968        <interval/>
5969        <descr/>
5970      </gateway_item>
5971      <gateway_item>
5972        <interface>opt10</interface>
5973        <gateway>10.1.10.254</gateway>
5974        <name>110gw</name>
5975        <weight>1</weight>
5976        <interval/>
5977        <descr/>
5978      </gateway_item>
5979      <gateway_item>
5980        <interface>opt1</interface>
5981        <gateway>10.1.118.254</gateway>
5982        <name>118gw</name>
5983        <weight>1</weight>
5984        <interval/>
5985        <descr/>
5986      </gateway_item>
5987      <gateway_item>
5988        <interface>opt2</interface>
5989        <gateway>10.1.251.14</gateway>
5990        <name>admin</name>
5991        <weight>1</weight>
5992        <interval/>
5993        <descr/>
5994      </gateway_item>
5995      <gateway_item>
5996        <interface>opt11</interface>
5997        <gateway>10.1.1.254</gateway>
5998        <name>gwCAM</name>
```

```
5999        <weight>1</weight>
6000        <interval/>
6001        <descr/>
6002      </gateway_item>
6003      <gateway_item>
6004        <interface>opt12</interface>
6005        <gateway>10.1.9.254</gateway>
6006        <name>gwifi</name>
6007        <weight>1</weight>
6008        <interval/>
6009        <descr/>
6010      </gateway_item>
6011      <gateway_item>
6012        <interface>opt13</interface>
6013        <gateway>10.1.23.254</gateway>
6014        <name>cisco</name>
6015        <weight>1</weight>
6016        <interval/>
6017        <descr><![CDATA[lab cisco]]></descr>
6018      </gateway_item>
6019    </gateways>
6020    <vlans>
6021      <vlan>
6022        <if>bce3</if>
6023        <tag>102</tag>
6024        <descr><![CDATA[A-PB]]></descr>
6025        <vlanif>bce3_vlan102</vlanif>
6026      </vlan>
6027      <vlan>
6028        <if>bce3</if>
6029        <tag>103</tag>
6030        <descr><![CDATA[A-PP,SP]]></descr>
6031        <vlanif>bce3_vlan103</vlanif>
6032      </vlan>
6033      <vlan>
6034        <if>bce3</if>
6035        <tag>104</tag>
6036        <descr><![CDATA[B-PB]]></descr>
6037        <vlanif>bce3_vlan104</vlanif>
6038      </vlan>
6039      <vlan>
6040        <if>bce3</if>
6041        <tag>105</tag>
6042        <descr><![CDATA[B-PP,SP]]></descr>
6043        <vlanif>bce3_vlan105</vlanif>
6044      </vlan>
6045      <vlan>
```

```
6046        <if>bce3</if>
6047        <tag>107</tag>
6048        <descr><![CDATA[C–PB,PP,SP]]></descr>
6049        <</prv>
6050    </cert>
6051      </vlan>
6052      <vlan>
6053        <if>bce3</if>
6054        <tag>108</tag>
6055        <descr><![CDATA[D–PB,PP,SP]]></descr>
6056        <vlanif>bce3_vlan108</vlanif>
6057      </vlan>
6058      <vlan>
6059        <if>bce3</if>
6060        <tag>109</tag>
6061        <descr><![CDATA[JB–PB]]></descr>
6062        <vlanif>bce3_vlan109</vlanif>
6063      </vlan>
6064      <vlan>
6065        <if>bce3</if>
6066        <tag>110</tag>
6067        <descr><![CDATA[COLECCIONES]]></descr>
6068        <vlanif>bce3_vlan110</vlanif>
6069      </vlan>
6070      <vlan>
6071        <if>bce3</if>
6072        <tag>118</tag>
6073        <descr><![CDATA[wifi]]></descr>
6074        <vlanif>bce3_vlan118</vlanif>
6075      </vlan>
6076      <vlan>
6077        <if>bce3</if>
6078        <tag>399</tag>
6079        <descr><![CDATA[VlanAdmin]]></descr>
6080        <vlanif>bce3_vlan399</vlanif>
6081      </vlan>
6082      <vlan>
6083        <if>bce3</if>
6084        <tag>500</tag>
6085        <descr><![CDATA[C]]></descr>
6086        <vlanif>bce3_vlan500</vlanif>
6087      </vlan>
6088      <vlan>
6089        <if>bce3</if>
6090        <tag>66</tag>
6091        <descr><![CDATA[WIFI]]></descr>
6092        <vlanif>bce3_vlan66</vlanif>
```

```
6093      </vlan>
6094      <vlan>
6095        <if>bce3</if>
6096        <tag>23</tag>
6097        <descr><![CDATA[Laboratorio Cisco]]></descr>
6098        <vlanif>bce3_vlan23</vlanif>
6099      </vlan>
6100    </vlans>
6101    <installedpackages>
6102      <menu>
6103        <name>NMap</name>
6104        <tooltiptext>NMap is a utility for network exploration or ↩
              security auditing. It supports ping scanning (determine ↩
              which hosts are up), many port scanning techniques (↩
              determine what services the hosts are offering), version ↩
              detection (determine what application/service is runing on↩
               a port), and TCP/IP fingerprinting (remote host OS or ↩
              device identification). It also offers flexible target and↩
               port specification, decoy/stealth scanning, SunRPC ↩
              scanning, and more. Most Unix and Windows platforms are ↩
              supported in both GUI and command line modes. Several ↩
              popular handheld devices are also supported, including the↩
               Sharp Zaurus and the iPAQ.</tooltiptext>
6105        <section>Diagnostics</section>
6106        <configfile>nmap.xml</configfile>
6107      </menu>
6108      <menu>
6109        <name>phpsysinfo</name>
6110        <tooltiptext/>
6111        <section>Status</section>
6112        <url>/pkg_edit.php?xml=phpsysinfo.xml&amp;id=0</url>
6113      </menu>
6114      <menu>
6115        <name>BandwidthD</name>
6116        <tooltiptext/>
6117        <section>Services</section>
6118        <url>/pkg_edit.php?xml=bandwidthd.xml&amp;id=0</url>
6119      </menu>
6120      <menu>
6121        <name>TFTP</name>
6122        <tooltiptext>Add or Remove files for TFTP.</tooltiptext>
6123        <section>Services</section>
6124        <configfile>tftp.xml</configfile>
6125        <url>tftp_files.php</url>
6126      </menu>
6127      <menu>
6128        <name>Proxy server</name>
```

```
6129        <tooltiptext>Modify the proxy servers settings</tooltiptext>
6130        <section>Services</section>
6131        <url>/pkg_edit.php?xml=squid.xml&amp;id=0</url>
6132      </menu>
6133      <menu>
6134        <name>Dansguardian</name>
6135        <tooltiptext>Configure dansguardian</tooltiptext>
6136        <section>Services</section>
6137        <url>/pkg_edit.php?xml=dansguardian.xml</url>
6138      </menu>
6139      <service/>
6140      <service>
6141        <name>bandwidthd</name>
6142        <rcfile>bandwidthd.sh</rcfile>
6143        <executable>bandwidthd</executable>
6144      </service>
6145      <service>
6146        <name>tftp</name>
6147        <executable>inetd</executable>
6148        <description><![CDATA[Trivial File Transport Protocol is a ↩
              very simple file transfer protocol. Often used with ↩
              routers, voip phones and more.]]></description>
6149      </service>
6150      <service>
6151        <name>squid</name>
6152        <rcfile>squid.sh</rcfile>
6153        <executable>squid</executable>
6154        <description><![CDATA[Proxy server Service]]></description>
6155      </service>
6156      <service>
6157        <name>dansguardian</name>
6158        <rcfile>dansguardian</rcfile>
6159        <executable>dansguardian</executable>
6160        <description><![CDATA[Award winning Open Source web content ↩
              filter]]></description>
6161      </service>
6162      <package>
6163        <name>nmap</name>
6164        <maintainer>jimp@pfsense.org</maintainer>
6165        <descr><![CDATA[NMap is a utility for network exploration or ↩
              security auditing. It supports ping scanning (determine ↩
              which hosts are up), many port scanning techniques (↩
              determine what services the hosts are offering), version ↩
              detection (determine what application/service is runing on↩
               a port), and TCP/IP fingerprinting (remote host OS or ↩
              device identification). It also offers flexible target and↩
               port specification, decoy/stealth scanning, SunRPC ↩
```

```
        scanning, and more. Most Unix and Windows platforms are ↩
        supported in both GUI and command line modes. Several ↩
        popular handheld devices are also supported, including the↩
         Sharp Zaurus and the iPAQ.]]></descr>
6166    <category>Security</category>
6167    <depends_on_package_base_url>http://files.pfsense.org/↩
        packages/amd64/8/All/</depends_on_package_base_url>
6168    <depends_on_package>lua-5.1.5_4.tbz</depends_on_package>
6169    <depends_on_package>nmap-6.01.tbz</depends_on_package>
6170    <depends_on_package>libpcap-1.2.1.tbz</depends_on_package>
6171    <depends_on_package_pbi>nmap-6.01_1-amd64.pbi</↩
        depends_on_package_pbi>
6172    <config_file>http://www.pfsense.com/packages/config/nmap/nmap↩
        .xml</config_file>
6173    <version>nmap-6.01 pkg v1.2</version>
6174    <status>Stable</status>
6175    <pkginfolink>http://doc.pfsense.org/index.php/Nmap_package</↩
        pkginfolink>
6176    <required_version>2.0</required_version>
6177    <configurationfile>nmap.xml</configurationfile>
6178    <build_port_path>/usr/ports/security/nmap</build_port_path>
6179  </package>
6180  <package>
6181    <name>phpSysInfo</name>
6182    <website>http://phpsysinfo.sourceforge.net/</website>
6183    <descr><![CDATA[PHPSysInfo is a customizable PHP Script that ↩
        parses /proc, and formats information nicely. It will ↩
        display information about system facts like Uptime, CPU, ↩
        Memory, PCI devices, SCSI devices, IDE devices, Network ↩
        adapters, Disk usage, and more.]]></descr>
6184    <category>System</category>
6185    <version>2.5.4</version>
6186    <status>Beta</status>
6187    <required_version>1.0</required_version>
6188    <depends_on_package_base_url>http://files.pfsense.org/↩
        packages/amd64/8/All/</depends_on_package_base_url>
6189    <depends_on_package>mbmon-205_5.tbz</depends_on_package>
6190    <depends_on_package_pbi>mbmon-205_6-amd64.pbi</↩
        depends_on_package_pbi>
6191    <build_port_path>/usr/ports/sysutils/mbmon</build_port_path>
6192    <config_file>http://www.pfsense.com/packages/config/↩
        phpsysinfo/phpsysinfo.xml</config_file>
6193    <configurationfile>phpsysinfo.xml</configurationfile>
6194    <noembedded>true</noembedded>
6195  </package>
6196  <package>
6197    <name>bandwidthd</name>
```

```
6198        <website>http://bandwidthd.sourceforge.net/</website>
6199        <descr><![CDATA[BandwidthD tracks usage of TCP/IP network ↩
               subnets and builds html files with graphs to display ↩
               utilization. Charts are built by individual IPs, and by ↩
               default display utilization over 2 day, 8 day, 40 day, and↩
                400 day periods. Furthermore, each ip address utilization↩
                can be logged out at intervals of 3.3 minutes, 10 minutes↩
               , 1 hour or 12 hours in cdf format, or to a backend ↩
               database server. HTTP, TCP, UDP, ICMP, VPN, and P2P ↩
               traffic are color coded.]]></descr>
6200        <category>System</category>
6201        <version>2.0.1_5</version>
6202        <status>BETA</status>
6203        <required_version>1.2.1</required_version>
6204        <depends_on_package_base_url>http://files.pfsense.org/↩
               packages/amd64/8/All/</depends_on_package_base_url>
6205        <depends_on_package>bandwidthd-2.0.1_5.tbz</↩
               depends_on_package>
6206        <depends_on_package>libpcap-1.1.1.tbz</depends_on_package>
6207        <depends_on_package>postgresql-client-8.4.12.tbz</↩
               depends_on_package>
6208        <depends_on_package_pbi>bandwidthd-2.0.1_5-amd64.pbi</↩
               depends_on_package_pbi>
6209        <config_file>http://www.pfsense.org/packages/config/↩
               bandwidthd/bandwidthd.xml</config_file>
6210        <configurationfile>bandwidthd.xml</configurationfile>
6211        <build_port_path>/usr/ports/net/libpcap</build_port_path>
6212        <build_port_path>/usr/ports/databases/postgresql84-client</↩
               build_port_path>
6213        <build_port_path>/usr/ports/net-mgmt/bandwidthd</↩
               build_port_path>
6214        <build_pbi>
6215          <ports_before>net/libpcap databases/postgresql91-client ↩
                 graphics/gd</ports_before>
6216          <port>net-mgmt/bandwidthd</port>
6217        </build_pbi>
6218        <build_options>WITH_NLS=true;WITHOUT_PAM=true;WITHOUT_LDAP=↩
               true;WITHOUT_MIT_KRB5=true;WITHOUT_HEIMDAL_KRB5=true;↩
               WITHOUT_OPTIMIZED_CFLAGS=true;WITHOUT_XML=true;↩
               WITHOUT_TZDATA=true;WITHOUT_DEBUG=true;WITHOUT_GSSAPI=true↩
               ;WITHOUT_ICU=true;WITH_INTDATE=true</build_options>
6219      </package>
6220      <package>
6221        <name>TFTP</name>
6222        <website/>
6223        <descr><![CDATA[Trivial File Transport Protocol is a very ↩
               simple file transfer protocol. Often used with routers, ↩
```

```
        voip phones and more.]]></descr>
6224    <category>Services</category>
6225    <pkginfolink/>
6226    <config_file>http://www.pfsense.com/packages/config/tftp2/↩
        tftp.xml</config_file>
6227    <depends_on_package_base_url>http://files.pfsense.org/↩
        packages/amd64/8/All/</depends_on_package_base_url>
6228    <version>2.0</version>
6229    <status>Stable</status>
6230    <required_version>2.0</required_version>
6231    <configurationfile>tftp.xml</configurationfile>
6232    <filter_rule_function>tftp_generate_rules</↩
        filter_rule_function>
6233  </package>
6234  <package>
6235    <name>squid</name>
6236    <descr><![CDATA[High performance web proxy cache.]]></descr>
6237    <website>http://www.squid-cache.org/</website>
6238    <category>Network</category>
6239    <version>2.7.9 pkg v.4.3.3</version>
6240    <status>Stable</status>
6241    <required_version>2</required_version>
6242    <maintainer>fernando@netfilter.com.br seth.mos@dds.nl ↩
        mfuchs77@googlemail.com jimp@pfsense.org</maintainer>
6243    <depends_on_package_base_url>http://files.pfsense.org/↩
        packages/amd64/8/All/</depends_on_package_base_url>
6244    <depends_on_package>squid-2.7.9_3.tbz</depends_on_package>
6245    <depends_on_package>squid_radius_auth-1.10.tbz</↩
        depends_on_package>
6246    <depends_on_package>libwww-5.4.0_4.tbz</depends_on_package>
6247    <depends_on_package_pbi>squid-2.7.9_3-amd64.pbi</↩
        depends_on_package_pbi>
6248    <build_port_path>/usr/ports/www/squid</build_port_path>
6249    <build_port_path>/usr/ports/www/squid_radius_auth</↩
        build_port_path>
6250    <build_port_path>/usr/ports/www/libwww</build_port_path>
6251    <build_pbi>
6252      <ports_before>www/libwww</ports_before>
6253      <port>www/squid</port>
6254      <ports_after>www/squid_radius_auth</ports_after>
6255    </build_pbi>
6256    <build_options>squid_UNSET=DNS_HELPER IPFILTER PINGER ↩
        STACKTRACES STRICT_HTTP_DESC USERAGENT_LOG WCCPV2;↩
        squid_SET=PF LDAP_AUTH NIS_AUTH SASL_AUTH ARP_ACL AUFS ↩
        CACHE_DIGESTS CARP COSS DELAY_POOLS FOLLOW_XFF HTCP IDENT ↩
        KERB_AUTH KQUEUE LARGEFILE REFERER_LOG SNMP SSL VIA_DB ↩
        WCCP;SQUID_UID=proxy;SQUID_GID=proxy</build_options>
```

```
6257        <config_file>http://www.pfsense.org/packages/config/squid/↩
                squid.xml</config_file>
6258        <configurationfile>squid.xml</configurationfile>
6259      </package>
6260      <package>
6261        <name>Dansguardian</name>
6262        <website>http://www.dansguardian.org/</website>
6263        <descr><![CDATA[DansGuardian is an award winning Open Source ↩
                web content filter.&lt;br /&gt;
6264                  It filters the actual content of pages based on many ↩
                      methods including phrase matching, PICS filtering ↩
                      and URL filtering.&lt;br /&gt;
6265                  It does not purely filter based on a banned list of ↩
                      sites like lesser totally commercial filters.&lt;br ↩
                      /&gt;
6266                  For all non-commercial its free, without cost.&lt;br /&↩
                      gt;
6267                  For all commercial use visit dansguardian website to ↩
                      get a licence.]]></descr>
6268        <category>Services</category>
6269        <config_file>http://www.pfsense.com/packages/config/↩
                dansguardian/dansguardian.xml</config_file>
6270        <pkginfolink>http://forum.pfsense.org/index.php/topic↩
                ,43786.0.html</pkginfolink>
6271        <depends_on_package_base_url>http://files.pfsense.org/↩
                packages/amd64/8/All/</depends_on_package_base_url>
6272        <depends_on_package>dansguardian-2.12.0.3.tbz</↩
                depends_on_package>
6273        <depends_on_package>ca_root_nss-3.14.1.tbz</↩
                depends_on_package>
6274        <depends_on_package_pbi>dansguardian-2.12.0.3-amd64.pbi</↩
                depends_on_package_pbi>
6275        <version>2.12.0.3 pkg v.0.1.8</version>
6276        <status>beta</status>
6277        <required_version>2.0</required_version>
6278        <configurationfile>dansguardian.xml</configurationfile>
6279        <build_port_path>/usr/ports/www/dansguardian-devel</↩
                build_port_path>
6280        <build_port_path>/usr/ports/www/ca_root_nss</build_port_path>
6281        <build_options>dansguardian-devel_UNSET=APACHE;dansguardian-↩
                devel_SET=TRICKLE CLAMD ICAP NTLM SSL</build_options>
6282      </package>
6283      <phpsysinfo>
6284        <config>
6285          <hidepicklist/>
6286          <sensorprogram/>
6287          <showmountpoint>on</showmountpoint>
```

```
6288          <showinodes>on</showinodes>
6289          <loadbar>on</loadbar>
6290          <showerrors/>
6291        </config>
6292      </phpsysinfo>
6293      <bandwidthd>
6294        <config>
6295          <enable>on</enable>
6296          <active_interface>wan</active_interface>
6297          <subnets_custom>10.1.0.0/16</subnets_custom>
6298          <skipintervals/>
6299          <graphcutoff/>
6300          <promiscuous>on</promiscuous>
6301          <outputcdf/>
6302          <recovercdf>on</recovercdf>
6303          <filter/>
6304          <drawgraphs>on</drawgraphs>
6305          <meta_refresh/>
6306          <graph_log_info/>
6307        </config>
6308      </bandwidthd>
6309      <tab>
6310        <text>General</text>
6311        <url>/pkg_edit.php?xml=squid.xml&amp;id=0</url>
6312        <active/>
6313      </tab>
6314      <dansguardian>
6315        <config>
6316          <interface>lo0</interface>
6317          <daemon_options>softrestart</daemon_options>
6318        </config>
6319      </dansguardian>
6320      <dansguardianconfig>
6321        <config>
6322          <auth_plugin/>
6323          <scan_options>scancleancache,createlistcachefiles,↩
                 deletedownloadedtempfiles</scan_options>
6324          <weightedphrasemode>2</weightedphrasemode>
6325          <preservecase>0</preservecase>
6326          <phrasefiltermode>2</phrasefiltermode>
6327          <cron>day</cron>
6328        </config>
6329      </dansguardianconfig>
6330      <dansguardianlog>
6331        <config>
6332          <report_level>3</report_level>
6333          <report_language>ukenglish</report_language>
```

```
6334          <report_options>showweightedfound,usecustombannedimage,↩
                  nonstandarddelimiter</report_options>
6335          <logging_options>logconnectionhandlingerrors</↩
                  logging_options>
6336          <loglevel>2</loglevel>
6337          <logexceptionhits>2</logexceptionhits>
6338          <logfileformat>1</logfileformat>
6339
6340      </dansguardianlog>
6341      <dansguardianphraseacl>
6342        <config>
6343          <name>Default</name>
6344          <description><![CDATA[Default Phrase access list setup]]></↩
                  description>
6345          <banned_enabled>on</banned_enabled>
6346          <weighted_enabled>on</weighted_enabled>
6347          <exception_enabled>on</exception_enabled>
6348          <banned_includes>/usr/local/etc/dansguardian/lists/↩
                  phraselists/safelabel/banned,/usr/local/etc/dansguardian↩
                  /lists/phraselists/pornography/banned</banned_includes>
6349          <weighted_includes>/usr/local/etc/dansguardian/lists/↩
                  phraselists/goodphrases/weighted_general,/usr/local/etc/↩
                  dansguardian/lists/phraselists/goodphrases/weighted_news↩
                  ,/usr/local/etc/dansguardian/lists/phraselists/↩
                  goodphrases/weighted_general_danish,/usr/local/etc/↩
                  dansguardian/lists/phraselists/goodphrases/↩
                  weighted_general_dutch,/usr/local/etc/dansguardian/lists↩
                  /phraselists/goodphrases/weighted_general_malay,/usr/↩
                  local/etc/dansguardian/lists/phraselists/goodphrases/↩
                  weighted_general_polish,/usr/local/etc/dansguardian/↩
                  lists/phraselists/goodphrases/↩
                  weighted_general_portuguese,/usr/local/etc/dansguardian/↩
                  lists/phraselists/goodphrases/weighted_general_swedish,/↩
                  usr/local/etc/dansguardian/lists/phraselists/pornography↩
                  /weighted,/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_chinese,/usr/local/etc/dansguardian↩
                  /lists/phraselists/pornography/weighted_danish,/usr/↩
                  local/etc/dansguardian/lists/phraselists/pornography/↩
                  weighted_dutch,/usr/local/etc/dansguardian/lists/↩
                  phraselists/pornography/weighted_
6350  french,/usr/local/etc/dansguardian/lists/phraselists/pornography/↩
        weighted_german,/usr/local/etc/dansguardian/lists/phraselists/↩
        pornography/weighted_italian,/usr/local/etc/dansguardian/lists/↩
        phraselists/pornography/weighted_japanese,/usr/local/etc/↩
        dansguardian/lists/phraselists/pornography/weighted_malay,/usr/↩
        local/etc/dansguardian/lists/phraselists/pornography/↩
        weighted_norwegian,/usr/local/etc/dansguardian/lists/phraselists↩
```

```
      /pornography/weighted_polish,/usr/local/etc/dansguardian/lists/↩
      phraselists/pornography/weighted_portuguese,/usr/local/etc/↩
      dansguardian/lists/phraselists/pornography/weighted_russian,/usr↩
      /local/etc/dansguardian/lists/phraselists/pornography/↩
      weighted_russian_utf8,/usr/local/etc/dansguardian/lists/↩
      phraselists/pornography/weighted_spanish,/usr/local/etc/↩
      dansguardian/lists/phraselists/pornography/weighted_swedish,/usr↩
      /local/etc/dansguardian/lists/phraselists/nudism/weighted,/usr/↩
      local/etc/dansguardian/lists/phraselists/badwords/weighted_dutch↩
      ,/usr/local/etc/dansguardian/lists/phraselists/
6351  badwords/weighted_french,/usr/local/etc/dansguardian/lists/↩
      phraselists/badwords/weighted_german,/usr/local/etc/dansguardian↩
      /lists/phraselists/badwords/weighted_portuguese,/usr/local/etc/↩
      dansguardian/lists/phraselists/badwords/weighted_spanish,/usr/↩
      local/etc/dansguardian/lists/phraselists/malware/weighted,/usr/↩
      local/etc/dansguardian/lists/phraselists/proxies/weighted,/usr/↩
      local/etc/dansguardian/lists/phraselists/warezhacking/weighted</↩
      weighted_includes>
6352              </config>
6353     </dansguardianphraseacl>
6354     <dansguardiansiteacl>
6355       <config>
6356         <name>Default</name>
6357         <description><![CDATA[Default Site access list setup]]></↩
               description>
6358         <exceptionsite_enabled>on</exceptionsite_enabled>
6359         <bannedsite_enabled>on</bannedsite_enabled>
6360         <greysite_enabled>on</greysite_enabled>
6361         <urlsite_enabled>on</urlsite_enabled>
6362             </config>
6363     </dansguardiansiteacl>
6364     <dansguardianurlacl>
6365       <config>
6366         <name>Default</name>
6367         <description><![CDATA[Default Url access list setup]]></↩
               description>
6368         <bannedurl_enabled>on</bannedurl_enabled>
6369         <exceptionurl_enabled>on</exceptionurl_enabled>
6370         <contenturl_enabled>on</contenturl_enabled>
6371         <greyurl_enabled>on</greyurl_enabled>
6372               </config>
6373     </dansguardianpicsacl>
6374     <dansguardiansearchacl>
6375       <config>
6376         <name>Default</name>
6377         <description><![CDATA[Default search engine list setup]]></↩
               description>
```

```
6378          <searchengineregexplist/>
6379          <banned_searchtermlist/>
6380          <weighted_searchtermlist/>
6381          <exception_searchtermlist/>
6382        </config>
6383      </dansguardiansearchacl>
6384      <dansguardianfileacl>
6385        <config>
6386          <name>Default</name>
6387          <description><![CDATA[Default file access list setup]]></↩
                description>
6388          <exception_enabled>on</exception_enabled>
6389          <banned_enabled>on</banned_enabled>
6390            </dansguardianheaderacl>
6391      <dansguardiancontentacl>
6392        <config>
6393          <name>Default</name>
6394          <description><![CDATA[Default content setup]]></description↩
                >
6395                  </config>
6396      </dansguardiancontentacl>
6397      <dansguardianantivirusacl>
6398        <config>
6399                  </config>
6400      </dansguardianantivirusacl>
6401      <dansguardianips>
6402        <config>
6403          <     </config>
6404      </dansguardianips>
6405      <dansguardiangroups>
6406        <config>
6407          <name>Default</name>
6408          <description><![CDATA[Default dansguardian filtergroup]]></↩
                description>
6409          <picsacl>Default</picsacl>
6410          <phraseacl>Default</phraseacl>
6411          <siteacl>Default</siteacl>
6412          <extensionacl>Default</extensionacl>
6413          <headeracl>Default</headeracl>
6414          <contentacl>Default</contentacl>
6415          <searchacl>Default</searchacl>
6416          <urlacl>Default</urlacl>
6417          <group_options>scancleancache,infectionbypasserrorsonly</↩
                group_options>
6418          <reportinglevel>3</reportinglevel>
6419          <group_name_source>name</group_name_source>
6420          <mode>1</mode>
```

```
6421          <report_level>global</report_level>
6422        </config>
6423      </dansguardiangroups>
6424      <dansguardianphraselistsweighted>
6425        <config>
6426          <descr><![CDATA[badwords weighted_dutch]]></descr>
6427          <list>badwords</list>
6428          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                badwords/weighted_dutch</file>
6429        </config>
6430        <config>
6431          <descr><![CDATA[badwords weighted_french]]></descr>
6432          <list>badwords</list>
6433          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                badwords/weighted_french</file>
6434        </config>
6435        <config>
6436          <descr><![CDATA[badwords weighted_german]]></descr>
6437          <list>badwords</list>
6438          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                badwords/weighted_german</file>
6439        </config>
6440        <config>
6441          <descr><![CDATA[badwords weighted_portuguese]]></descr>
6442          <list>badwords</list>
6443          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                badwords/weighted_portuguese</file>
6444        </config>
6445        <config>
6446          <descr><![CDATA[badwords weighted_spanish]]></descr>
6447          <list>badwords</list>
6448          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                badwords/weighted_spanish</file>
6449        </config>
6450        <config>
6451          <descr><![CDATA[chat weighted]]></descr>
6452          <list>chat</list>
6453          <file>/usr/local/etc/dansguardian/lists/phraselists/chat/↩
                weighted</file>
6454        </config>
6455        <config>
6456          <descr><![CDATA[chat weighted_italian]]></descr>
6457          <list>chat</list>
6458          <file>/usr/local/etc/dansguardian/lists/phraselists/chat/↩
                weighted_italian</file>
6459        </config>
6460        <config>
```

```
6461          <descr><![CDATA[conspiracy weighted]]></descr>
6462          <list>conspiracy</list>
6463          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 conspiracy/weighted</file>
6464        </config>
6465        <config>
6466          <descr><![CDATA[domainsforsale weighted]]></descr>
6467          <list>domainsforsale</list>
6468          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 domainsforsale/weighted</file>
6469        </config>
6470        <config>
6471          <descr><![CDATA[drugadvocacy weighted]]></descr>
6472          <list>drugadvocacy</list>
6473          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 drugadvocacy/weighted</file>
6474        </config>
6475        <config>
6476          <descr><![CDATA[forums weighted]]></descr>
6477          <list>forums</list>
6478          <file>/usr/local/etc/dansguardian/lists/phraselists/forums/↩
                 weighted</file>
6479        </config>
6480        <config>
6481          <descr><![CDATA[gambling weighted]]></descr>
6482          <list>gambling</list>
6483          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 gambling/weighted</file>
6484        </config>
6485        <config>
6486          <descr><![CDATA[gambling weighted_portuguese]]></descr>
6487          <list>gambling</list>
6488          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 gambling/weighted_portuguese</file>
6489        </config>
6490        <config>
6491          <descr><![CDATA[games weighted]]></descr>
6492          <list>games</list>
6493          <file>/usr/local/etc/dansguardian/lists/phraselists/games/↩
                 weighted</file>
6494        </config>
6495        <config>
6496          <descr><![CDATA[goodphrases weighted_general]]></descr>
6497          <list>goodphrases</list>
6498          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 goodphrases/weighted_general</file>
6499        </config>
```

```
6500        <config>
6501          <descr><![CDATA[goodphrases weighted_general_danish]]></descr>
6502          <list>goodphrases</list>
6503          <file>/usr/local/etc/dansguardian/lists/phraselists/goodphrases/weighted_general_danish</file>
6504        </config>
6505        <config>
6506          <descr><![CDATA[goodphrases weighted_general_dutch]]></descr>
6507          <list>goodphrases</list>
6508          <file>/usr/local/etc/dansguardian/lists/phraselists/goodphrases/weighted_general_dutch</file>
6509        </config>
6510        <config>
6511          <descr><![CDATA[goodphrases weighted_general_malay]]></descr>
6512          <list>goodphrases</list>
6513          <file>/usr/local/etc/dansguardian/lists/phraselists/goodphrases/weighted_general_malay</file>
6514        </config>
6515        <config>
6516          <descr><![CDATA[goodphrases weighted_general_polish]]></descr>
6517          <list>goodphrases</list>
6518          <file>/usr/local/etc/dansguardian/lists/phraselists/goodphrases/weighted_general_polish</file>
6519        </config>
6520        <config>
6521          <descr><![CDATA[goodphrases weighted_general_portuguese]]></descr>
6522          <list>goodphrases</list>
6523          <file>/usr/local/etc/dansguardian/lists/phraselists/goodphrases/weighted_general_portuguese</file>
6524        </config>
6525        <config>
6526          <descr><![CDATA[goodphrases weighted_general_swedish]]></descr>
6527          <list>goodphrases</list>
6528          <file>/usr/local/etc/dansguardian/lists/phraselists/goodphrases/weighted_general_swedish</file>
6529        </config>
6530        <config>
6531          <descr><![CDATA[goodphrases weighted_news]]></descr>
6532          <list>goodphrases</list>
6533          <file>/usr/local/etc/dansguardian/lists/phraselists/goodphrases/weighted_news</file>
```

```
6534        </config>
6535        <config>
6536          <descr><![CDATA[gore weighted]]></descr>
6537          <list>gore</list>
6538          <file>/usr/local/etc/dansguardian/lists/phraselists/gore/↩
                weighted</file>
6539        </config>
6540        <config>
6541          <descr><![CDATA[gore weighted_portuguese]]></descr>
6542          <list>gore</list>
6543          <file>/usr/local/etc/dansguardian/lists/phraselists/gore/↩
                weighted_portuguese</file>
6544        </config>
6545        <config>
6546          <descr><![CDATA[idtheft weighted]]></descr>
6547          <list>idtheft</list>
6548          <file>/usr/local/etc/dansguardian/lists/phraselists/idtheft↩
                /weighted</file>
6549        </config>
6550        <config>
6551          <descr><![CDATA[illegaldrugs weighted]]></descr>
6552          <list>illegaldrugs</list>
6553          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                illegaldrugs/weighted</file>
6554        </config>
6555        <config>
6556          <descr><![CDATA[illegaldrugs weighted_portuguese]]></descr>
6557          <list>illegaldrugs</list>
6558          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                illegaldrugs/weighted_portuguese</file>
6559        </config>
6560        <config>
6561          <descr><![CDATA[intolerance weighted]]></descr>
6562          <list>intolerance</list>
6563          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                intolerance/weighted</file>
6564        </config>
6565        <config>
6566          <descr><![CDATA[intolerance weighted_portuguese]]></descr>
6567          <list>intolerance</list>
6568          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                intolerance/weighted_portuguese</file>
6569        </config>
6570        <config>
6571          <descr><![CDATA[legaldrugs weighted]]></descr>
6572          <list>legaldrugs</list>
```

```
6573          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 legaldrugs/weighted</file>
6574        </config>
6575        <config>
6576          <descr><![CDATA[malware weighted]]></descr>
6577          <list>malware</list>
6578          <file>/usr/local/etc/dansguardian/lists/phraselists/malware↩
                 /weighted</file>
6579        </config>
6580        <config>
6581          <descr><![CDATA[music weighted]]></descr>
6582          <list>music</list>
6583          <file>/usr/local/etc/dansguardian/lists/phraselists/music/↩
                 weighted</file>
6584        </config>
6585        <config>
6586          <descr><![CDATA[news weighted]]></descr>
6587          <list>news</list>
6588          <file>/usr/local/etc/dansguardian/lists/phraselists/news/↩
                 weighted</file>
6589        </config>
6590        <config>
6591          <descr><![CDATA[nudism weighted]]></descr>
6592          <list>nudism</list>
6593          <file>/usr/local/etc/dansguardian/lists/phraselists/nudism/↩
                 weighted</file>
6594        </config>
6595        <config>
6596          <descr><![CDATA[peer2peer weighted]]></descr>
6597          <list>peer2peer</list>
6598          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 peer2peer/weighted</file>
6599        </config>
6600        <config>
6601          <descr><![CDATA[personals weighted]]></descr>
6602          <list>personals</list>
6603          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 personals/weighted</file>
6604        </config>
6605        <config>
6606          <descr><![CDATA[personals weighted_portuguese]]></descr>
6607          <list>personals</list>
6608          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 personals/weighted_portuguese</file>
6609        </config>
6610        <config>
6611          <descr><![CDATA[pornography weighted]]></descr>
```

```
6612          <list>pornography</list>
6613          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted</file>
6614        </config>
6615        <config>
6616          <descr><![CDATA[pornography weighted_chinese]]></descr>
6617          <list>pornography</list>
6618          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_chinese</file>
6619        </config>
6620        <config>
6621          <descr><![CDATA[pornography weighted_danish]]></descr>
6622          <list>pornography</list>
6623          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_danish</file>
6624        </config>
6625        <config>
6626          <descr><![CDATA[pornography weighted_dutch]]></descr>
6627          <list>pornography</list>
6628          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_dutch</file>
6629        </config>
6630        <config>
6631          <descr><![CDATA[pornography weighted_french]]></descr>
6632          <list>pornography</list>
6633          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_french</file>
6634        </config>
6635        <config>
6636          <descr><![CDATA[pornography weighted_german]]></descr>
6637          <list>pornography</list>
6638          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_german</file>
6639        </config>
6640        <config>
6641          <descr><![CDATA[pornography weighted_italian]]></descr>
6642          <list>pornography</list>
6643          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_italian</file>
6644        </config>
6645        <config>
6646          <descr><![CDATA[pornography weighted_japanese]]></descr>
6647          <list>pornography</list>
6648          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_japanese</file>
6649        </config>
6650        <config>
```

```
6651          <descr><![CDATA[pornography weighted_malay]]></descr>
6652          <list>pornography</list>
6653          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_malay</file>
6654        </config>
6655        <config>
6656          <descr><![CDATA[pornography weighted_norwegian]]></descr>
6657          <list>pornography</list>
6658          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_norwegian</file>
6659        </config>
6660        <config>
6661          <descr><![CDATA[pornography weighted_polish]]></descr>
6662          <list>pornography</list>
6663          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_polish</file>
6664        </config>
6665        <config>
6666          <descr><![CDATA[pornography weighted_portuguese]]></descr>
6667          <list>pornography</list>
6668          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_portuguese</file>
6669        </config>
6670        <config>
6671          <descr><![CDATA[pornography weighted_russian]]></descr>
6672          <list>pornography</list>
6673          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_russian</file>
6674        </config>
6675        <config>
6676          <descr><![CDATA[pornography weighted_russian_utf8]]></descr↩
                 >
6677          <list>pornography</list>
6678          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_russian_utf8</file>
6679        </config>
6680        <config>
6681          <descr><![CDATA[pornography weighted_spanish]]></descr>
6682          <list>pornography</list>
6683          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_spanish</file>
6684        </config>
6685        <config>
6686          <descr><![CDATA[pornography weighted_swedish]]></descr>
6687          <list>pornography</list>
6688          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_swedish</file>
```

```
6689        </config>
6690        <config>
6691          <descr><![CDATA[proxies weighted]]></descr>
6692          <list>proxies</list>
6693          <file>/usr/local/etc/dansguardian/lists/phraselists/proxies↩
                /weighted</file>
6694        </config>
6695        <config>
6696          <descr><![CDATA[secretsocieties weighted]]></descr>
6697          <list>secretsocieties</list>
6698          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                secretsocieties/weighted</file>
6699        </config>
6700        <config>
6701          <descr><![CDATA[sport weighted]]></descr>
6702          <list>sport</list>
6703          <file>/usr/local/etc/dansguardian/lists/phraselists/sport/↩
                weighted</file>
6704        </config>
6705        <config>
6706          <descr><![CDATA[translation weighted]]></descr>
6707          <list>translation</list>
6708          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                translation/weighted</file>
6709        </config>
6710        <config>
6711          <descr><![CDATA[travel weighted]]></descr>
6712          <list>travel</list>
6713          <file>/usr/local/etc/dansguardian/lists/phraselists/travel/↩
                weighted</file>
6714        </config>
6715        <config>
6716          <descr><![CDATA[upstreamfilter weighted]]></descr>
6717          <list>upstreamfilter</list>
6718          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                upstreamfilter/weighted</file>
6719        </config>
6720        <config>
6721          <descr><![CDATA[violence weighted]]></descr>
6722          <list>violence</list>
6723          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                violence/weighted</file>
6724        </config>
6725        <config>
6726          <descr><![CDATA[violence weighted_portuguese]]></descr>
6727          <list>violence</list>
```

```
6728          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  violence/weighted_portuguese</file>
6729        </config>
6730        <config>
6731          <descr><![CDATA[warezhacking weighted]]></descr>
6732          <list>warezhacking</list>
6733          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  warezhacking/weighted</file>
6734        </config>
6735        <config>
6736          <descr><![CDATA[weapons weighted]]></descr>
6737          <list>weapons</list>
6738          <file>/usr/local/etc/dansguardian/lists/phraselists/weapons↩
                  /weighted</file>
6739        </config>
6740        <config>
6741          <descr><![CDATA[weapons weighted_portuguese]]></descr>
6742          <list>weapons</list>
6743          <file>/usr/local/etc/dansguardian/lists/phraselists/weapons↩
                  /weighted_portuguese</file>
6744        </config>
6745        <config>
6746          <descr><![CDATA[webmail weighted]]></descr>
6747          <list>webmail</list>
6748          <file>/usr/local/etc/dansguardian/lists/phraselists/webmail↩
                  /weighted</file>
6749        </config>
6750      </dansguardianphraselistsweighted>
6751      <dansguardianphraselistsbanned>
6752        <config>
6753          <descr><![CDATA[gambling banned]]></descr>
6754          <list>gambling</list>
6755          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  gambling/banned</file>
6756        </config>
6757        <config>
6758          <descr><![CDATA[gambling banned_portuguese]]></descr>
6759          <list>gambling</list>
6760          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  gambling/banned_portuguese</file>
6761        </config>
6762        <config>
6763          <descr><![CDATA[googlesearches banned]]></descr>
6764          <list>googlesearches</list>
6765          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  googlesearches/banned</file>
6766        </config>
```

```
6767        <config>
6768          <descr><![CDATA[illegaldrugs banned]]></descr>
6769          <list>illegaldrugs</list>
6770          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 illegaldrugs/banned</file>
6771        </config>
6772        <config>
6773          <descr><![CDATA[intolerance banned_portuguese]]></descr>
6774          <list>intolerance</list>
6775          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 intolerance/banned_portuguese</file>
6776        </config>
6777        <config>
6778          <descr><![CDATA[pornography banned]]></descr>
6779          <list>pornography</list>
6780          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/banned</file>
6781        </config>
6782        <config>
6783          <descr><![CDATA[pornography banned_portuguese]]></descr>
6784          <list>pornography</list>
6785          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/banned_portuguese</file>
6786        </config>
6787        <config>
6788          <descr><![CDATA[rta banned]]></descr>
6789          <list>rta</list>
6790          <file>/usr/local/etc/dansguardian/lists/phraselists/rta/↩
                 banned</file>
6791        </config>
6792        <config>
6793          <descr><![CDATA[safelabel banned]]></descr>
6794          <list>safelabel</list>
6795          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 safelabel/banned</file>
6796        </config>
6797      </dansguardianphraselistsbanned>
6798      <dansguardianphraselistsexception>
6799        <config>
6800          <descr><![CDATA[goodphrases exception]]></descr>
6801          <list>goodphrases</list>
6802          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 goodphrases/exception</file>
6803        </config>
6804        <config>
6805          <descr><![CDATA[goodphrases exception_email]]></descr>
6806          <list>goodphrases</list>
```

```
6807          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 goodphrases/exception_email</file>
6808        </config>
6809      </dansguardianphraselistsexception>
6810      <dansguardianblacklistsdomains>
6811        <config>
6812          <descr><![CDATA[ads domains]]></descr>
6813          <list>ads</list>
6814          <file>/usr/local/etc/dansguardian/lists/blacklists/ads/↩
                 domains</file>
6815        </config>
6816      </dansguardianblacklistsdomains>
6817      <dansguardianblacklistsurls>
6818        <config>
6819          <descr><![CDATA[ads urls]]></descr>
6820          <list>ads</list>
6821          <file>/usr/local/etc/dansguardian/lists/blacklists/ads/urls↩
                 </file>
6822        </config>
6823      </dansguardianblacklistsurls>
6824    </installedpackages>
6825    <dhcrelay/>
6826
6827      <allowedip>
6828        <ip>132.248.x.y</ip>
6829        <sn>32</sn>
6830        <dir>both</dir>
6831        <descr><![CDATA[ibiologia]]></descr>
6832        <bw_up>1000</bw_up>
6833        <bw_down>1000</bw_down>
6834      </allowedip>
6835      <allowedip>
6836        <ip>132.248.x.y</ip>
6837        <sn>32</sn>
6838        <dir>both</dir>
6839        <descr><![CDATA[apoyo.ibiologia]]></descr>
6840        <bw_up>1000</bw_up>
6841        <bw_down>1000</bw_down>
6842      </allowedip>
6843      <allowedip>
6844        <ip>132.248.x.y</ip>
6845        <sn>32</sn>
6846        <dir>both</dir>
6847        <descr><![CDATA[web]]></descr>
6848        <bw_up>1000</bw_up>
6849        <bw_down>1000</bw_down>
6850      </allowedip>
```

```
6851        <interface>opt1</interface>
6852        <timeout/>
6853        <idletimeout/>
6854        <freelogins_count/>
6855        <freelogins_resettimeout/>
6856        <auth_method>none</auth_method>
6857        <reauthenticateacct/>
6858        <httpsname/>
6859        <preauthurl/>
6860        <bwdefaultdn/>
6861        <bwdefaultup/>
6862        <certificate/>
6863        <cacertificate/>
6864        <private-key/>
6865        <redirurl/>
6866        <radiusip/>
6867        <radiusip2/>
6868        <radiusport/>
6869        <radiusport2/>
6870        <radiusacctport/>
6871        <radiuskey/>
6872        <radiuskey2/>
6873        <radiusvendor>default</radiusvendor>
6874        <radiussrcip_attribute>wan</radiussrcip_attribute>
6875        <radmac_format>default</radmac_format>
6876        <page>
6877          <htmltext>PEhUTUw+↩
                CjxIRUFEPgoKPFRJVExFPnJlZGlyZWN0PC9USVRMRT4KPE1FVEEgSFRUUC1FUVVJV↩

6878          0↩
                icmVmcmVzaCIgCkNPTlRFTlQ9IjA7VVJMPWh0dHA6Ly9hcG95by5pYmlvbG9naWEudW5hbS5te

6879          pL3VwbG9hZC9pbmRleC5waHAiPgo8L0hFQUQ+CjxCT0RZPgpSZWRpcmV
6880          jY2lvbmFuZG8uLgo8L2E+LiAKPC9CT0RZPgo8L0hUTUw+Cg==</htmltext>
6881        </page>
6882        <enable/>
6883      </captiveportal>
6884      <ezshaper>
6885        <step1>
6886          <numberofconnections>5</numberofconnections>
6887        </step1>
6888      </ezshaper>
6889    </pfsense>
6890          <interface>wan</interface>
6891          <tag/>
6892          <tagged/>
6893          <max/>
```

```
6894        <max-src-nodes/>
6895        <max-src-conn/>
6896        <max-src-states/>
6897        <statetimeout/>
6898        <statetype>keep state</statetype>
6899        <os/>
6900        <protocol>tcp/udp</protocol>
6901        <source>
6902          <any/>
6903        </source>
6904        <destination>
6905          <address>132.288.x.y</address>
6906          <port>8000</port>
6907        </destination>
6908        <descr><![CDATA[C PP]]></descr>
6909      </rule>
6910      <rule>
6911        <id/>
6912        <type>pass</type>
6913        <interface>wan</interface>
6914        <tag/>
6915        <tagged/>
6916        <max/>
6917        <max-src-nodes/>
6918        <max-src-conn/>
6919        <max-src-states/>
6920        <statetimeout/>
6921        <statetype>keep state</statetype>
6922        <os/>
6923        <protocol>tcp/udp</protocol>
6924        <source>
6925          <any/>
6926        </source>
6927        <destination>
6928          <address>132.288.x.y</address>
6929          <port>5000</port>
6930        </destination>
6931        <descr><![CDATA[D PP]]></descr>
6932      </rule>
6933      <rule>
6934        <id/>
6935        <type>pass</type>
6936        <interface>wan</interface>
6937        <tag/>
6938        <tagged/>
6939        <max/>
6940        <max-src-nodes/>
```

```
6941        <max-src-conn/>
6942        <max-src-states/>
6943        <statetimeout/>
6944        <statetype>keep state</statetype>
6945        <os/>
6946        <protocol>tcp/udp</protocol>
6947        <source>
6948          <any/>
6949        </source>
6950        <destination>
6951          <address>132.248.x.y</address>
6952          <port>88080</port>
6953        </destination>
6954        <descr><![CDATA[Estudiantes]]></descr>
6955      </rule>
6956      <rule>
6957        <id/>
6958        <type>pass</type>
6959        <interface>wan</interface>
6960        <tag/>
6961        <tagged/>
6962        <max/>
6963        <max-src-nodes/>
6964        <max-src-conn/>
6965        <max-src-states/>
6966        <statetimeout/>
6967        <statetype>keep state</statetype>
6968        <os/>
6969        <protocol>tcp/udp</protocol>
6970        <source>
6971          <any/>
6972        </source>
6973        <destination>
6974          <address>132.248.x.y</address>
6975          <port>88888</port>
6976        </destination>
6977        <descr><![CDATA[Glass Fish]]></descr>
6978      </rule>
6979      <rule>
6980        <id/>
6981        <type>pass</type>
6982        <interface>wan</interface>
6983        <tag/>
6984        <tagged/>
6985        <max/>
6986        <max-src-nodes/>
6987        <max-src-conn/>
```

```
6988        <max-src-states/>
6989        <statetimeout/>
6990        <statetype>keep state</statetype>
6991        <os/>
6992        <protocol>tcp/udp</protocol>
6993        <source>
6994          <any/>
6995        </source>
6996        <destination>
6997          <address>132.248.x.y</address>
6998          <port>58080</port>
6999        </destination>
7000        <descr><![CDATA[Consulta estudiantes]]></descr>
7001      </rule>
7002      <rule>
7003        <id/>
7004        <type>pass</type>
7005        <interface>wan</interface>
7006        <tag/>
7007        <tagged/>
7008        <max/>
7009        <max-src-nodes/>
7010        <max-src-conn/>
7011        <max-src-states/>
7012        <statetimeout/>
7013        <statetype>keep state</statetype>
7014        <os/>
7015        <protocol>tcp/udp</protocol>
7016        <source>
7017          <any/>
7018        </source>
7019        <destination>
7020          <address>132.248.x.y</address>
7021          <port>58888</port>
7022        </destination>
7023        <descr><![CDATA[Glass Fish 2]]></descr>
7024      </rule>
7025      <rule>
7026        <id/>
7027        <type>pass</type>
7028        <interface>wan</interface>
7029        <tag/>
7030        <tagged/>
7031        <max/>
7032        <max-src-nodes/>
7033        <max-src-conn/>
7034        <max-src-states/>
```

```
7035        <statetimeout/>
7036        <statetype>keep state</statetype>
7037        <os/>
7038        <protocol>tcp/udp</protocol>
7039        <source>
7040          <any/>
7041        </source>
7042        <destination>
7043          <address>132.248.x.y</address>
7044          <port>5832</port>
7045        </destination>
7046        <descr><![CDATA[Registro bd]]></descr>
7047      </rule>
7048      <rule>
7049        <id/>
7050        <type>pass</type>
7051        <interface>wan</interface>
7052        <tag/>
7053        <tagged/>
7054        <max/>
7055        <max-src-nodes/>
7056        <max-src-conn/>
7057        <max-src-states/>
7058        <statetimeout/>
7059        <statetype>keep state</statetype>
7060        <os/>
7061        <protocol>tcp/udp</protocol>
7062        <source>
7063          <any/>
7064        </source>
7065        <destination>
7066          <address>132.248.x.y</address>
7067          <port>80</port>
7068        </destination>
7069        <descr><![CDATA[Hongos]]></descr>
7070      </rule>
7071      <rule>
7072        <id/>
7073        <type>pass</type>
7074        <interface>wan</interface>
7075        <tag/>
7076        <tagged/>
7077        <max/>
7078        <max-src-nodes/>
7079        <max-src-conn/>
7080        <max-src-states/>
7081        <statetimeout/>
```

```
7082        <statetype>keep state</statetype>
7083        <os/>
7084        <protocol>tcp/udp</protocol>
7085        <source>
7086          <any/>
7087        </source>
7088        <destination>
7089          <address>132.248.x.y</address>
7090          <port>22</port>
7091        </destination>
7092        <descr><![CDATA[Peterson ssh]]></descr>
7093      </rule>
7094      <rule>
7095        <id/>
7096        <type>pass</type>
7097        <interface>wan</interface>
7098        <tag/>
7099        <tagged/>
7100        <max/>
7101        <max-src-nodes/>
7102        <max-src-conn/>
7103        <max-src-states/>
7104        <statetimeout/>
7105        <statetype>keep state</statetype>
7106        <os/>
7107        <protocol>tcp/udp</protocol>
7108        <source>
7109          <any/>
7110        </source>
7111        <destination>
7112          <address>132.288.x.y</address>
7113          <port>80</port>
7114        </destination>
7115        <descr><![CDATA[Peterson Web]]></descr>
7116      </rule>
7117      <rule>
7118        <id/>
7119        <tag/>
7120        <tagged/>
7121        <max/>
7122        <max-src-nodes/>
7123        <max-src-conn/>
7124        <max-src-states/>
7125        <statetimeout/>
7126        <statetype>keep state</statetype>
7127        <os/>
7128        <type>reject</type>
```

```
7129        <descr><![CDATA[pfBlockerEurope auto rule]]></descr>
7130        <source>
7131          <any/>
7132        </source>
7133        <destination>
7134          <address>pfBlockerEurope</address>
7135        </destination>
7136        <log/>
7137        <interface>lan</interface>
7138      </rule>
7139      <rule>
7140        <id/>
7141        <tag/>
7142        <tagged/>
7143        <max/>
7144        <max-src-nodes/>
7145        <max-src-conn/>
7146        <max-src-states/>
7147        <statetimeout/>
7148        <statetype>keep state</statetype>
7149        <os/>
7150        <type>reject</type>
7151        <descr><![CDATA[pfBlockerTopSpammers auto rule]]></descr>
7152        <source>
7153          <any/>
7154        </source>
7155        <destination>
7156          <address>pfBlockerTopSpammers</address>
7157        </destination>
7158        <log/>
7159        <interface>lan</interface>
7160      </rule>
7161      <rule>
7162        <id/>
7163        <tag/>
7164        <tagged/>
7165        <max/>
7166        <max-src-nodes/>
7167        <max-src-conn/>
7168        <max-src-states/>
7169        <statetimeout/>
7170        <statetype>keep state</statetype>
7171        <os/>
7172        <type>reject</type>
7173        <descr><![CDATA[pfBlockerzeroaccess auto rule]]></descr>
7174        <source>
7175          <any/>
```

```
7176        </source>
7177        <destination>
7178          <address>pfBlockerzeroaccess</address>
7179        </destination>
7180        <log/>
7181        <interface>lan</interface>
7182      </rule>
7183      <rule>
7184        <id/>
7185        <type>pass</type>
7186        <interface>lan</interface>
7187        <tag/>
7188        <tagged/>
7189        <max/>
7190        <max-src-nodes/>
7191        <max-src-conn/>
7192        <max-src-states/>
7193        <statetimeout/>
7194        <statetype>keep state</statetype>
7195        <os/>
7196        <source>
7197          <any/>
7198        </source>
7199        <destination>
7200          <any/>
7201        </destination>
7202        <log/>
7203        <descr><![CDATA[Open LAN]]></descr>
7204      </rule>
7205      <rule>
7206        <id/>
7207        <type>pass</type>
7208        <interface>enc0</interface>
7209        <tag/>
7210        <tagged/>
7211        <max/>
7212        <max-src-nodes/>
7213        <max-src-conn/>
7214        <max-src-states/>
7215        <statetimeout/>
7216        <statetype>keep state</statetype>
7217        <os/>
7218        <source>
7219          <any/>
7220        </source>
7221        <destination>
7222          <any/>
```

```
7223        </destination>
7224        <descr/>
7225      </rule>
7226      <rule>
7227        <descr><![CDATA[OpenVPN  wizard]]></descr>
7228        <source>
7229          <any/>
7230        </source>
7231        <destination>
7232          <any/>
7233        </destination>
7234        <interface>openvpn</interface>
7235        <type>pass</type>
7236        <enabled>on</enabled>
7237      </rule>
7238      <rule>
7239        <descr><![CDATA[OpenVPN  wizard]]></descr>
7240        <source>
7241          <any/>
7242        </source>
7243        <destination>
7244          <any/>
7245        </destination>
7246        <interface>openvpn</interface>
7247        <type>pass</type>
7248        <enabled>on</enabled>
7249      </rule>
7250    </filter>
7251    <shaper/>
7252    <ipsec>
7253      <preferoldsa/>
7254      <phase1>
7255        <ikeid>1</ikeid>
7256        <interface>wan</interface>
7257        <remote-gateway>132.288.126.8</remote-gateway>
7258        <mode>aggressive</mode>
7259        <myid_type>myaddress</myid_type>
7260        <myid_data/>
7261        <peerid_type>peeraddress</peerid_type>
7262        <peerid_data/>
7263        <encryption-algorithm>
7264          <name>3des</name>
7265        </encryption-algorithm>
7266        <hash-algorithm>sha1</hash-algorithm>
7267        <dhgroup>2</dhgroup>
7268        <lifetime>3600</lifetime>
7269        <pre-shared-key>ibunam</pre-shared-key>
```

```
7270        <private-key/>
7271        <certref/>
7272        <caref/>
7273        <authentication_method>pre_shared_key</authentication_method>
7274        <generate_policy/>
7275        <proposal_check/>
7276        <descr><![CDATA[Tunel Hacia Unibio]]></descr>
7277        <nat_traversal>on</nat_traversal>
7278        <dpd_delay>10</dpd_delay>
7279        <dpd_maxfail>5</dpd_maxfail>
7280      </phase1>
7281      <client/>
7282      <phase2>
7283        <ikeid>1</ikeid>
7284        <mode>tunnel</mode>
7285        <localid>
7286          <type>network</type>
7287          <address>10.0.0.0</address>
7288          <netbits>8</netbits>
7289        </localid>
7290        <remoteid>
7291          <type>network</type>
7292          <address>10.1.6.0</address>
7293          <netbits>28</netbits>
7294        </remoteid>
7295        <protocol>esp</protocol>
7296        <encryption-algorithm-option>
7297          <name>3des</name>
7298        </encryption-algorithm-option>
7299        <hash-algorithm-option>hmac_sha1</hash-algorithm-option>
7300        <pfsgroup>2</pfsgroup>
7301        <lifetime>3600</lifetime>
7302        <pinghost/>
7303        <descr><![CDATA[RED Unibio]]></descr>
7304      </phase2>
7305    </ipsec>
7306    <aliases>
7307      <alias>
7308        <name>pfBlockerEurope</name>
7309        <url>http://127.0.0.1:80/pfblocker.php?pfb=pfBlockerEurope</↩
              url>
7310        <updatefreq>32</updatefreq>
7311        <address/>
7312        <descr><![CDATA[pfBlocker country list]]></descr>
7313        <type>urltable</type>
7314        <detail><![CDATA[DO NOT EDIT THIS ALIAS]]></detail>
7315      </alias>
```

```
7316      <alias>
7317        <name>pfBlockerTopSpammers</name>
7318        <url>http://127.0.0.1:80/pfblocker.php?pfb=↩
              pfBlockerTopSpammers</url>
7319        <updatefreq>32</updatefreq>
7320        <address/>
7321        <descr><![CDATA[pfBlocker country list]]></descr>
7322        <type>urltable</type>
7323        <detail><![CDATA[DO NOT EDIT THIS ALIAS]]></detail>
7324      </alias>
7325      <alias>
7326        <name>pfBlockerzeroaccess</name>
7327        <url>http://127.0.0.1:80/pfblocker.php?pfb=↩
              pfBlockerzeroaccess</url>
7328        <updatefreq>32</updatefreq>
7329        <address/>
7330        <descr><![CDATA[pfBlocker user list]]></descr>
7331        <type>urltable</type>
7332        <detail><![CDATA[DO NOT EDIT THIS ALIAS]]></detail>
7333      </alias>
7334      <alias>
7335        <name>Cams</name>
7336        <address>1000 2000 3000 8000 5000</address>
7337        <descr><![CDATA[DVRs]]></descr>
7338        <type>port</type>
7339        <detail><![CDATA[Entry added Tue, 16 Jul 2013 18:35:08 ↩
              -0500||Entry added Tue, 16 Jul 2013 18:35:08 -0500||Entry ↩
              added Tue, 16 Jul 2013 18:35:27 -0500||Entry added Tue, 16↩
               Jul 2013 18:35:27 -0500||Entry added Tue, 16 Jul 2013 18↩
              :35:27 -0500]]></detail>
7340      </alias>
7341      <alias>
7342        <name>Peterson</name>
7343        <address>80 22</address>
7344        <descr><![CDATA[Ports Peterson]]></descr>
7345        <type>port</type>
7346        <detail><![CDATA[Entry added Mon, 29 Jul 2013 13:53:09 ↩
              -0500||Entry added Mon, 29 Jul 2013 13:53:09 -0500]]></↩
              detail>
7347      </alias>
7348    </aliases>
7349    <proxyarp/>
7350    <cron>
7351      <item>
7352        <minute>0</minute>
7353        <hour>*</hour>
7354        <mday>*</mday>
```

```
7355        <month>*</month>
7356        <wday>*</wday>
7357        <who>root</who>
7358        <command>/usr/bin/nice -n20 newsyslog</command>
7359      </item>
7360      <item>
7361        <minute>1,31</minute>
7362        <hour>0-5</hour>
7363        <mday>*</mday>
7364        <month>*</month>
7365        <wday>*</wday>
7366        <who>root</who>
7367        <command>/usr/bin/nice -n20 adjkerntz -a</command>
7368      </item>
7369      <item>
7370        <minute>1</minute>
7371        <hour>3</hour>
7372        <mday>1</mday>
7373        <month>*</month>
7374        <wday>*</wday>
7375        <who>root</who>
7376        <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command↩
               >
7377      </item>
7378      <item>
7379        <minute>*/60</minute>
7380        <hour>*</hour>
7381        <mday>*</mday>
7382        <month>*</month>
7383        <wday>*</wday>
7384        <who>root</who>
7385        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t↩
               3600 sshlockout</command>
7386      </item>
7387      <item>
7388        <minute>1</minute>
7389        <hour>1</hour>
7390        <mday>*</mday>
7391        <month>*</month>
7392        <wday>*</wday>
7393        <who>root</who>
7394        <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
7395      </item>
7396      <item>
7397        <minute>*/60</minute>
7398        <hour>*</hour>
7399        <mday>*</mday>
```

```
7400        <month>*</month>
7401        <wday>*</wday>
7402        <who>root</who>
7403        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t↩
                3600 virusprot</command>
7404      </item>
7405      <item>
7406        <minute>30</minute>
7407        <hour>12</hour>
7408        <mday>*</mday>
7409        <month>*</month>
7410        <wday>*</wday>
7411        <who>root</who>
7412        <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command↩
              >
7413      </item>
7414      <item>
7415        <minute>0</minute>
7416        <hour>*</hour>
7417        <mday>*</mday>
7418        <month>*</month>
7419        <wday>*</wday>
7420        <who>root</who>
7421        <command>/usr/local/bin/php -q /usr/local/www/pfblocker.php ↩
              cron</command>
7422      </item>
7423    </cron>
7424    <wol/>
7425    <rrd>
7426      <enable/>
7427    </rrd>
7428    <load_balancer>
7429      <monitor_type>
7430        <name>ICMP</name>
7431        <type>icmp</type>
7432        <descr><![CDATA[ICMP]]></descr>
7433        <options/>
7434      </monitor_type>
7435      <monitor_type>
7436        <name>TCP</name>
7437        <type>tcp</type>
7438        <descr><![CDATA[Generic TCP]]></descr>
7439        <options/>
7440      </monitor_type>
7441      <monitor_type>
7442        <name>HTTP</name>
7443        <type>http</type>
```

```
7444        <descr><![CDATA[Generic HTTP]]></descr>
7445        <options>
7446          <path>/</path>
7447          <host/>
7448          <code>200</code>
7449        </options>
7450      </monitor_type>
7451      <monitor_type>
7452        <name>HTTPS</name>
7453        <type>https</type>
7454        <descr><![CDATA[Generic HTTPS]]></descr>
7455        <options>
7456          <path>/</path>
7457          <host/>
7458          <code>200</code>
7459        </options>
7460      </monitor_type>
7461      <monitor_type>
7462        <name>SMTP</name>
7463        <type>send</type>
7464        <descr><![CDATA[Generic SMTP]]></descr>
7465        <options>
7466          <send>EHLO nosuchhost</send>
7467          <expect>250-</expect>
7468        </options>
7469      </monitor_type>
7470    </load_balancer>
7471    <widgets>
7472      <sequence>traffic_graphs-container:col1:show,system_information↩
           -container:col1:show,captive_portal_status-↩
           container:col1:close,carp_status-container:col1:close,↩
           cpu_graphs-container:col1:close,gmirror_status-↩
           container:col1:close,installed_packages-container:col1:close↩
           ,interface_statistics-container:col1:close,picture-↩
           container:col2:show,gateways-container:col2:show,interfaces-↩
           container:col2:show,ipsec-container:col2:close,↩
           load_balancer_status-container:col2:close,log-↩
           container:col2:close,rss-container:col2:close,↩
           services_status-container:col2:close,openvpn-↩
           container:col2:none,wake_on_lan-container:col2:none</↩
           sequence>
7473
7474      <picturewidget_filename>ibunamlogo.JPG</picturewidget_filename>
7475    </widgets>
7476    <revision>
7477      <time>1380816730</time>
```

```
7478      <description><![CDATA[admin@10.1.8.233: /firewall_rules_edit.↩
              php made unknown change]]></description>
7479      <username>admin@10.1.8.233</username>
7480    </revision>
7481    <openvpn>
7482      <openvpn-server>
7483        <vpnid>1</vpnid>
7484        <mode>server_tls_user</mode>
7485        <authmode>Local Database</authmode>
7486        <protocol>UDP</protocol>
7487        <dev_mode>tun</dev_mode>
7488        <ipaddr/>
7489        <interface>wan</interface>
7490        <local_port>1198</local_port>
7491        <description/>
7492        <custom_options/>
7493        <tls>↩
              Iw0KIyAyMDQ8IGJpdCBPcGVuVlBOIHN0YXRpYyBrZXkNCiMNCi0tLS0tQkVHSU8gT3BlblZQTi

7494        ga2V5IFYxLS0tLS0NCmFmNDMwZmI1MGM8MzVlYTZmOTMxNTcyMTFkZjA1Njg2DQoxZjQ2NjM2Y2U2

7495        kyZjI5NzM1Mw0KMjQ8MjBlZGE2Nzk8NWEwMGNhYTdkZDFlMWUxYzBmNWQNCjZiN2FmMjcwMzUzYzk

7496        YWQ1MmViMDc3DQo1ZTBkNzdjNDk8YTI8NThlYzIyYzZhMTk3YzA5MDlmYQ0KOGM1YTkxNDI8YTcyY

7497        WE2OTZlYmYNCjgwMWIzMTJmYzhkZjJjNTlmOGFmNWM5ODY3OWIwOWIwDQozMzI5ZjU0MTk2ZTM2ZD

7498        GYxYTI8Ng0KZGI8OWU3NmRiOGVjMjZmYWU8OTIxMTA8NjA8YTgwMzANCjdmMzg2N2FiNTJkYzcwNj

7499        NDkyYmY3YzhlDQoyMDk5OWQ5MGNiODViMmJlYWFjNzM5ZTg0ZTZlYTZlMQ0KODlkMWQ8YmY0N2EyN

7500        zcxNWZiMzM1ZWINCjY1MzE0Mjc1OWNlZGJlNWRjYzEyMjI0NDhiZWYxOTFkDQo8MjZkZWE5ZjRhMj

7501        E0ODUzMjg0NGQzMA0KYTNmY2Q2ZjYzMzdhMjBkODNmMGVhNGJmNmQwYWY0MzkNCjFlNTQ2MjBhNTA

7502        lMjAwOTczM2UwOWYwDQotLS0tLUVORCBPcGVuVlBOIFN0YXRpYyBrZXkgVjEtLS0tLQ0K↩
              </tls>
7503        <caref>50a18d2802392</caref>
7504        <crlref/>
7505        <certref>50a18e500a587</certref>
7506        <dh_length>1028</dh_length>
7507        <strictusercn/>
7508        <crypto>AES-128-CBC</crypto>
7509        <engine>none</engine>
7510        <tunnel_network>192.168.10.0/28</tunnel_network>
7511        <remote_network/>
7512        <gwredir>yes</gwredir>
```

```
7513        <local_network>10.1.0.0/16</local_network>
7514        <maxclients/>
7515        <compression>yes</compression>
7516        <passtos/>
7517        <client2client/>
7518        <dynamic_ip>yes</dynamic_ip>
7519        <pool_enable>yes</pool_enable>
7520        <dns_server1>132.288.237.250</dns_server1>
7521        <dns_server2/>
7522        <dns_server3/>
7523        <dns_server8/>
7524        <netbios_enable/>
7525        <netbios_ntype>0</netbios_ntype>
7526        <netbios_scope/>
7527      </openvpn-server>
7528    </openvpn>
7529    <l7shaper>
7530      <container/>
7531    </l7shaper>
7532    <dnshaper/>
7533
7534    <ppps/>
7535    <gateways>
7536      <gateway_item>
7537        <interface>wan</interface>
7538        <gateway>132.248.x.y</gateway>
7539        <name>GW13</name>
7540        <weight>1</weight>
7541        <interval/>
7542        <descr><![CDATA[gateway 1]]></descr>
7543        <defaultgw/>
7544      </gateway_item>
7545      <gateway_item>
7546        <interface>wan</interface>
7547        <gateway>132.288.y.z</gateway>
7548        <name>GW126</name>
7549        <weight/>
7550        <interval/>
7551        <descr><![CDATA[gateway 2]]></descr>
7552      </gateway_item>
7553      <gateway_item>
7554        <interface>lan</interface>
7555        <gateway>10.1.16.253</gateway>
7556        <name>LANGW</name>
7557        <weight/>
7558        <interval/>
7559        <descr><![CDATA[lan gateway]]></descr>
```

```
7560      </gateway_item>
7561      <gateway_item>
7562        <interface>lan</interface>
7563        <gateway>10.1.16.2</gateway>
7564        <name>gwlan</name>
7565        <weight>1</weight>
7566        <interval/>
7567        <descr><![CDATA[hacia fw2]]></descr>
7568      </gateway_item>
7569      <gateway_group>
7570        <name>multiple</name>
7571        <item>GW1|1</item>
7572        <item>GW2|2</item>
7573        <trigger>down</trigger>
7574        <descr><![CDATA[multiples gateways]]></descr>
7575      </gateway_group>
7576    </gateways>
7577    <captiveportal/>
7578    <virtualip>
7579      <vip>
7580        <mode>carp</mode>
7581        <interface>wan</interface>
7582        <vhid>2</vhid>
7583        <advskew>0</advskew>
7584        <advbase>1</advbase>
7585        <password>12385</password>
7586        <descr><![CDATA[vmware]]></descr>
7587        <type>single</type>
7588        <subnet_bits>32</subnet_bits>
7589        <subnet>132.248.x.y</subnet>
7590      </vip>
7591      <vip>
7592        <mode>proxyarp</mode>
7593        <interface>wan</interface>
7594        <descr/>
7595        <type>single</type>
7596        <subnet_bits>32</subnet_bits>
7597        <subnet>132.248.x.y</subnet>
7598      </vip>
7599      <vip>
7600        <mode>carp</mode>
7601        <interface>wan</interface>
7602        <vhid>3</vhid>
7603        <advskew>0</advskew>
7604        <advbase>1</advbase>
7605        <password>12385</password>
7606        <descr><![CDATA[Hacia Informe y registro]]></descr>
```

```
7607        <type>single</type>
7608        <subnet_bits>32</subnet_bits>
7609        <subnet>132.248.x.y</subnet>
7610      </vip>
7611      <vip>
7612        <mode>carp</mode>
7613        <interface>wan</interface>
7614        <vhid>5</vhid>
7615        <advskew>0</advskew>
7616        <advbase>1</advbase>
7617        <password>12385</password>
7618        <descr><![CDATA[Rupa]]></descr>
7619        <type>single</type>
7620        <subnet_bits>32</subnet_bits>
7621        <subnet>132.248.x.y</subnet>
7622      </vip>
7623      <vip>
7624        <mode>carp</mode>
7625        <interface>wan</interface>
7626        <vhid>8</vhid>
7627        <advskew>0</advskew>
7628        <advbase>1</advbase>
7629        <password>123856</password>
7630        <descr><![CDATA[Page Congreso de Cactaceas]]></descr>
7631        <type>single</type>
7632        <subnet_bits>32</subnet_bits>
7633        <subnet>132.248.x.y</subnet>
7634      </vip>
7635      <vip>
7636        <mode>carp</mode>
7637        <interface>wan</interface>
7638        <vhid>9</vhid>
7639        <advskew>0</advskew>
7640        <advbase>1</advbase>
7641        <password>12385</password>
7642        <descr><![CDATA[Pruebas LAB]]></descr>
7643        <type>single</type>
7644        <subnet_bits>32</subnet_bits>
7645        <subnet>132.248.x.y</subnet>
7646      </vip>
7647      <vip>
7648        <mode>carp</mode>
7649        <interface>wan</interface>
7650        <vhid>10</vhid>
7651        <advskew>0</advskew>
7652        <advbase>1</advbase>
7653        <password>12385</password>
```

```
7654        <descr><![CDATA[Hongos]]></descr>
7655        <type>single</type>
7656        <subnet_bits>32</subnet_bits>
7657        <subnet>132.248.x.y</subnet>
7658      </vip>
7659      <vip>
7660        <mode>carp</mode>
7661        <interface>wan</interface>
7662        <vhid>11</vhid>
7663        <advskew>0</advskew>
7664        <advbase>1</advbase>
7665        <password>12385</password>
7666        <descr><![CDATA[Peterson]]></descr>
7667        <type>single</type>
7668        <subnet_bits>32</subnet_bits>
7669        <subnet>132.248.x.y</subnet>
7670      </vip>
7671      <vip>
7672        <mode>carp</mode>
7673        <interface>wan</interface>
7674        <vhid>12</vhid>
7675        <advskew>0</advskew>
7676        <advbase>1</advbase>
7677        <password>12385</password>
7678        <descr><![CDATA[Quanxi]]></descr>
7679        <type>single</type>
7680        <subnet_bits>32</subnet_bits>
7681        <subnet>132.248.x.y</subnet>
7682      </vip>
7683      <vip>
7684        <mode>carp</mode>
7685        <interface>wan</interface>
7686        <vhid>13</vhid>
7687        <advskew>0</advskew>
7688        <advbase>1</advbase>
7689        <password>12385</password>
7690        <descr><![CDATA[FTP NAS]]></descr>
7691        <type>single</type>
7692        <subnet_bits>32</subnet_bits>
7693        <subnet>132.248.x.y</subnet>
7694      </vip>
7695      <vip>
7696        <mode>carp</mode>
7697        <interface>wan</interface>
7698        <vhid>18</vhid>
7699        <advskew>0</advskew>
7700        <advbase>1</advbase>
```

```
7701        <password>12385</password>
7702        <descr><![CDATA[Prueba Hathor]]></descr>
7703        <type>single</type>
7704        <subnet_bits>32</subnet_bits>
7705        <subnet>132.248.x.y</subnet>
7706      </vip>
7707    </virtualip>
7708
7709    <installedpackages>
7710      <package>
7711        <name>phpSysInfo</name>
7712        <website>http://phpsysinfo.sourceforge.net/</website>
7713        <descr><![CDATA[PHPSysInfo is a customizable PHP Script that ↩
               parses /proc, and formats information nicely. It will ↩
               display information about system facts like Uptime, CPU, ↩
               Memory, PCI devices, SCSI devices, IDE devices, Network ↩
               adapters, Disk usage, and more.]]></descr>
7714        <category>System</category>
7715        <version>2.5.8</version>
7716        <status>Beta</status>
7717        <required_version>1.0</required_version>
7718        <depends_on_package_base_url>http://files.pfsense.org/↩
               packages/amd68/8/All/</depends_on_package_base_url>
7719        <depends_on_package>mbmon-205_5.tbz</depends_on_package>
7720        <depends_on_package_pbi>mbmon-205_6-amd68.pbi</↩
               depends_on_package_pbi>
7721        <build_port_path>/usr/ports/sysutils/mbmon</build_port_path>
7722        <config_file>http://www.pfsense.com/packages/config/↩
               phpsysinfo/phpsysinfo.xml</config_file>
7723        <configurationfile>phpsysinfo.xml</configurationfile>
7724        <noembedded>true</noembedded>
7725      </package>
7726      <package>
7727        <name>pfBlocker</name>
7728        <website/>
7729        <descr><![CDATA[Introduce Enhanced Aliastable Feature to ↩
               pfsense.&lt;br /&gt;
7730        Assign many IP urls lists from sites like I-blocklist to a ↩
               single alias and then choose rule action to take.&lt;br /&↩
               gt;
7731        This package also Block countries and IP ranges.&lt;br /&gt;
7732        pfBlocker replaces Countryblock and IPblocklist]]></descr>
7733        <category>Firewall</category>
7734        <pkginfolink>http://forum.pfsense.org/index.php/topic↩
               ,82583.0.html</pkginfolink>
7735        <config_file>http://pfsense.org/packages/config/pf-blocker/↩
               pfblocker.xml</config_file>
```

```
7736        <depends_on_package_base_url>http://files.pfsense.org/↩
               packages/amd68/8/All/</depends_on_package_base_url>
7737        <version>1.0.2</version>
7738        <status>Release</status>
7739        <required_version>2.0</required_version>
7740        <maintainer>tom@tomschaefer.org marcellocoutinho@gmail.com</↩
               maintainer>
7741        <configurationfile>pfblocker.xml</configurationfile>
7742      </package>
7743      <package>
7744        <name>nmap</name>
7745        <maintainer>jimp@pfsense.org</maintainer>
7746        <descr><![CDATA[NMap is a utility for network exploration or ↩
               security auditing. It supports ping scanning (determine ↩
               which hosts are up), many port scanning techniques (↩
               determine what services the hosts are offering), version ↩
               detection (determine what application/service is runing on↩
                a port), and TCP/IP fingerprinting (remote host OS or ↩
               device identification). It also offers flexible target and↩
                port specification, decoy/stealth scanning, SunRPC ↩
               scanning, and more. Most Unix and Windows platforms are ↩
               supported in both GUI and command line modes. Several ↩
               popular handheld devices are also supported, including the↩
                Sharp Zaurus and the iPAQ.]]></descr>
7747        <category>Security</category>
7748        <depends_on_package_base_url>http://files.pfsense.org/↩
               packages/amd68/8/All/</depends_on_package_base_url>
7749        <depends_on_package>lua-5.1.5_8.tbz</depends_on_package>
7750        <depends_on_package>nmap-6.25_1.tbz</depends_on_package>
7751        <depends_on_package>libpcap-1.2.1.tbz</depends_on_package>
7752        <depends_on_package_pbi>nmap-6.25_1-amd68.pbi</↩
               depends_on_package_pbi>
7753        <config_file>http://www.pfsense.com/packages/config/nmap/nmap↩
               .xml</config_file>
7754        <version>nmap-6.25_1 pkg v1.2</version>
7755        <status>Stable</status>
7756        <pkginfolink>http://doc.pfsense.org/index.php/Nmap_package</↩
               pkginfolink>
7757        <required_version>2.0</required_version>
7758        <configurationfile>nmap.xml</configurationfile>
7759        <build_port_path>/usr/ports/security/nmap</build_port_path>
7760      </package>
7761      <package>
7762        <name>OpenVPN Client Export Utility</name>
7763        <descr><![CDATA[Allows a pre-configured OpenVPN Windows ↩
               Client or Mac OSXs Viscosity configuration bundle to be ↩
               exported directly from pfSense.]]></descr>
```

```
7764        <category>Security</category>
7765        <depends_on_package_base_url>http://files.pfsense.org/↩
                packages/amd68/8/All/</depends_on_package_base_url>
7766        <depends_on_package>p7zip-9.20.1.tbz</depends_on_package>
7767        <depends_on_package>zip-3.0.tbz</depends_on_package>
7768        <depends_on_package_pbi>p7zip-9.20.1-amd68.pbi zip-3.0-amd68.↩
                pbi</depends_on_package_pbi>
7769        <build_port_path>/usr/ports/archivers/p7zip</build_port_path>
7770        <build_port_path>/usr/ports/archivers/zip</build_port_path>
7771        <version>1.0.11</version>
7772        <status>RELEASE</status>
7773        <required_version>2.0</required_version>
7774        <config_file>http://www.pfsense.com/packages/config/openvpn-↩
                client-export/openvpn-client-export.xml</config_file>
7775        <configurationfile>openvpn-client-export.xml</↩
                configurationfile>
7776      </package>
7777      <package>
7778        <name>iperf</name>
7779        <website>http://dast.nlanr.net/Projects/Iperf/</website>
7780        <descr><![CDATA[Iperf is a tool for testing network ↩
                throughput, loss, and jitter.]]></descr>
7781        <category>Network Management</category>
7782        <config_file>http://www.pfsense.com/packages/config/iperf.xml↩
                </config_file>
7783        <depends_on_package_base_url>http://files.pfsense.org/↩
                packages/amd68/8/All/</depends_on_package_base_url>
7784        <depends_on_package>iperf-2.0.5.tbz</depends_on_package>
7785        <depends_on_package_pbi>iperf-2.0.5-amd68.pbi</↩
                depends_on_package_pbi>
7786        <version>2.0.5</version>
7787        <status>Beta</status>
7788        <pkginfolink>http://doc.pfsense.org/index.php/Iperf_package</↩
                pkginfolink>
7789        <required_version>1.2.1</required_version>
7790        <configurationfile>iperf.xml</configurationfile>
7791        <build_port_path>/usr/ports/benchmarks/iperf</build_port_path↩
                >
7792      </package>
7793      <package>
7794        <name>bandwidthd</name>
7795        <website>http://bandwidthd.sourceforge.net/</website>
7796        <descr><![CDATA[BandwidthD tracks usage of TCP/IP network ↩
                subnets and builds html files with graphs to display ↩
                utilization. Charts are built by individual IPs, and by ↩
                default display utilization over 2 day, 8 day, 80 day, and↩
                 800 day periods. Furthermore, each ip address utilization↩
```

```
        can be logged out at intervals of 3.3 minutes, 10 minutes, 1 hour or 12 hours in cdf format, or to a backend database server. HTTP, TCP, UDP, ICMP, VPN, and P2P traffic are color coded.]]></descr>
7797    <category>System</category>
7798    <version>2.0.1_5 pkg v.0.1</version>
7799    <status>BETA</status>
7800    <required_version>1.2.1</required_version>
7801    <depends_on_package_base_url>http://files.pfsense.org/packages/amd68/8/All/</depends_on_package_base_url>
7802    <depends_on_package>bandwidthd-2.0.1_5.tbz</depends_on_package>
7803    <depends_on_package>libpcap-1.1.1.tbz</depends_on_package>
7804    <depends_on_package>postgresql-client-8.8.12.tbz</depends_on_package>
7805    <depends_on_package_pbi>bandwidthd-2.0.1_5-amd68.pbi</depends_on_package_pbi>
7806    <config_file>http://www.pfsense.org/packages/config/bandwidthd/bandwidthd.xml</config_file>
7807    <configurationfile>bandwidthd.xml</configurationfile>
7808    <build_port_path>/usr/ports/net/libpcap</build_port_path>
7809    <build_port_path>/usr/ports/databases/postgresql88-client</build_port_path>
7810    <build_port_path>/usr/ports/net-mgmt/bandwidthd</build_port_path>
7811    <build_pbi>
7812      <ports_before>net/libpcap databases/postgresql91-client graphics/gd</ports_before>
7813      <port>net-mgmt/bandwidthd</port>
7814    </build_pbi>
7815    <build_options>WITH_NLS=true;WITHOUT_PAM=true;WITHOUT_LDAP=true;WITHOUT_MIT_KRB5=true;WITHOUT_HEIMDAL_KRB5=true;WITHOUT_OPTIMIZED_CFLAGS=true;WITHOUT_XML=true;WITHOUT_TZDATA=true;WITHOUT_DEBUG=true;WITHOUT_GSSAPI=true;WITHOUT_ICU=true;WITH_INTDATE=true</build_options>
7816  </package>
7817  <tab>
7818    <name>Client Export</name>
7819    <tabgroup>OpenVPN</tabgroup>
7820    <url>/vpn_openvpn_export.php</url>
7821  </tab>
7822  <tab>
7823    <name>Shared Key Export</name>
7824    <tabgroup>OpenVPN</tabgroup>
7825    <url>/vpn_openvpn_export_shared.php</url>
7826  </tab>
7827  <tab>
```

```
7828        <text>BandwidthD</text>
7829        <url>/pkg_edit.php?xml=bandwidthd.xml&amp;id=0</url>
7830        <active/>
7831      </tab>
7832      <menu>
7833        <name>phpsysinfo</name>
7834        <tooltiptext/>
7835        <section>Status</section>
7836        <url>/pkg_edit.php?xml=phpsysinfo.xml&amp;id=0</url>
7837      </menu>
7838      <menu>
7839        <name>pfBlocker</name>
7840        <tooltiptext>Configure pfblocker</tooltiptext>
7841        <section>Firewall</section>
7842        <url>/pkg_edit.php?xml=pfblocker.xml</url>
7843      </menu>
7844      <menu>
7845        <name>NMap</name>
7846        <tooltiptext>NMap is a utility for network exploration or ↩
              security auditing. It supports ping scanning (determine ↩
              which hosts are up), many port scanning techniques (↩
              determine what services the hosts are offering), version ↩
              detection (determine what application/service is runing on↩
               a port), and TCP/IP fingerprinting (remote host OS or ↩
              device identification). It also offers flexible target and↩
               port specification, decoy/stealth scanning, SunRPC ↩
              scanning, and more. Most Unix and Windows platforms are ↩
              supported in both GUI and command line modes. Several ↩
              popular handheld devices are also supported, including the↩
               Sharp Zaurus and the iPAQ.</tooltiptext>
7847        <section>Diagnostics</section>
7848        <configfile>nmap.xml</configfile>
7849      </menu>
7850      <menu>
7851        <name>iperf</name>
7852        <tooltiptext>Run iperf in client or server mode.</tooltiptext↩
              >
7853        <section>Diagnostics</section>
7854        <configfile>iperf.xml</configfile>
7855      </menu>
7856      <menu>
7857        <name>BandwidthD</name>
7858        <tooltiptext/>
7859        <section>Services</section>
7860        <url>/pkg_edit.php?xml=bandwidthd.xml&amp;id=0</url>
7861      </menu>
7862      <service>
```

```
7863        <name>iperf</name>
7864        <executable>iperf</executable>
7865      </service>
7866      <service>
7867        <name>bandwidthd</name>
7868        <rcfile>bandwidthd.sh</rcfile>
7869        <executable>bandwidthd</executable>
7870      </service>
7871      <bandwidthd>
7872        <config>
7873          <enable>on</enable>
7874          <active_interface>lan</active_interface>
7875          <subnets_custom>10.1.2.0/28;10.1.8.0/28</subnets_custom>
7876          <skipintervals/>
7877          <graphcutoff/>
7878          <promiscuous>on</promiscuous>
7879          <outputcdf/>
7880          <recovercdf>on</recovercdf>
7881          <filter/>
7882          <drawgraphs>on</drawgraphs>
7883          <meta_refresh/>
7884          <graph_log_info/>
7885        </config>
7886      </bandwidthd>
7887      <phpsysinfo>
7888        <config>
7889          <hidepicklist/>
7890          <sensorprogram>on</sensorprogram>
7891          <showmountpoint>on</showmountpoint>
7892          <showinodes>on</showinodes>
7893          <loadbar>on</loadbar>
7894          <showerrors/>
7895        </config>
7896      </phpsysinfo>
7897      <pfblockereurope>
7898        <config>
7899          <countries>RU</countries>
7900          <action>Deny_Both</action>
7901        </config>
7902      </pfblockereurope>
7903      <pfblocker>
7904        <config>
7905          <enable_cb>on</enable_cb>
7906          <enable_log>on</enable_log>
7907          <inbound_interface>wan</inbound_interface>
7908          <inbound_deny_action>block</inbound_deny_action>
7909          <outbound_interface>lan</outbound_interface>
```

```
7910          <outbound_deny_action>reject</outbound_deny_action>
7911          <credits/>
7912          <donation/>
7913        </config>
7914      </pfblocker>
7915      <pfblockertopspammers>
7916        <config>
7917          <countries>RU</countries>
7918          <action>Deny_Both</action>
7919        </config>
7920      </pfblockertopspammers>
7921      <pfblockerlists>
7922        <config>
7923          <aliasname>zero access</aliasname>
7924          <description><![CDATA[zero akses home]]></description>
7925          <row>
7926            <format>gz</format>
7927          </row>
7928          <action>Deny_Both</action>
7929          <cron>Never</cron>
7930          <custom>↩
                NjkuMTc2LjE0Ljc2LzMyDQo3Ni8yOC8xMTIuMjEvMzINCjI0LjEyNy8xNTcuMTE3LzMy↩

7931          DQoxMTcMjA1LjEzLjExMy8zMg0KMjAwLjU5LjcuMjE2LzMyDQoxMTMuMTkzL↩

7932          jQ5LjU0LzMyDQo0MS80Ni8yNDguMTY3LzMy</custom>
7933        </config>
7934      </pfblockerlists>
7935    </installedpackages>
7936    <ovpnserver>
7937      <step1>
7938        <type>local</type>
7939      </step1>
7940      <step6>
7941        <authcertca>50a18d2802392</authcertca>
7942      </step6>
7943      <step9>
7944        <authcertname>50a18e500a587</authcertname>
7945        <certname>ibserver</certname>
7946        <keylength>2088</keylength>
7947        <lifetime>3650</lifetime>
7948        <country>MX</country>
7949        <state>Mexico</state>
7950        <city>DF</city>
7951        <organization>IB</organization>
7952        <email></email>
7953      </step9>
```

```
7954      <step10>
7955        <protocol>UDP</protocol>
7956        <localport>1198</localport>
7957        <tlsauth>on</tlsauth>
7958        <gentlskey>on</gentlskey>
7959        <dhkey>1028</dhkey>
7960        <crypto>AES-128-CBC</crypto>
7961        <engine>none</engine>
7962        <tunnelnet>192.168.10.0/28</tunnelnet>
7963        <rdrgw>on</rdrgw>
7964        <localnet>10.1.0.0/16</localnet>
7965        <compression>on</compression>
7966        <dynip>on</dynip>
7967        <addrpool>on</addrpool>
7968        <nbttype>0</nbttype>
7969        <interface>wan</interface>
7970      </step10>
7971      <step11>
7972        <ovpnrule>on</ovpnrule>
7973        <ovpnallow>on</ovpnallow>
7974      </step11>
7975    </ovpnserver>
7976    <dhcrelay/>
7977  </pfsense>
```

Codigo Fuente Firewall 2

```
1  <?xml version="1.0"?>
2  <pfsense>
3    <version>8.0</version>
4    <lastchange/>
5    <theme>the_wall</theme>
6    <sysctl>
7      <item>
8        <descr><![CDATA[Disable the pf ftp proxy handler.]]></descr>
9        <tunable>debug.pfftpproxy</tunable>
10       <value>default</value>
11     </item>
12     <item>
13       <descr><![CDATA[Increase UFS read-ahead speeds to match ↩
             current state of hard drives and NCQ. More information ↩
             here: http://ivoras.sharanet.org/blog/tree/2010-11-19.ufs-↩
             read-ahead.html]]></descr>
14       <tunable>vfs.read_max</tunable>
15       <value>default</value>
```

```
16      </item>
17      <item>
18        <descr><![CDATA[Set the ephemeral port range to be lower.]]><↩
              /descr>
19        <tunable>net.inet.ip.portrange.first</tunable>
20        <value>default</value>
21      </item>
22      <item>
23        <descr><![CDATA[Drop packets to closed TCP ports without ↩
              returning a RST]]></descr>
24        <tunable>net.inet.tcp.blackhole</tunable>
25        <value>default</value>
26      </item>
27      <item>
28        <descr><![CDATA[Do not send ICMP port unreachable messages ↩
              for closed UDP ports]]></descr>
29        <tunable>net.inet.udp.blackhole</tunable>
30        <value>default</value>
31      </item>
32      <item>
33        <descr><![CDATA[Randomize the ID field in IP packets (default↩
               is 0: sequential IP IDs)]]></descr>
34        <tunable>net.inet.ip.random_id</tunable>
35        <value>default</value>
36      </item>
37      <item>
38        <descr><![CDATA[Drop SYN-FIN packets (breaks RFC1379, but ↩
              nobody uses it anyway)]]></descr>
39        <tunable>net.inet.tcp.drop_synfin</tunable>
40        <value>default</value>
41      </item>
42      <item>
43        <descr><![CDATA[Enable sending IPv4 redirects]]></descr>
44        <tunable>net.inet.ip.redirect</tunable>
45        <value>default</value>
46      </item>
47      <item>
48        <descr><![CDATA[Enable sending IPv6 redirects]]></descr>
49        <tunable>net.inet6.ip6.redirect</tunable>
50        <value>default</value>
51      </item>
52      <item>
53        <descr><![CDATA[Generate SYN cookies for outbound SYN-ACK ↩
              packets]]></descr>
54        <tunable>net.inet.tcp.syncookies</tunable>
55        <value>default</value>
56      </item>
```

```
57      <item>
58        <descr><![CDATA[Maximum incoming/outgoing TCP datagram size (↩
              receive)]]></descr>
59        <tunable>net.inet.tcp.recvspace</tunable>
60        <value>default</value>
61      </item>
62      <item>
63        <descr><![CDATA[Maximum incoming/outgoing TCP datagram size (↩
              send)]]></descr>
64        <tunable>net.inet.tcp.sendspace</tunable>
65        <value>default</value>
66      </item>
67      <item>
68        <descr><![CDATA[IP Fastforwarding]]></descr>
69        <tunable>net.inet.ip.fastforwarding</tunable>
70        <value>default</value>
71      </item>
72      <item>
73        <descr><![CDATA[Do not delay ACK to try and piggyback it onto↩
              a data packet]]></descr>
74        <tunable>net.inet.tcp.delayed_ack</tunable>
75        <value>default</value>
76      </item>
77      <item>
78        <descr><![CDATA[Maximum outgoing UDP datagram size]]></descr>
79        <tunable>net.inet.udp.maxdgram</tunable>
80        <value>default</value>
81      </item>
82      <item>
83        <descr><![CDATA[Handling of non-IP packets which are not ↩
              passed to pfil (see if_bridge(4))]]></descr>
84        <tunable>net.link.bridge.pfil_onlyip</tunable>
85        <value>default</value>
86      </item>
87      <item>
88        <descr><![CDATA[Set to 0 to disable filtering on the incoming↩
              and outgoing member interfaces.]]></descr>
89        <tunable>net.link.bridge.pfil_member</tunable>
90        <value>default</value>
91      </item>
92      <item>
93        <descr><![CDATA[Set to 1 to enable filtering on the bridge ↩
              interface]]></descr>
94        <tunable>net.link.bridge.pfil_bridge</tunable>
95        <value>default</value>
96      </item>
97      <item>
```

```
98        <descr><![CDATA[Allow unprivileged access to tap(4) device ↩
              nodes]]></descr>
99        <tunable>net.link.tap.user_open</tunable>
100       <value>default</value>
101     </item>
102     <item>
103       <descr><![CDATA[Randomize PIDs (see src/sys/kern/kern_fork.c:↩
              sysctl_kern_randompid())]]></descr>
104       <tunable>kern.randompid</tunable>
105       <value>default</value>
106     </item>
107     <item>
108       <descr><![CDATA[Maximum size of the IP input queue]]></descr>
109       <tunable>net.inet.ip.intr_queue_maxlen</tunable>
110       <value>default</value>
111     </item>
112     <item>
113       <descr><![CDATA[Disable CTRL+ALT+Delete reboot from keyboard.↩
              ]]></descr>
114       <tunable>hw.syscons.kbd_reboot</tunable>
115       <value>default</value>
116     </item>
117     <item>
118       <descr><![CDATA[Enable TCP Inflight mode]]></descr>
119       <tunable>net.inet.tcp.inflight.enable</tunable>
120       <value>default</value>
121     </item>
122     <item>
123       <descr><![CDATA[Enable TCP extended debugging]]></descr>
124       <tunable>net.inet.tcp.log_debug</tunable>
125       <value>default</value>
126     </item>
127     <item>
128       <descr><![CDATA[Set ICMP Limits]]></descr>
129       <tunable>net.inet.icmp.icmplim</tunable>
130       <value>default</value>
131     </item>
132     <item>
133       <descr><![CDATA[TCP Offload Engine]]></descr>
134       <tunable>net.inet.tcp.tso</tunable>
135       <value>default</value>
136     </item>
137     <item>
138       <descr><![CDATA[Maximum socket buffer size]]></descr>
139       <tunable>kern.ipc.maxsockbuf</tunable>
140       <value>default</value>
141     </item>
```

```
142   </sysctl>
143   <system>
144     <optimization>normal</optimization>
145     <hostname>hook</hostname>
146     <domain>ib.unam.mx</domain>
147     <group>
148       <name>all</name>
149       <description><![CDATA[All Users]]></description>
150       <scope>system</scope>
151       <gid>1998</gid>
152     </group>
153     <group>
154       <name>admins</name>
155       <description><![CDATA[System Administrators]]></description>
156       <scope>system</scope>
157       <gid>1999</gid>
158       <member>0</member>
159       <priv>page-all</priv>
160     </group>
161
162     <user>
163       <scope>user</scope>
164       <name>alfredo</name>
165       <descr><![CDATA[Alfredo Wong]]></descr>
166       <expires/>
167       <authorizedkeys/>
168       <ipsecpsk/>
169       <uid>2000</uid>
170       <priv>page-dashboard-all</priv>
171       <priv>page-diagnostics-crash-reporter</priv>
172       <priv>page-diagnostics-logs-dhcp</priv>
173       <priv>page-diagnostics-logs-firewall</priv>
174       <priv>page-diagnostics-packetcapture</priv>
175       <priv>page-diagnostics-ping</priv>
176       <priv>page-diagnostics-routingtables</priv>
177       <priv>page-diagnostics-showstates</priv>
178       <priv>page-diagnostics-wirelessstatus</priv>
179       <priv>page-services-captiveportal</priv>
180       <priv>page-services-captiveportal-allowedhostnames</priv>
181       <priv>page-services-captiveportal-allowedips</priv>
182       <priv>page-services-captiveportal-editallowedhostnames</priv>
183       <priv>page-services-captiveportal-editallowedips</priv>
184       <priv>page-services-captiveportal-editmacaddresses</priv>
185       <priv>page-services-captiveportal-filemanager</priv>
186       <priv>page-services-captiveportal-macaddresses</priv>
187       <priv>page-services-captiveportal-voucher-edit</priv>
188       <priv>page-services-captiveportal-vouchers</priv>
```

```
189         <priv>page-services-dhcpserver</priv>
190         <priv>page-services-dhcpserver-editstaticmapping</priv>
191         <priv>page-status-captiveportal</priv>
192         <priv>page-status-captiveportal-test</priv>
193         <priv>page-status-captiveportal-voucher-rolls</priv>
194         <priv>page-status-captiveportal-vouchers</priv>
195         <priv>page-status-dhcpleases</priv>
196         <priv>page-status-filterreloadstatus</priv>
197         <priv>page-status-trafficgraph</priv>
198         <priv>page-diagnostics-arptable</priv>
199         <priv>page-diagnostics-backup/restore</priv>
200         <priv>page-diagnostics-command</priv>
201         <priv>page-diagnostics-configurationhistory</priv>
202         <priv>page-diagnostics-tables</priv>
203         <priv>page-diagnostics-traceroute</priv>
204       </user>
205       <nextuid>2001</nextuid>
206       <nextgid>2000</nextgid>
207       <timezone>America/Mexico_City</timezone>
208       <time-update-interval/>
209       <timeservers>0.pfsense.pool.ntp.org</timeservers>
210       <webgui>
211         <protocol>http</protocol>
212         <ssl-certref>4fe4a0973902d</ssl-certref>
213         <port/>
214         <max_procs>2</max_procs>
215         <nohttpreferercheck/>
216         <noantilockout/>
217       </webgui>
218       <disablenatreflection>yes</disablenatreflection>
219       <disablesegmentationoffloading/>
220       <disablelargereceiveoffloading/>
221       <enablesshd>enabled</enablesshd>
222       <dns1gwint>none</dns1gwint>
223       <dns2gwint>none</dns2gwint>
224       <dns3gwint>none</dns3gwint>
225       <dns4gwint>none</dns4gwint>
226       <dnsserver>10.1.16.253</dnsserver>
227     </system>
228     <interfaces>
229       <wan>
230         <enable/>
231         <if>bce1</if>
232         <ipaddr>10.1.16.2</ipaddr>
233         <subnet>24</subnet>
234         <gateway>WANGW</gateway>
235         <media/>
```

```
236         <mediaopt/>
237         <descr><![CDATA[WAN]]></descr>
238       </wan>
239       <lan>
240         <enable/>
241         <if>bce3</if>
242         <descr><![CDATA[LAN]]></descr>
243         <ipaddr>10.1.0.253</ipaddr>
244         <subnet>24</subnet>
245         <spoofmac/>
246       </lan>
247       <opt1>
248         <descr><![CDATA[vlan118]]></descr>
249         <if>bce3_vlan118</if>
250         <enable/>
251         <spoofmac/>
252         <ipaddr>10.1.118.254</ipaddr>
253         <subnet>24</subnet>
254       </opt1>
255       <opt2>
256         <descr><![CDATA[VlanAdmin]]></descr>
257         <if>bce3_vlan399</if>
258         <spoofmac/>
259         <ipaddr>10.1.251.14</ipaddr>
260         <subnet>16</subnet>
261       </opt2>
262       <opt3>
263         <descr><![CDATA[vlan102]]></descr>
264         <if>bce3_vlan102</if>
265         <enable/>
266         <spoofmac/>
267         <ipaddr>10.1.2.254</ipaddr>
268         <subnet>24</subnet>
269       </opt3>
270       <opt4>
271         <descr><![CDATA[vlan103]]></descr>
272         <if>bce3_vlan103</if>
273         <enable/>
274         <spoofmac/>
275         <ipaddr>10.1.3.254</ipaddr>
276         <subnet>24</subnet>
277       </opt4>
278       <opt5>
279         <descr><![CDATA[vlan104]]></descr>
280         <if>bce3_vlan104</if>
281         <enable/>
282         <spoofmac>78:2b:cb:3c:ce:d9</spoofmac>
```

```
283         <ipaddr>10.1.4.254</ipaddr>
284         <subnet>24</subnet>
285       </opt5>
286       <opt6>
287         <descr><![CDATA[vlan105]]></descr>
288         <if>bce3_vlan105</if>
289         <enable/>
290         <ipaddr>10.1.5.254</ipaddr>
291         <subnet>24</subnet>
292         <spoofmac/>
293       </opt6>
294       <opt7>
295         <descr><![CDATA[vlan107]]></descr>
296         <if>bce3_vlan107</if>
297         <enable/>
298         <ipaddr>10.1.7.254</ipaddr>
299         <subnet>24</subnet>
300         <spoofmac/>
301       </opt7>
302       <opt8>
303         <descr><![CDATA[vlan108]]></descr>
304         <if>bce3_vlan108</if>
305         <enable/>
306         <ipaddr>10.1.8.254</ipaddr>
307         <subnet>24</subnet>
308         <spoofmac/>
309       </opt8>
310       <opt9>
311         <descr><![CDATA[vlan109]]></descr>
312         <if>bce3_vlan109</if>
313         <enable/>
314         <ipaddr>10.1.9.254</ipaddr>
315         <subnet>24</subnet>
316         <spoofmac/>
317       </opt9>
318       <opt10>
319         <descr><![CDATA[vlan110]]></descr>
320         <if>bce3_vlan110</if>
321         <enable/>
322         <ipaddr>10.1.10.254</ipaddr>
323         <subnet>24</subnet>
324         <spoofmac/>
325       </opt10>
326       <opt11>
327         <descr><![CDATA[CAM]]></descr>
328         <if>bce3_vlan500</if>
329         <enable/>
```

```
330         <ipaddr>10.1.100.254</ipaddr>
331         <subnet>24</subnet>
332         <spoofmac/>
333       </opt11>
334       <opt12>
335         <descr><![CDATA[WifiOpen]]></descr>
336         <if>bce3_vlan66</if>
337         <enable/>
338         <ipaddr>10.1.66.254</ipaddr>
339         <subnet>24</subnet>
340         <spoofmac/>
341       </opt12>
342       <opt13>
343         <descr><![CDATA[LAB]]></descr>
344         <if>bce3_vlan23</if>
345         <enable/>
346         <ipaddr>10.1.23.254</ipaddr>
347         <subnet>24</subnet>
348         <spoofmac/>
349       </opt13>
350     </interfaces>
351     <staticroutes>
352       <route>
353         <network>10.1.0.0/16</network>
354         <gateway>WANGW</gateway>
355         <descr/>
356       </route>
357     </staticroutes>
358     <dhcpd>
359       <lan>
360         <range>
361           <from>10.1.0.1</from>
362           <to>10.1.0.252</to>
363         </range>
364         <defaultleasetime/>
365         <maxleasetime/>
366         <netmask/>
367         <failover_peerip/>
368         <gateway/>
369         <domain/>
370         <domainsearchlist/>
371         <ddnsdomain/>
372         <tftp/>
373         <ldap/>
374         <next-server/>
375         <filename/>
376         <rootpath/>
```

```
377         <numberoptions/>
378       </lan>
379       <opt3>
380         <range>
381           <from>10.1.2.1</from>
382           <to>10.1.2.253</to>
383         </range>
384         <defaultleasetime/>
385         <maxleasetime/>
386         <netmask/>
387         <failover_peerip/>
388         <gateway>10.1.2.254</gateway>
389         <domain/>
390         <domainsearchlist/>
391         <enable/>
392         <ddnsdomain/>
393         <tftp/>
394         <ldap/>
395         <next-server/>
396         <filename/>
397         <rootpath/>
398         <numberoptions/>
399       </opt3>
400       <opt4>
401         <range>
402           <from>10.1.3.1</from>
403           <to>10.1.3.240</to>
404         </range>
405         <defaultleasetime/>
406         <maxleasetime/>
407         <netmask/>
408         <failover_peerip/>
409         <gateway>10.1.3.254</gateway>
410         <domain/>
411         <domainsearchlist/>
412         <enable/>
413         <ddnsdomain/>
414         <tftp/>
415         <ldap/>
416         <next-server/>
417         <filename/>
418         <rootpath/>
419         <numberoptions/>
420         <staticmap>
421           <mac>00:25:b3:fb:5f:bd</mac>
422           <ipaddr>10.1.3.241</ipaddr>
423           <hostname>hp_laserjet_P2035n</hostname>
```

```
424         <descr><![CDATA[Dra. helga Ochoterena]]></descr>
425         <netbootfile/>
426       </staticmap>
427     </opt4>
428     <opt5>
429       <range>
430         <from>10.1.4.1</from>
431         <to>10.1.4.220</to>
432       </range>
433       <defaultleasetime/>
434       <maxleasetime/>
435       <netmask/>
436       <failover_peerip/>
437       <gateway>10.1.4.254</gateway>
438       <domain/>
439       <domainsearchlist/>
440       <enable/>
441       <ddnsdomain/>
442       <tftp/>
443       <ldap/>
444       <next-server/>
445       <filename/>
446       <rootpath/>
447       <numberoptions/>
448       <staticmap>
449         <mac>38:60:77:8b:de:ef</mac>
450         <ipaddr>10.1.4.227</ipaddr>
451         <hostname>Personal</hostname>
452         <descr/>
453         <netbootfile/>
454       </staticmap>
455       <staticmap>
456         <mac>00:50:56:8c:e0:f5</mac>
457         <ipaddr>10.1.4.228</ipaddr>
458         <hostname>ciscoiou</hostname>
459         <descr><![CDATA[lab cisco]]></descr>
460         <netbootfile/>
461       </staticmap>
462       <staticmap>
463         <mac>f8:1a:67:d6:d4:96</mac>
464         <ipaddr>10.1.4.229</ipaddr>
465         <hostname>ap_secacad_test</hostname>
466         <descr><![CDATA[Nuevo AP TPlink de prueba]]></descr>
467         <netbootfile/>
468       </staticmap>
469       <staticmap>
470         <mac>00:50:56:8c:26:af</mac>
```

```
471         <ipaddr>10.1.4.230</ipaddr>
472         <hostname>moodle</hostname>
473         <descr><![CDATA[moodle]]></descr>
474         <netbootfile/>
475       </staticmap>
476       <staticmap>
477         <mac>00:0c:29:3c:a5:f6</mac>
478         <ipaddr>10.1.4.231</ipaddr>
479         <hostname>vegeta_t</hostname>
480         <descr/>
481         <netbootfile/>
482       </staticmap>
483       <staticmap>
484         <mac>70:71:bc:a8:31:4a</mac>
485         <ipaddr>10.1.4.233</ipaddr>
486         <hostname>mena</hostname>
487         <descr><![CDATA[yop]]></descr>
488         <netbootfile/>
489       </staticmap>
490       <staticmap>
491         <mac>00:14:22:27:26:6a</mac>
492         <ipaddr>10.1.4.238</ipaddr>
493         <hostname>admon_ds009</hostname>
494         <descr><![CDATA[Administrativa]]></descr>
495         <netbootfile/>
496       </staticmap>
497       <staticmap>
498         <mac>00:40:05:06:6e:ad</mac>
499         <ipaddr>10.1.4.240</ipaddr>
500         <hostname>informe</hostname>
501         <descr><![CDATA[informe y registro de alumnos]]></descr>
502         <netbootfile/>
503       </staticmap>
504       <staticmap>
505         <mac>68:7f:74:12:0c:1c</mac>
506         <ipaddr>10.1.4.241</ipaddr>
507         <hostname>ap_presup</hostname>
508         <descr><![CDATA[Don Jefe Comi wireless]]></descr>
509         <netbootfile/>
510       </staticmap>
511       <staticmap>
512         <mac>00:00:85:40:3e:ac</mac>
513         <ipaddr>10.1.4.242</ipaddr>
514         <hostname>Canon_3570</hostname>
515         <descr><![CDATA[Sandy copiadora]]></descr>
516         <netbootfile/>
517       </staticmap>
```

```
518         <staticmap>
519           <mac>00:01:e6:a9:d7:94</mac>
520           <ipaddr>10.1.4.243</ipaddr>
521           <hostname>UDC_8150</hostname>
522           <descr><![CDATA[HP Laser Jet 8150]]></descr>
523           <netbootfile/>
524         </staticmap>
525         <staticmap>
526           <mac>00:00:85:59:1a:86</mac>
527           <ipaddr>10.1.4.244</ipaddr>
528           <hostname>canon_IR</hostname>
529           <descr/>
530           <netbootfile/>
531         </staticmap>
532         <staticmap>
533           <mac>00:00:85:73:55:98</mac>
534           <ipaddr>10.1.4.247</ipaddr>
535           <hostname>Secretaria_Academica</hostname>
536           <descr><![CDATA[Impresora]]></descr>
537           <netbootfile/>
538         </staticmap>
539         <staticmap>
540           <mac>78:2b:cb:b5:e7:37</mac>
541           <ipaddr>10.1.4.248</ipaddr>
542           <hostname>Victor</hostname>
543           <descr><![CDATA[Dr. Victor Sanchez Cordero]]></descr>
544           <netbootfile/>
545         </staticmap>
546         <staticmap>
547           <mac>70:71:bc:63:cc:25</mac>
548           <ipaddr>10.1.4.250</ipaddr>
549           <hostname>Marilu</hostname>
550           <descr><![CDATA[Direccion Marilu]]></descr>
551           <netbootfile/>
552         </staticmap>
553         <staticmap>
554           <mac>70:71:bc:63:d1:39</mac>
555           <ipaddr>10.1.4.251</ipaddr>
556           <hostname>Alicia</hostname>
557           <descr><![CDATA[Direccion Alicia]]></descr>
558           <netbootfile/>
559         </staticmap>
560         <staticmap>
561           <mac>00:1a:92:25:e0:0b</mac>
562           <ipaddr>10.1.4.252</ipaddr>
563           <hostname>Rupa_server</hostname>
564           <descr><![CDATA[Rupa]]></descr>
```

```
565         <netbootfile/>
566       </staticmap>
567       <staticmap>
568         <mac>00:50:56:8c:de:19</mac>
569         <ipaddr>10.1.4.253</ipaddr>
570         <hostname>Web_Page</hostname>
571         <descr><![CDATA[Peterson]]></descr>
572         <netbootfile/>
573       </staticmap>
574     </opt5>
575     <opt6>
576       <range>
577         <from>10.1.5.1</from>
578         <to>10.1.5.239</to>
579       </range>
580       <defaultleasetime/>
581       <maxleasetime/>
582       <netmask/>
583       <failover_peerip/>
584       <gateway>10.1.5.254</gateway>
585       <domain/>
586       <domainsearchlist/>
587       <enable/>
588       <ddnsdomain/>
589       <tftp/>
590       <ldap/>
591       <next-server/>
592       <filename/>
593       <rootpath/>
594       <numberoptions/>
595       <staticmap>
596         <mac>00:10:18:b5:24:70</mac>
597         <ipaddr>10.1.5.240</ipaddr>
598         <hostname>Secuenciador</hostname>
599         <descr><![CDATA[Secuenciador Laura nuevo]]></descr>
600         <netbootfile/>
601       </staticmap>
602       <staticmap>
603         <mac>00:11:09:d2:f6:e1</mac>
604         <ipaddr>10.1.5.241</ipaddr>
605         <hostname>Tipos_printer</hostname>
606         <descr><![CDATA[Equipo con impresora compartida Tipos]]></↩
              descr>
607         <netbootfile/>
608       </staticmap>
609     </opt6>
610     <opt7>
```

```
611         <range>
612           <from>10.1.7.1</from>
613           <to>10.1.7.240</to>
614         </range>
615         <defaultleasetime/>
616         <maxleasetime/>
617         <netmask/>
618         <failover_peerip/>
619         <gateway>10.1.7.254</gateway>
620         <domain/>
621         <domainsearchlist/>
622         <enable/>
623         <ddnsdomain/>
624         <tftp/>
625         <ldap/>
626         <next-server/>
627         <filename/>
628         <rootpath/>
629         <numberoptions/>
630         <staticmap>
631           <mac>00:1f:29:29:72:62</mac>
632           <ipaddr>10.1.7.241</ipaddr>
633           <hostname>hp_LaserJet_P2015</hostname>
634           <descr><![CDATA[Dr. Luis Zambrano]]></descr>
635           <netbootfile/>
636         </staticmap>
637         <staticmap>
638           <mac>00:21:5a:8d:b7:74</mac>
639           <ipaddr>10.1.7.242</ipaddr>
640           <hostname>hp_laserjet_P2035n</hostname>
641           <descr><![CDATA[Dr.Victor Sanchez Cordero]]></descr>
642           <netbootfile/>
643         </staticmap>
644         <staticmap>
645           <mac>00:50:aa:27:67:1a</mac>
646           <ipaddr>10.1.7.243</ipaddr>
647           <hostname>Konica_Minolta</hostname>
648           <descr><![CDATA[Copiadora Sec Tec]]></descr>
649           <netbootfile/>
650         </staticmap>
651         <staticmap>
652           <mac>78:ca:39:ff:03:ac</mac>
653           <ipaddr>10.1.7.244</ipaddr>
654           <hostname>capsula</hostname>
655           <descr><![CDATA[time capsule]]></descr>
656           <netbootfile/>
657         </staticmap>
```

```
658     </opt7>
659     <opt8>
660       <range>
661         <from>10.1.8.3</from>
662         <to>10.1.8.240</to>
663       </range>
664       <defaultleasetime/>
665       <maxleasetime/>
666       <netmask/>
667       <failover_peerip/>
668       <gateway>10.1.8.254</gateway>
669       <domain/>
670       <domainsearchlist/>
671       <enable/>
672       <ddnsdomain/>
673       <tftp/>
674       <ldap/>
675       <next-server/>
676       <filename/>
677       <rootpath/>
678       <numberoptions/>
679       <staticmap>
680         <mac>00:09:f6:02:e6:3c</mac>
681         <ipaddr>10.1.8.2</ipaddr>
682         <hostname>Sys_control_entrada</hostname>
683         <descr><![CDATA[Pluma de estacionamiento.]]></descr>
684         <netbootfile/>
685       </staticmap>
686       <staticmap>
687         <mac>00:21:5a:96:9c:5e</mac>
688         <ipaddr>10.1.8.246</ipaddr>
689         <hostname>hp_laserjet_p1505</hostname>
690         <descr><![CDATA[Dr. Johanssen]]></descr>
691         <netbootfile/>
692       </staticmap>
693       <staticmap>
694         <mac>44:1e:a1:32:db:8b</mac>
695         <ipaddr>10.1.8.247</ipaddr>
696         <hostname>hp_Laser_Cp1525</hostname>
697         <descr/>
698         <netbootfile/>
699       </staticmap>
700       <staticmap>
701         <mac>00:90:4c:60:04:00</mac>
702         <ipaddr>10.1.8.248</ipaddr>
703         <hostname>ap_acaros</hostname>
704         <descr><![CDATA[lab acaros]]></descr>
```

```
705         <netbootfile/>
706       </staticmap>
707       <staticmap>
708         <mac>64:66:b3:5d:46:1a</mac>
709         <ipaddr>10.1.8.252</ipaddr>
710         <hostname>ap_caseta2</hostname>
711         <descr><![CDATA[Caseta de vigilancia instalada]]></descr>
712         <netbootfile/>
713       </staticmap>
714       <staticmap>
715         <mac>90:f6:52:be:d7:56</mac>
716         <ipaddr>10.1.8.253</ipaddr>
717         <hostname>nodo_cas</hostname>
718         <descr><![CDATA[Nodo casetal laboratorio]]></descr>
719         <netbootfile/>
720       </staticmap>
721     </opt8>
722     <opt9>
723       <range>
724         <from>10.1.9.1</from>
725         <to>10.1.9.200</to>
726       </range>
727       <defaultleasetime/>
728       <maxleasetime/>
729       <netmask/>
730       <failover_peerip/>
731       <gateway>10.1.9.254</gateway>
732       <domain/>
733       <domainsearchlist/>
734       <enable/>
735       <ddnsdomain/>
736       <tftp/>
737       <ldap/>
738       <next-server/>
739       <filename/>
740       <rootpath/>
741       <numberoptions/>
742       <staticmap>
743         <mac>38:ea:a7:09:66:57</mac>
744         <ipaddr>10.1.9.209</ipaddr>
745         <hostname>Printer_New</hostname>
746         <descr><![CDATA[Impresora Fija JB]]></descr>
747         <netbootfile/>
748       </staticmap>
749       <staticmap>
750         <mac>e8:40:f2:e2:45:ad</mac>
751         <ipaddr>10.1.9.210</ipaddr>
```

```
752         <hostname>tigrida</hostname>
753         <descr><![CDATA[server]]></descr>
754         <netbootfile/>
755       </staticmap>
756     </opt9>
757     <opt10>
758       <range>
759         <from>10.1.10.1</from>
760         <to>10.1.10.153</to>
761       </range>
762       <defaultleasetime/>
763       <maxleasetime/>
764       <netmask/>
765       <failover_peerip/>
766       <gateway>10.1.10.254</gateway>
767       <domain/>
768       <domainsearchlist/>
769       <enable/>
770       <ddnsdomain/>
771       <tftp/>
772       <ldap/>
773       <next-server/>
774       <filename/>
775       <rootpath/>
776       <numberoptions/>
777     </opt10>
778     <opt11>
779       <staticmap>
780         <mac>00:40:48:37:78:63</mac>
781         <ipaddr>10.1.100.1</ipaddr>
782         <hostname>CAM-b-pp</hostname>
783         <descr><![CDATA[DVR B-pp]]></descr>
784         <netbootfile/>
785       </staticmap>
786       <staticmap>
787         <mac>00:40:48:3a:64:10</mac>
788         <ipaddr>10.1.100.2</ipaddr>
789         <hostname>CAM_Bpb</hostname>
790         <descr><![CDATA[DVR ED.Bpb]]></descr>
791         <netbootfile/>
792       </staticmap>
793       <staticmap>
794         <mac>00:40:48:37:03:b0</mac>
795         <ipaddr>10.1.100.3</ipaddr>
796         <hostname>CAM-App</hostname>
797         <descr><![CDATA[DVR Ed.A pp]]></descr>
798         <netbootfile/>
```

```
799         </staticmap>
800         <staticmap>
801           <mac>00:40:48:20:23:79</mac>
802           <ipaddr>10.1.100.4</ipaddr>
803           <hostname>CAM_Cpp</hostname>
804           <descr><![CDATA[DVR Ed.Cpp]]></descr>
805           <netbootfile/>
806         </staticmap>
807         <staticmap>
808           <mac>00:40:48:37:77:f9</mac>
809           <ipaddr>10.1.100.5</ipaddr>
810           <hostname>CAM_Dpp</hostname>
811           <descr><![CDATA[DVR Ed. Dpp]]></descr>
812           <netbootfile/>
813         </staticmap>
814         <staticmap>
815           <mac>00:18:ae:2f:b0:33</mac>
816           <ipaddr>10.1.100.6</ipaddr>
817           <hostname>DVR_ED_Principal</hostname>
818           <descr><![CDATA[camara de edificio principal]]></descr>
819           <netbootfile/>
820         </staticmap>
821         <staticmap>
822           <mac>00:18:ae:2f:b0:31</mac>
823           <ipaddr>10.1.100.7</ipaddr>
824           <hostname>DVR_Ed_Col</hostname>
825           <descr><![CDATA[Camaras de edificio de colecciones]]></↩
                descr>
826           <netbootfile/>
827         </staticmap>
828         <staticmap>
829           <mac>00:18:ae:2f:b0:30</mac>
830           <ipaddr>10.1.100.8</ipaddr>
831           <hostname>dvr_tigridia</hostname>
832           <descr><![CDATA[tienda]]></descr>
833           <netbootfile/>
834         </staticmap>
835         <range>
836           <from>10.1.100.10</from>
837           <to>10.1.100.20</to>
838         </range>
839         <defaultleasetime/>
840         <maxleasetime/>
841         <netmask/>
842         <failover_peerip/>
843         <gateway>10.1.100.254</gateway>
844         <domain/>
```

```
845         <domainsearchlist/>
846         <enable/>
847         <ddnsdomain/>
848         <tftp/>
849         <ldap/>
850         <next-server/>
851         <filename/>
852         <rootpath/>
853         <numberoptions/>
854       </opt11>
855       <opt12>
856         <range>
857           <from>10.1.66.20</from>
858           <to>10.1.66.250</to>
859         </range>
860         <defaultleasetime/>
861         <maxleasetime/>
862         <netmask/>
863         <failover_peerip/>
864         <gateway>10.1.66.254</gateway>
865         <domain/>
866         <domainsearchlist/>
867         <enable/>
868         <ddnsdomain/>
869         <tftp/>
870         <ldap/>
871         <next-server/>
872         <filename/>
873         <rootpath/>
874         <numberoptions/>
875         <staticmap>
876           <mac>00:11:88:92:68:33</mac>
877           <ipaddr>10.1.66.1</ipaddr>
878           <hostname>ap_videoconferencia</hostname>
879           <descr/>
880           <netbootfile/>
881         </staticmap>
882         <staticmap>
883           <mac>68:7f:74:6a:88:a8</mac>
884           <ipaddr>10.1.66.2</ipaddr>
885           <hostname>ap_biblioteca</hostname>
886           <descr/>
887           <netbootfile/>
888         </staticmap>
889         <staticmap>
890           <mac>00:12:17:74:b6:8f</mac>
891           <ipaddr>10.1.66.3</ipaddr>
```

```
892           <hostname>ap_UDC</hostname>
893           <descr/>
894           <netbootfile/>
895         </staticmap>
896         <staticmap>
897           <mac>00:12:17:7b:2f:3a</mac>
898           <ipaddr>10.1.66.5</ipaddr>
899           <hostname/>
900           <descr/>
901           <netbootfile/>
902         </staticmap>
903         <staticmap>
904           <mac>a0:f3:c1:6c:49:8d</mac>
905           <ipaddr>10.1.66.6</ipaddr>
906           <hostname>biblioteca</hostname>
907           <descr/>
908           <netbootfile/>
909         </staticmap>
910       </opt12>
911       <opt1>
912         <range>
913           <from>10.1.118.40</from>
914           <to>10.1.118.250</to>
915         </range>
916         <defaultleasetime/>
917         <maxleasetime/>
918         <netmask></netmask>
919         <failover_peerip/>
920         <gateway>10.1.118.254</gateway>
921         <domain/>
922         <domainsearchlist/>
923         <enable/>
924         <ddnsdomain/>
925         <tftp/>
926         <ldap/>
927         <next-server/>
928         <filename/>
929         <rootpath/>
930         <numberoptions/>
931         <staticmap>
932           <mac>64:66:b3:8c:36:da</mac>
933           <ipaddr>10.1.118.1</ipaddr>
934           <hostname>ap_mastozologia</hostname>
935           <descr/>
936           <netbootfile/>
937         </staticmap>
938         <staticmap>
```

```
939           <mac>a0:f3:c1:64:30:6e</mac>
940           <ipaddr>10.1.118.2</ipaddr>
941           <hostname>ap_helmintos</hostname>
942           <descr><![CDATA[Dr. Gerardo Perez Ponce de Leon Ed.D–2pp ↩
                  LAB]]></descr>
943           <netbootfile/>
944         </staticmap>
945         <staticmap>
946           <mac>00:0c:41:d8:0f:c3</mac>
947           <ipaddr>10.1.118.3</ipaddr>
948           <hostname>ap_carcinologia</hostname>
949           <descr/>
950           <netbootfile/>
951         </staticmap>
952         <staticmap>
953           <mac>64:70:02:ca:4f:f7</mac>
954           <ipaddr>10.1.118.4</ipaddr>
955           <hostname>ap_gernandt</hostname>
956           <descr><![CDATA[Tp–Link]]></descr>
957           <netbootfile/>
958         </staticmap>
959         <staticmap>
960           <mac>68:7f:74:69:57:8e</mac>
961           <ipaddr>10.1.118.5</ipaddr>
962           <hostname>ap_restauracion</hostname>
963           <descr/>
964           <netbootfile/>
965         </staticmap>
966         <staticmap>
967           <mac>00:12:17:70:6d:f7</mac>
968           <ipaddr>10.1.118.6</ipaddr>
969           <hostname>ap_emm</hostname>
970           <descr/>
971           <netbootfile/>
972         </staticmap>
973         <staticmap>
974           <mac>00:12:17:a9:ef:29</mac>
975           <ipaddr>10.1.118.7</ipaddr>
976           <hostname>ap_cgonzalez</hostname>
977           <descr/>
978           <netbootfile/>
979         </staticmap>
980         <staticmap>
981           <mac>00:0f:66:75:26:a8</mac>
982           <ipaddr>10.1.118.8</ipaddr>
983           <hostname>ap_molecular</hostname>
984           <descr/>
```

```
985           <netbootfile/>
986         </staticmap>
987         <staticmap>
988           <mac>00:0f:66:19:7b:d2</mac>
989           <ipaddr>10.1.118.9</ipaddr>
990           <hostname>ap_espaciales</hostname>
991           <descr/>
992           <netbootfile/>
993         </staticmap>
994         <staticmap>
995           <mac>00:12:17:7a:ea:91</mac>
996           <ipaddr>10.1.118.10</ipaddr>
997           <hostname>ap_magdac</hostname>
998           <descr/>
999           <netbootfile/>
1000        </staticmap>
1001        <staticmap>
1002          <mac>00:21:29:98:7b:46</mac>
1003          <ipaddr>10.1.118.11</ipaddr>
1004          <hostname>ap_sanchezcordero</hostname>
1005          <descr/>
1006          <netbootfile/>
1007        </staticmap>
1008        <staticmap>
1009          <mac>00:12:17:74:b8:e8</mac>
1010          <ipaddr>10.1.118.12</ipaddr>
1011          <hostname>ap_malacologia</hostname>
1012          <descr/>
1013          <netbootfile/>
1014        </staticmap>
1015        <staticmap>
1016          <mac>00:22:3f:0b:78:59</mac>
1017          <ipaddr>10.1.118.13</ipaddr>
1018          <hostname>ap_zaragoza</hostname>
1019          <descr/>
1020          <netbootfile/>
1021        </staticmap>
1022        <staticmap>
1023          <mac>00:1e:58:ec:79:9a</mac>
1024          <ipaddr>10.1.118.16</ipaddr>
1025          <hostname>ap_psilva</hostname>
1026          <descr/>
1027          <netbootfile/>
1028        </staticmap>
1029        <staticmap>
1030          <mac>00:14:bf:7d:96:58</mac>
1031          <ipaddr>10.1.118.17</ipaddr>
```

```
1032          <hostname>ap_smagallon</hostname>
1033          <descr/>
1034          <netbootfile/>
1035        </staticmap>
1036        <staticmap>
1037          <mac>68:7f:74:69:1b:72</mac>
1038          <ipaddr>10.1.118.19</ipaddr>
1039          <hostname>ap_pescados</hostname>
1040          <descr/>
1041          <netbootfile/>
1042        </staticmap>
1043        <staticmap>
1044          <mac>00:25:9c:9e:ee:f1</mac>
1045          <ipaddr>10.1.118.20</ipaddr>
1046          <hostname>ap_atilano</hostname>
1047          <descr/>
1048          <netbootfile/>
1049        </staticmap>
1050        <staticmap>
1051          <mac>08:00:46:d0:04:be</mac>
1052          <ipaddr>10.1.118.21</ipaddr>
1053          <hostname>ap_acaros</hostname>
1054          <descr/>
1055          <netbootfile/>
1056        </staticmap>
1057        <staticmap>
1058          <mac>00:12:17:70:0a:a8</mac>
1059          <ipaddr>10.1.118.23</ipaddr>
1060          <hostname>ap_orquideas</hostname>
1061          <descr/>
1062          <netbootfile/>
1063        </staticmap>
1064        <staticmap>
1065          <mac>00:1d:0f:d8:cd:e8</mac>
1066          <ipaddr>10.1.118.25</ipaddr>
1067          <hostname>ap_taniat</hostname>
1068          <descr><![CDATA[Router Tania Terrazas JB Colecciones]]></↩
                descr>
1069          <netbootfile/>
1070        </staticmap>
1071        <staticmap>
1072          <mac>64:66:b3:8c:33:31</mac>
1073          <ipaddr>10.1.118.26</ipaddr>
1074          <hostname>ap_ornitologia</hostname>
1075          <descr><![CDATA[Coleccion Nacional de Aves]]></descr>
1076          <netbootfile/>
1077        </staticmap>
```

```
1078        <staticmap>
1079          <mac>64:70:02:e0:4b:04</mac>
1080          <ipaddr>10.1.118.27</ipaddr>
1081          <hostname>ap_presup</hostname>
1082          <descr><![CDATA[ap Jefe Comi]]></descr>
1083          <netbootfile/>
1084        </staticmap>
1085        <staticmap>
1086          <mac>64:70:02:bb:8f:2a</mac>
1087          <ipaddr>10.1.118.28</ipaddr>
1088          <hostname>ap_jardin2</hostname>
1089          <descr><![CDATA[Ap del Lobby del Jardin]]></descr>
1090          <netbootfile/>
1091        </staticmap>
1092        <staticmap>
1093          <mac>64:70:02:bb:a1:08</mac>
1094          <ipaddr>10.1.118.29</ipaddr>
1095          <hostname>ap_jardin1</hostname>
1096          <descr><![CDATA[Lugar por definir por Don Dogor]]></descr>
1097          <netbootfile/>
1098        </staticmap>
1099        <staticmap>
1100          <mac>9c:2a:70:6d:0c:94</mac>
1101          <ipaddr>10.1.118.30</ipaddr>
1102          <hostname>HP_David_Gernard</hostname>
1103          <descr/>
1104          <netbootfile/>
1105        </staticmap>
1106        <staticmap>
1107          <mac>f8:1a:67:d6:d4:f5</mac>
1108          <ipaddr>10.1.118.31</ipaddr>
1109          <hostname>ap_agaves</hostname>
1110          <descr><![CDATA[Dr. Abisai]]></descr>
1111          <netbootfile/>
1112        </staticmap>
1113        <staticmap>
1114          <mac>a0:f3:c1:5e:d3:9a</mac>
1115          <ipaddr>10.1.118.32</ipaddr>
1116          <hostname>ap_col</hostname>
1117          <descr><![CDATA[colecciones]]></descr>
1118          <netbootfile/>
1119        </staticmap>
1120        <staticmap>
1121          <mac>00:18:39:02:bc:a6</mac>
1122          <ipaddr>10.1.118.33</ipaddr>
1123          <hostname>ap_Olson</hostname>
1124          <descr><![CDATA[Cubiculo Dr. Mark Olson]]></descr>
```

```
1125          <netbootfile/>
1126        </staticmap>
1127        <staticmap>
1128          <mac>f8:1a:67:d6:d5:45</mac>
1129          <ipaddr>10.1.118.34</ipaddr>
1130          <hostname>ap_Ponce</hostname>
1131          <descr><![CDATA[Ap cubiculo Dr. Gerardo Perez Ponce de Leon↩
                  ]]></descr>
1132          <netbootfile/>
1133        </staticmap>
1134      </opt1>
1135      <wan>
1136        <range>
1137          <from/>
1138          <to/>
1139        </range>
1140        <defaultleasetime/>
1141        <maxleasetime/>
1142        <netmask/>
1143        <failover_peerip/>
1144        <gateway/>
1145        <domain/>
1146        <domainsearchlist/>
1147        <ddnsdomain/>
1148        <tftp/>
1149        <ldap/>
1150        <next-server/>
1151        <filename/>
1152        <rootpath/>
1153        <numberoptions/>
1154      </wan>
1155    </dhcpd>
1156    <pptpd>
1157      <mode/>
1158      <redir/>
1159      <localip/>
1160      <remoteip/>
1161    </pptpd>
1162    <dnsmasq>
1163      <enable/>
1164      <custom_options/>
1165      <hosts>
1166        <host>app</host>
1167        <domain>ib.unam.mx</domain>
1168        <ip>10.1.100.3</ip>
1169        <descr><![CDATA[Ed A primer piso]]></descr>
1170      </hosts>
```

```
1171      <hosts>
1172        <host>colecciones</host>
1173        <domain>ib.unam.mx</domain>
1174        <ip>10.1.100.7</ip>
1175        <descr><![CDATA[col]]></descr>
1176      </hosts>
1177      <hosts>
1178        <host>congresoslccs</host>
1179        <domain>unam.mx</domain>
1180        <ip>10.1.4.239</ip>
1181        <descr><![CDATA[Congreso cactaceas]]></descr>
1182      </hosts>
1183      <hosts>
1184        <host>correo</host>
1185        <domain>ib.unam.mx</domain>
1186        <ip>10.1.4.98</ip>
1187        <descr/>
1188      </hosts>
1189      <hosts>
1190        <host>jb</host>
1191        <domain>ib.unam.mx</domain>
1192        <ip>10.1.100.6</ip>
1193        <descr><![CDATA[dvr jb]]></descr>
1194      </hosts>
1195      <hosts>
1196        <host>secuenciador</host>
1197        <domain>ib.unam.mx</domain>
1198        <ip>10.1.5.240</ip>
1199        <descr><![CDATA[hacia secuenciador]]></descr>
1200      </hosts>
1201    </dnsmasq>
1202    <snmpd>
1203      <syslocation/>
1204      <syscontact/>
1205      <rocommunity>public</rocommunity>
1206    </snmpd>
1207    <diag>
1208      <ipv6nat>
1209        <ipaddr/>
1210      </ipv6nat>
1211    </diag>
1212    <bridge/>
1213    <syslog>
1214      <reverse/>
1215      <nentries>100</nentries>
1216      <filter/>
1217      <system/>
```

```
1218      <remoteserver>10.1.4.20</remoteserver>
1219      <remoteserver2/>
1220      <remoteserver3/>
1221      <dhcp/>
1222      <enable/>
1223    </syslog>
1224    <nat>
1225      <ipsecpassthru>
1226        <enable/>
1227      </ipsecpassthru>
1228      <advancedoutbound>
1229        <enable/>
1230      </advancedoutbound>
1231    </nat>
1232    <filter>
1233      <rule>
1234        <id/>
1235        <type>pass</type>
1236        <interface>lan,opt1</interface>
1237        <tag/>
1238        <tagged/>
1239        <direction>any</direction>
1240        <floating>yes</floating>
1241        <max/>
1242        <max-src-nodes/>
1243        <max-src-conn/>
1244        <max-src-states/>
1245        <statetimeout/>
1246        <statetype>keep state</statetype>
1247        <os/>
1248        <source>
1249          <any/>
1250        </source>
1251        <destination>
1252          <any/>
1253        </destination>
1254        <descr/>
1255      </rule>
1256      <rule>
1257        <id/>
1258        <type>pass</type>
1259        <interface>wan</interface>
1260        <tag/>
1261        <tagged/>
1262        <max/>
1263        <max-src-nodes/>
1264        <max-src-conn/>
```

```
1265        <max-src-states/>
1266        <statetimeout/>
1267        <statetype>keep state</statetype>
1268        <os/>
1269        <source>
1270          <any/>
1271        </source>
1272        <destination>
1273          <any/>
1274        </destination>
1275        <log/>
1276        <descr><![CDATA[Open Wan]]></descr>
1277      </rule>
1278      <rule>
1279        <id/>
1280        <type>pass</type>
1281        <interface>lan</interface>
1282        <tag/>
1283        <tagged/>
1284        <max/>
1285        <max-src-nodes/>
1286        <max-src-conn/>
1287        <max-src-states/>
1288        <statetimeout/>
1289        <statetype>keep state</statetype>
1290        <os/>
1291        <source>
1292          <any/>
1293        </source>
1294        <destination>
1295          <any/>
1296        </destination>
1297        <descr><![CDATA[Default allow LAN to any rule]]></descr>
1298      </rule>
1299      <rule>
1300        <id/>
1301        <type>pass</type>
1302        <interface>opt1</interface>
1303        <tag/>
1304        <tagged/>
1305        <max/>
1306        <max-src-nodes/>
1307        <max-src-conn/>
1308        <max-src-states/>
1309        <statetimeout/>
1310        <statetype>keep state</statetype>
1311        <os/>
```

```
1312        <source>
1313          <any/>
1314        </source>
1315        <destination>
1316          <any/>
1317        </destination>
1318        <descr/>
1319      </rule>
1320      <rule>
1321        <id/>
1322        <type>pass</type>
1323        <interface>opt2</interface>
1324        <tag/>
1325        <tagged/>
1326        <max/>
1327        <max-src-nodes/>
1328        <max-src-conn/>
1329        <max-src-states/>
1330        <statetimeout/>
1331        <statetype>keep state</statetype>
1332        <os/>
1333        <source>
1334          <any/>
1335        </source>
1336        <destination>
1337          <any/>
1338        </destination>
1339        <descr><![CDATA[Trafico administrativo]]></descr>
1340      </rule>
1341      <rule>
1342        <id/>
1343        <type>pass</type>
1344        <interface>opt3</interface>
1345        <tag/>
1346        <tagged/>
1347        <max/>
1348        <max-src-nodes/>
1349        <max-src-conn/>
1350        <max-src-states/>
1351        <statetimeout/>
1352        <statetype>keep state</statetype>
1353        <os/>
1354        <source>
1355          <any/>
1356        </source>
1357        <destination>
1358          <any/>
```

```
1359        </destination>
1360        <descr/>
1361        <dnpipe>1</dnpipe>
1362        <pdnpipe>2</pdnpipe>
1363      </rule>
1364      <rule>
1365        <id/>
1366        <type>pass</type>
1367        <interface>opt4</interface>
1368        <tag/>
1369        <tagged/>
1370        <max/>
1371        <max-src-nodes/>
1372        <max-src-conn/>
1373        <max-src-states/>
1374        <statetimeout/>
1375        <statetype>keep state</statetype>
1376        <os/>
1377        <source>
1378          <any/>
1379        </source>
1380        <destination>
1381          <any/>
1382        </destination>
1383        <descr/>
1384      </rule>
1385      <rule>
1386        <id/>
1387        <type>block</type>
1388        <interface>opt5</interface>
1389        <tag/>
1390        <tagged/>
1391        <max/>
1392        <max-src-nodes/>
1393        <max-src-conn/>
1394        <max-src-states/>
1395        <statetimeout/>
1396        <statetype>keep state</statetype>
1397        <os/>
1398        <protocol>tcp/udp</protocol>
1399        <source>
1400          <address>10.1.4.238</address>
1401        </source>
1402        <destination>
1403          <any/>
1404        </destination>
1405        <log/>
```

```
1406        <descr><![CDATA[block internet]]></descr>
1407      </rule>
1408      <rule>
1409        <id/>
1410        <type>pass</type>
1411        <interface>opt5</interface>
1412        <tag/>
1413        <tagged/>
1414        <max/>
1415        <max-src-nodes/>
1416        <max-src-conn/>
1417        <max-src-states/>
1418        <statetimeout/>
1419        <statetype>keep state</statetype>
1420        <os/>
1421        <source>
1422          <any/>
1423        </source>
1424        <destination>
1425          <any/>
1426        </destination>
1427        <descr/>
1428      </rule>
1429      <rule>
1430        <id/>
1431        <type>pass</type>
1432        <interface>opt6</interface>
1433        <tag/>
1434        <tagged/>
1435        <max/>
1436        <max-src-nodes/>
1437        <max-src-conn/>
1438        <max-src-states/>
1439        <statetimeout/>
1440        <statetype>keep state</statetype>
1441        <os/>
1442        <source>
1443          <any/>
1444        </source>
1445        <destination>
1446          <any/>
1447        </destination>
1448        <descr/>
1449        <dnpipe>1</dnpipe>
1450        <pdnpipe>2</pdnpipe>
1451      </rule>
1452      <rule>
```

```
1453        <id/>
1454        <type>pass</type>
1455        <interface>opt7</interface>
1456        <tag/>
1457        <tagged/>
1458        <max/>
1459        <max-src-nodes/>
1460        <max-src-conn/>
1461        <max-src-states/>
1462        <statetimeout/>
1463        <statetype>keep state</statetype>
1464        <os/>
1465        <source>
1466          <any/>
1467        </source>
1468        <destination>
1469          <any/>
1470        </destination>
1471        <descr/>
1472      </rule>
1473      <rule>
1474        <id/>
1475        <type>pass</type>
1476        <interface>opt8</interface>
1477        <tag/>
1478        <tagged/>
1479        <max/>
1480        <max-src-nodes/>
1481        <max-src-conn/>
1482        <max-src-states/>
1483        <statetimeout/>
1484        <statetype>keep state</statetype>
1485        <os/>
1486        <source>
1487          <any/>
1488        </source>
1489        <destination>
1490          <any/>
1491        </destination>
1492        <descr/>
1493      </rule>
1494      <rule>
1495        <id/>
1496        <type>pass</type>
1497        <interface>opt9</interface>
1498        <tag/>
1499        <tagged/>
```

```
1500        <max/>
1501        <max-src-nodes/>
1502        <max-src-conn/>
1503        <max-src-states/>
1504        <statetimeout/>
1505        <statetype>keep state</statetype>
1506        <os/>
1507        <source>
1508          <any/>
1509        </source>
1510        <destination>
1511          <any/>
1512        </destination>
1513        <descr/>
1514        <dnpipe>1</dnpipe>
1515        <pdnpipe>2</pdnpipe>
1516      </rule>
1517      <rule>
1518        <id/>
1519        <type>pass</type>
1520        <interface>opt9</interface>
1521        <tag/>
1522        <tagged/>
1523        <max/>
1524        <max-src-nodes/>
1525        <max-src-conn/>
1526        <max-src-states/>
1527        <statetimeout/>
1528        <statetype>keep state</statetype>
1529        <os/>
1530        <protocol>tcp/udp</protocol>
1531        <source>
1532          <any/>
1533        </source>
1534        <destination>
1535          <any/>
1536          <port>3050</port>
1537        </destination>
1538        <descr/>
1539      </rule>
1540      <rule>
1541        <id/>
1542        <type>pass</type>
1543        <interface>opt10</interface>
1544        <tag/>
1545        <tagged/>
1546        <max/>
```

```
1547        <max-src-nodes/>
1548        <max-src-conn/>
1549        <max-src-states/>
1550        <statetimeout/>
1551        <statetype>keep state</statetype>
1552        <os/>
1553        <source>
1554          <any/>
1555        </source>
1556        <destination>
1557          <any/>
1558        </destination>
1559        <descr/>
1560        <dnpipe>1</dnpipe>
1561        <pdnpipe>2</pdnpipe>
1562      </rule>
1563      <rule>
1564        <id/>
1565        <type>pass</type>
1566        <interface>opt11</interface>
1567        <tag/>
1568        <tagged/>
1569        <max/>
1570        <max-src-nodes/>
1571        <max-src-conn/>
1572        <max-src-states/>
1573        <statetimeout/>
1574        <statetype>keep state</statetype>
1575        <os/>
1576        <source>
1577          <any/>
1578        </source>
1579        <destination>
1580          <any/>
1581        </destination>
1582        <descr/>
1583      </rule>
1584      <rule>
1585        <id/>
1586        <type>pass</type>
1587        <interface>opt12</interface>
1588        <tag/>
1589        <tagged/>
1590        <max/>
1591        <max-src-nodes/>
1592        <max-src-conn/>
1593        <max-src-states/>
```

```
1594        <statetimeout/>
1595        <statetype>keep state</statetype>
1596        <os/>
1597        <source>
1598          <any/>
1599        </source>
1600        <destination>
1601          <any/>
1602        </destination>
1603        <descr/>
1604        <dnpipe>1</dnpipe>
1605        <pdnpipe>2</pdnpipe>
1606      </rule>
1607      <rule>
1608        <id/>
1609        <type>pass</type>
1610        <interface>opt13</interface>
1611        <tag/>
1612        <tagged/>
1613        <max/>
1614        <max-src-nodes/>
1615        <max-src-conn/>
1616        <max-src-states/>
1617        <statetimeout/>
1618        <statetype>keep state</statetype>
1619        <os/>
1620        <source>
1621          <any/>
1622        </source>
1623        <destination>
1624          <any/>
1625        </destination>
1626        <descr><![CDATA[Open cisco]]></descr>
1627      </rule>
1628    </filter>
1629    <shaper/>
1630    <ipsec>
1631      <preferoldsa/>
1632    </ipsec>
1633    <aliases/>
1634    <proxyarp/>
1635    <cron>
1636      <item>
1637        <minute>0</minute>
1638        <hour>*</hour>
1639        <mday>*</mday>
1640        <month>*</month>
```

```
1641        <wday>*</wday>
1642        <who>root</who>
1643        <command>/usr/bin/nice -n20 newsyslog</command>
1644      </item>
1645      <item>
1646        <minute>1,31</minute>
1647        <hour>0-5</hour>
1648        <mday>*</mday>
1649        <month>*</month>
1650        <wday>*</wday>
1651        <who>root</who>
1652        <command>/usr/bin/nice -n20 adjkerntz -a</command>
1653      </item>
1654      <item>
1655        <minute>1</minute>
1656        <hour>3</hour>
1657        <mday>1</mday>
1658        <month>*</month>
1659        <wday>*</wday>
1660        <who>root</who>
1661        <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command↩
               >
1662      </item>
1663      <item>
1664        <minute>*/60</minute>
1665        <hour>*</hour>
1666        <mday>*</mday>
1667        <month>*</month>
1668        <wday>*</wday>
1669        <who>root</who>
1670        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t↩
               3600 sshlockout</command>
1671      </item>
1672      <item>
1673        <minute>1</minute>
1674        <hour>1</hour>
1675        <mday>*</mday>
1676        <month>*</month>
1677        <wday>*</wday>
1678        <who>root</who>
1679        <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
1680      </item>
1681      <item>
1682        <minute>*/60</minute>
1683        <hour>*</hour>
1684        <mday>*</mday>
1685        <month>*</month>
```

```
1686        <wday>*</wday>
1687        <who>root</who>
1688        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t↩
                3600 virusprot</command>
1689      </item>
1690      <item>
1691        <minute>30</minute>
1692        <hour>12</hour>
1693        <mday>*</mday>
1694        <month>*</month>
1695        <wday>*</wday>
1696        <who>root</who>
1697        <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command↩
              >
1698      </item>
1699      <item>
1700        <task_name>squid_rotate_logs</task_name>
1701        <minute>0</minute>
1702        <hour>0</hour>
1703        <mday>*</mday>
1704        <month>*</month>
1705        <wday>*</wday>
1706        <who>root</who>
1707        <command>/bin/rm /var/squid/cache/swap.state; /usr/local/sbin↩
              /squid -k rotate</command>
1708      </item>
1709      <item>
1710        <task_name>squid_check_swapstate</task_name>
1711        <minute>*/15</minute>
1712        <hour>*</hour>
1713        <mday>*</mday>
1714        <month>*</month>
1715        <wday>*</wday>
1716        <who>root</who>
1717        <command>/usr/local/pkg/swapstate_check.php</command>
1718      </item>
1719    </cron>
1720    <wol>
1721      <wolentry>
1722        <interface>opt12</interface>
1723        <mac>00:12:17:7b:2f:3a</mac>
1724        <descr/>
1725      </wolentry>
1726      <wolentry>
1727        <interface>opt5</interface>
1728        <mac>00:10:b5:72:8d:54</mac>
1729        <descr><![CDATA[Pfsense_UDC]]></descr>
```

```
1730      </wolentry>
1731      <wolentry>
1732        <interface>opt5</interface>
1733        <mac>00:14:22:27:26:6a</mac>
1734        <descr><![CDATA[admon_ds009]]></descr>
1735      </wolentry>
1736      <wolentry>
1737        <interface>opt8</interface>
1738        <mac>64:66:b3:5d:46:1a</mac>
1739        <descr><![CDATA[ap_caseta2]]></descr>
1740      </wolentry>
1741      <wolentry>
1742        <interface>opt1</interface>
1743        <mac>68:7f:74:12:0c:1c</mac>
1744        <descr><![CDATA[ap_presup]]></descr>
1745      </wolentry>
1746    </wol>
1747    <rrd>
1748      <enable/>
1749    </rrd>
1750    <load_balancer>
1751      <monitor_type>
1752        <name>ICMP</name>
1753        <type>icmp</type>
1754        <descr><![CDATA[ICMP]]></descr>
1755        <options/>
1756      </monitor_type>
1757      <monitor_type>
1758        <name>TCP</name>
1759        <type>tcp</type>
1760        <descr><![CDATA[Generic TCP]]></descr>
1761        <options/>
1762      </monitor_type>
1763      <monitor_type>
1764        <name>HTTP</name>
1765        <type>http</type>
1766        <descr><![CDATA[Generic HTTP]]></descr>
1767        <options>
1768          <path>/</path>
1769          <host/>
1770          <code>200</code>
1771        </options>
1772      </monitor_type>
1773      <monitor_type>
1774        <name>HTTPS</name>
1775        <type>https</type>
1776        <descr><![CDATA[Generic HTTPS]]></descr>
```

```
1777        <options>
1778          <path>/</path>
1779          <host/>
1780          <code>200</code>
1781        </options>
1782      </monitor_type>
1783      <monitor_type>
1784        <name>SMTP</name>
1785        <type>send</type>
1786        <descr><![CDATA[Generic SMTP]]></descr>
1787        <options>
1788          <send>EHLO nosuchhost</send>
1789          <expect>250-</expect>
1790        </options>
1791      </monitor_type>
1792    </load_balancer>
1793    <widgets>
1794      <sequence>gateways-container:col1:show,system_information-↩
           container:col1:show,captive_portal_status-↩
           container:col1:close,carp_status-container:col1:close,↩
           cpu_graphs-container:col1:close,gmirror_status-↩
           container:col1:close,installed_packages-container:col1:close↩
           ,interface_statistics-container:col1:close,picture-↩
           container:col2:show,interfaces-container:col2:show,ipsec-↩
           container:col2:close,load_balancer_status-↩
           container:col2:close,log-container:col2:close,rss-↩
           container:col2:close,services_status-container:col2:close,↩
           traffic_graphs-container:col2:close,openvpn-↩
           container:col2:none,wake_on_lan-container:col2:none</↩
           sequence>
1795
1796      <picturewidget_filename>anim-daemon2.gif</↩
           picturewidget_filename>
1797    </widgets>
1798    <revision>
1799      <time>1381165008</time>
1800      <description><![CDATA[admin@10.1.4.233: /services_dhcp.php made↩
            unknown change]]></description>
1801      <username>admin@10.1.4.233</username>
1802    </revision>
1803    <openvpn/>
1804    <l7shaper>
1805      <container/>
1806    </l7shaper>
1807    <dnshaper>
1808      <queue>
1809        <name>2MbS</name>
```

```
1810        <number/>
1811        <qlimit/>
1812        <plr/>
1813        <description><![CDATA[Para Evento LB]]></description>
1814        <bandwidth>2</bandwidth>
1815        <bandwidthtype>Mb</bandwidthtype>
1816        <enabled>on</enabled>
1817        <buckets/>
1818        <mask>srcaddress</mask>
1819        <delay>0</delay>
1820      </queue>
1821      <queue>
1822        <name>2MBD</name>
1823        <number/>
1824        <qlimit/>
1825        <plr/>
1826        <description/>
1827        <bandwidth>2</bandwidth>
1828        <bandwidthtype>Mb</bandwidthtype>
1829        <enabled>on</enabled>
1830        <buckets/>
1831        <mask>dstaddress</mask>
1832        <delay>0</delay>
1833      </queue>
1834    </dnshaper>
1835    <cert>
1836      <refid>4fe4a0973902d</refid>
1837      <descr><![CDATA[webConfigurator default]]></descr>
1838
1839    <ppps/>
1840    <gateways>
1841      <gateway_item>
1842        <interface>wan</interface>
1843        <gateway>10.1.10.253</gateway>
1844        <name>WANGW</name>
1845        <weight>1</weight>
1846        <descr><![CDATA[WAN Gateway]]></descr>
1847        <defaultgw/>
1848      </gateway_item>
1849      <gateway_item>
1850        <interface>opt3</interface>
1851        <gateway>10.1.2.254</gateway>
1852        <name>102gw</name>
1853        <weight>1</weight>
1854        <interval/>
1855        <descr/>
1856      </gateway_item>
```

```
1857      <gateway_item>
1858        <interface>opt4</interface>
1859        <gateway>10.1.3.254</gateway>
1860        <name>103gw</name>
1861        <weight>1</weight>
1862        <interval/>
1863        <descr/>
1864      </gateway_item>
1865      <gateway_item>
1866        <interface>opt5</interface>
1867        <gateway>10.1.4.254</gateway>
1868        <name>104gw</name>
1869        <weight>1</weight>
1870        <interval/>
1871        <descr/>
1872      </gateway_item>
1873      <gateway_item>
1874        <interface>opt6</interface>
1875        <gateway>10.1.5.254</gateway>
1876        <name>105gw</name>
1877        <weight>1</weight>
1878        <interval/>
1879        <descr/>
1880      </gateway_item>
1881      <gateway_item>
1882        <interface>opt7</interface>
1883        <gateway>10.1.7.254</gateway>
1884        <name>107gw</name>
1885        <weight>1</weight>
1886        <interval/>
1887        <descr/>
1888      </gateway_item>
1889      <gateway_item>
1890        <interface>opt8</interface>
1891        <gateway>10.1.8.254</gateway>
1892        <name>108gw</name>
1893        <weight>1</weight>
1894        <interval/>
1895        <descr/>
1896      </gateway_item>
1897      <gateway_item>
1898        <interface>opt9</interface>
1899        <gateway>10.1.9.254</gateway>
1900        <name>109gw</name>
1901        <weight>1</weight>
1902        <interval/>
1903        <descr/>
```

```
1904      </gateway_item>
1905      <gateway_item>
1906        <interface>opt10</interface>
1907        <gateway>10.1.10.254</gateway>
1908        <name>110gw</name>
1909        <weight>1</weight>
1910        <interval/>
1911        <descr/>
1912      </gateway_item>
1913      <gateway_item>
1914        <interface>opt1</interface>
1915        <gateway>10.1.118.254</gateway>
1916        <name>118gw</name>
1917        <weight>1</weight>
1918        <interval/>
1919        <descr/>
1920      </gateway_item>
1921      <gateway_item>
1922        <interface>opt2</interface>
1923        <gateway>10.1.251.14</gateway>
1924        <name>admin</name>
1925        <weight>1</weight>
1926        <interval/>
1927        <descr/>
1928      </gateway_item>
1929      <gateway_item>
1930        <interface>opt11</interface>
1931        <gateway>10.1.1.254</gateway>
1932        <name>gwCAM</name>
1933        <weight>1</weight>
1934        <interval/>
1935        <descr/>
1936      </gateway_item>
1937      <gateway_item>
1938        <interface>opt12</interface>
1939        <gateway>10.1.9.254</gateway>
1940        <name>gwifi</name>
1941        <weight>1</weight>
1942        <interval/>
1943        <descr/>
1944      </gateway_item>
1945      <gateway_item>
1946        <interface>opt13</interface>
1947        <gateway>10.1.23.254</gateway>
1948        <name>cisco</name>
1949        <weight>1</weight>
1950        <interval/>
```

```
1951        <descr><![CDATA[lab cisco]]></descr>
1952      </gateway_item>
1953    </gateways>
1954    <vlans>
1955      <vlan>
1956        <if>bce3</if>
1957        <tag>102</tag>
1958        <descr><![CDATA[A-PB]]></descr>
1959        <vlanif>bce3_vlan102</vlanif>
1960      </vlan>
1961      <vlan>
1962        <if>bce3</if>
1963        <tag>103</tag>
1964        <descr><![CDATA[A-PP,SP]]></descr>
1965        <vlanif>bce3_vlan103</vlanif>
1966      </vlan>
1967      <vlan>
1968        <if>bce3</if>
1969        <tag>104</tag>
1970        <descr><![CDATA[B-PB]]></descr>
1971        <vlanif>bce3_vlan104</vlanif>
1972      </vlan>
1973      <vlan>
1974        <if>bce3</if>
1975        <tag>105</tag>
1976        <descr><![CDATA[B-PP,SP]]></descr>
1977        <vlanif>bce3_vlan105</vlanif>
1978      </vlan>
1979      <vlan>
1980        <if>bce3</if>
1981        <tag>107</tag>
1982        <descr><![CDATA[C-PB,PP,SP]]></descr>
1983        <vlanif>bce3_vlan107</vlanif>
1984      </vlan>
1985      <vlan>
1986        <if>bce3</if>
1987        <tag>108</tag>
1988        <descr><![CDATA[D-PB,PP,SP]]></descr>
1989        <vlanif>bce3_vlan108</vlanif>
1990      </vlan>
1991      <vlan>
1992        <if>bce3</if>
1993        <tag>109</tag>
1994        <descr><![CDATA[JB-PB]]></descr>
1995        <vlanif>bce3_vlan109</vlanif>
1996      </vlan>
1997      <vlan>
```

```
1998        <if>bce3</if>
1999        <tag>110</tag>
2000        <descr><![CDATA[COLECCIONES]]></descr>
2001        <vlanif>bce3_vlan110</vlanif>
2002      </vlan>
2003      <vlan>
2004        <if>bce3</if>
2005        <tag>118</tag>
2006        <descr><![CDATA[wifi]]></descr>
2007        <vlanif>bce3_vlan118</vlanif>
2008      </vlan>
2009      <vlan>
2010        <if>bce3</if>
2011        <tag>399</tag>
2012        <descr><![CDATA[VlanAdmin]]></descr>
2013        <vlanif>bce3_vlan399</vlanif>
2014      </vlan>
2015      <vlan>
2016        <if>bce3</if>
2017        <tag>500</tag>
2018        <descr><![CDATA[C]]></descr>
2019        <vlanif>bce3_vlan500</vlanif>
2020      </vlan>
2021      <vlan>
2022        <if>bce3</if>
2023        <tag>66</tag>
2024        <descr><![CDATA[WIFI]]></descr>
2025        <vlanif>bce3_vlan66</vlanif>
2026      </vlan>
2027      <vlan>
2028        <if>bce3</if>
2029        <tag>23</tag>
2030        <descr><![CDATA[Laboratorio Cisco]]></descr>
2031        <vlanif>bce3_vlan23</vlanif>
2032      </vlan>
2033    </vlans>
2034    <installedpackages>
2035      <menu>
2036        <name>NMap</name>
2037        <tooltiptext>NMap is a utility for network exploration or ↩
              security auditing. It supports ping scanning (determine ↩
              which hosts are up), many port scanning techniques (↩
              determine what services the hosts are offering), version ↩
              detection (determine what application/service is runing on↩
               a port), and TCP/IP fingerprinting (remote host OS or ↩
              device identification). It also offers flexible target and↩
               port specification, decoy/stealth scanning, SunRPC ↩
```

```
        scanning, and more. Most Unix and Windows platforms are ↩
        supported in both GUI and command line modes. Several ↩
        popular handheld devices are also supported, including the↩
         Sharp Zaurus and the iPAQ.</tooltiptext>
2038      <section>Diagnostics</section>
2039      <configfile>nmap.xml</configfile>
2040    </menu>
2041    <menu>
2042      <name>phpsysinfo</name>
2043      <tooltiptext/>
2044      <section>Status</section>
2045      <url>/pkg_edit.php?xml=phpsysinfo.xml&amp;id=0</url>
2046    </menu>
2047    <menu>
2048      <name>BandwidthD</name>
2049      <tooltiptext/>
2050      <section>Services</section>
2051      <url>/pkg_edit.php?xml=bandwidthd.xml&amp;id=0</url>
2052    </menu>
2053    <menu>
2054      <name>TFTP</name>
2055      <tooltiptext>Add or Remove files for TFTP.</tooltiptext>
2056      <section>Services</section>
2057      <configfile>tftp.xml</configfile>
2058      <url>tftp_files.php</url>
2059    </menu>
2060    <menu>
2061      <name>Proxy server</name>
2062      <tooltiptext>Modify the proxy servers settings</tooltiptext>
2063      <section>Services</section>
2064      <url>/pkg_edit.php?xml=squid.xml&amp;id=0</url>
2065    </menu>
2066    <menu>
2067      <name>Dansguardian</name>
2068      <tooltiptext>Configure dansguardian</tooltiptext>
2069      <section>Services</section>
2070      <url>/pkg_edit.php?xml=dansguardian.xml</url>
2071    </menu>
2072    <service/>
2073    <service>
2074      <name>bandwidthd</name>
2075      <rcfile>bandwidthd.sh</rcfile>
2076      <executable>bandwidthd</executable>
2077    </service>
2078    <service>
2079      <name>tftp</name>
2080      <executable>inetd</executable>
```

```
2081        <description><![CDATA[Trivial File Transport Protocol is a very simple file transfer protocol. Often used with routers, voip phones and more.]]></description>
2082      </service>
2083      <service>
2084        <name>squid</name>
2085        <rcfile>squid.sh</rcfile>
2086        <executable>squid</executable>
2087        <description><![CDATA[Proxy server Service]]></description>
2088      </service>
2089      <service>
2090        <name>dansguardian</name>
2091        <rcfile>dansguardian</rcfile>
2092        <executable>dansguardian</executable>
2093        <description><![CDATA[Award winning Open Source web content filter]]></description>
2094      </service>
2095      <package>
2096        <name>nmap</name>
2097        <maintainer>jimp@pfsense.org</maintainer>
2098        <descr><![CDATA[NMap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques (determine what services the hosts are offering), version detection (determine what application/service is runing on a port), and TCP/IP fingerprinting (remote host OS or device identification). It also offers flexible target and port specification, decoy/stealth scanning, SunRPC scanning, and more. Most Unix and Windows platforms are supported in both GUI and command line modes. Several popular handheld devices are also supported, including the Sharp Zaurus and the iPAQ.]]></descr>
2099        <category>Security</category>
2100        <depends_on_package_base_url>http://files.pfsense.org/packages/amd64/8/All/</depends_on_package_base_url>
2101        <depends_on_package>lua-5.1.5_4.tbz</depends_on_package>
2102        <depends_on_package>nmap-6.01.tbz</depends_on_package>
2103        <depends_on_package>libpcap-1.2.1.tbz</depends_on_package>
2104        <depends_on_package_pbi>nmap-6.01_1-amd64.pbi</depends_on_package_pbi>
2105        <config_file>http://www.pfsense.com/packages/config/nmap/nmap.xml</config_file>
2106        <version>nmap-6.01 pkg v1.2</version>
2107        <status>Stable</status>
2108        <pkginfolink>http://doc.pfsense.org/index.php/Nmap_package</pkginfolink>
2109        <required_version>2.0</required_version>
```

```
2110        <configurationfile>nmap.xml</configurationfile>
2111        <build_port_path>/usr/ports/security/nmap</build_port_path>
2112      </package>
2113      <package>
2114        <name>phpSysInfo</name>
2115        <website>http://phpsysinfo.sourceforge.net/</website>
2116        <descr><![CDATA[PHPSysInfo is a customizable PHP Script that ↩
              parses /proc, and formats information nicely. It will ↩
              display information about system facts like Uptime, CPU, ↩
              Memory, PCI devices, SCSI devices, IDE devices, Network ↩
              adapters, Disk usage, and more.]]></descr>
2117        <category>System</category>
2118        <version>2.5.4</version>
2119        <status>Beta</status>
2120        <required_version>1.0</required_version>
2121        <depends_on_package_base_url>http://files.pfsense.org/↩
              packages/amd64/8/All/</depends_on_package_base_url>
2122        <depends_on_package>mbmon-205_5.tbz</depends_on_package>
2123        <depends_on_package_pbi>mbmon-205_6-amd64.pbi</↩
              depends_on_package_pbi>
2124        <build_port_path>/usr/ports/sysutils/mbmon</build_port_path>
2125        <config_file>http://www.pfsense.com/packages/config/↩
              phpsysinfo/phpsysinfo.xml</config_file>
2126        <configurationfile>phpsysinfo.xml</configurationfile>
2127        <noembedded>true</noembedded>
2128      </package>
2129      <package>
2130        <name>bandwidthd</name>
2131        <website>http://bandwidthd.sourceforge.net/</website>
2132        <descr><![CDATA[BandwidthD tracks usage of TCP/IP network ↩
              subnets and builds html files with graphs to display ↩
              utilization. Charts are built by individual IPs, and by ↩
              default display utilization over 2 day, 8 day, 40 day, and↩
               400 day periods. Furthermore, each ip address utilization↩
               can be logged out at intervals of 3.3 minutes, 10 minutes↩
              , 1 hour or 12 hours in cdf format, or to a backend ↩
              database server. HTTP, TCP, UDP, ICMP, VPN, and P2P ↩
              traffic are color coded.]]></descr>
2133        <category>System</category>
2134        <version>2.0.1_5</version>
2135        <status>BETA</status>
2136        <required_version>1.2.1</required_version>
2137        <depends_on_package_base_url>http://files.pfsense.org/↩
              packages/amd64/8/All/</depends_on_package_base_url>
2138        <depends_on_package>bandwidthd-2.0.1_5.tbz</↩
              depends_on_package>
2139        <depends_on_package>libpcap-1.1.1.tbz</depends_on_package>
```

```
2140        <depends_on_package>postgresql-client-8.4.12.tbz</↩
                depends_on_package>
2141        <depends_on_package_pbi>bandwidthd-2.0.1_5-amd64.pbi</↩
                depends_on_package_pbi>
2142        <config_file>http://www.pfsense.org/packages/config/↩
                bandwidthd/bandwidthd.xml</config_file>
2143        <configurationfile>bandwidthd.xml</configurationfile>
2144        <build_port_path>/usr/ports/net/libpcap</build_port_path>
2145        <build_port_path>/usr/ports/databases/postgresql84-client</↩
                build_port_path>
2146        <build_port_path>/usr/ports/net-mgmt/bandwidthd</↩
                build_port_path>
2147        <build_pbi>
2148          <ports_before>net/libpcap databases/postgresql91-client ↩
                graphics/gd</ports_before>
2149          <port>net-mgmt/bandwidthd</port>
2150        </build_pbi>
2151        <build_options>WITH_NLS=true;WITHOUT_PAM=true;WITHOUT_LDAP=↩
              true;WITHOUT_MIT_KRB5=true;WITHOUT_HEIMDAL_KRB5=true;↩
              WITHOUT_OPTIMIZED_CFLAGS=true;WITHOUT_XML=true;↩
              WITHOUT_TZDATA=true;WITHOUT_DEBUG=true;WITHOUT_GSSAPI=true↩
              ;WITHOUT_ICU=true;WITH_INTDATE=true</build_options>
2152      </package>
2153      <package>
2154        <name>TFTP</name>
2155        <website/>
2156        <descr><![CDATA[Trivial File Transport Protocol is a very ↩
              simple file transfer protocol. Often used with routers, ↩
              voip phones and more.]]></descr>
2157        <category>Services</category>
2158        <pkginfolink/>
2159        <config_file>http://www.pfsense.com/packages/config/tftp2/↩
              tftp.xml</config_file>
2160        <depends_on_package_base_url>http://files.pfsense.org/↩
              packages/amd64/8/All/</depends_on_package_base_url>
2161        <version>2.0</version>
2162        <status>Stable</status>
2163        <required_version>2.0</required_version>
2164        <configurationfile>tftp.xml</configurationfile>
2165        <filter_rule_function>tftp_generate_rules</↩
              filter_rule_function>
2166      </package>
2167      <package>
2168        <name>squid</name>
2169        <descr><![CDATA[High performance web proxy cache.]]></descr>
2170        <website>http://www.squid-cache.org/</website>
2171        <category>Network</category>
```

```
2172        <version>2.7.9 pkg v.4.3.3</version>
2173        <status>Stable</status>
2174        <required_version>2</required_version>
2175        <maintainer>fernando@netfilter.com.br seth.mos@dds.nl ↩
               mfuchs77@googlemail.com jimp@pfsense.org</maintainer>
2176        <depends_on_package_base_url>http://files.pfsense.org/↩
               packages/amd64/8/All/</depends_on_package_base_url>
2177        <depends_on_package>squid-2.7.9_3.tbz</depends_on_package>
2178        <depends_on_package>squid_radius_auth-1.10.tbz</↩
               depends_on_package>
2179        <depends_on_package>libwww-5.4.0_4.tbz</depends_on_package>
2180        <depends_on_package_pbi>squid-2.7.9_3-amd64.pbi</↩
               depends_on_package_pbi>
2181        <build_port_path>/usr/ports/www/squid</build_port_path>
2182        <build_port_path>/usr/ports/www/squid_radius_auth</↩
               build_port_path>
2183        <build_port_path>/usr/ports/www/libwww</build_port_path>
2184        <build_pbi>
2185          <ports_before>www/libwww</ports_before>
2186          <port>www/squid</port>
2187          <ports_after>www/squid_radius_auth</ports_after>
2188        </build_pbi>
2189        <build_options>squid_UNSET=DNS_HELPER IPFILTER PINGER ↩
               STACKTRACES STRICT_HTTP_DESC USERAGENT_LOG WCCPV2;↩
               squid_SET=PF LDAP_AUTH NIS_AUTH SASL_AUTH ARP_ACL AUFS ↩
               CACHE_DIGESTS CARP COSS DELAY_POOLS FOLLOW_XFF HTCP IDENT ↩
               KERB_AUTH KQUEUE LARGEFILE REFERER_LOG SNMP SSL VIA_DB ↩
               WCCP;SQUID_UID=proxy;SQUID_GID=proxy</build_options>
2190        <config_file>http://www.pfsense.org/packages/config/squid/↩
               squid.xml</config_file>
2191        <configurationfile>squid.xml</configurationfile>
2192      </package>
2193      <package>
2194        <name>Dansguardian</name>
2195        <website>http://www.dansguardian.org/</website>
2196        <descr><![CDATA[DansGuardian is an award winning Open Source ↩
               web content filter.&lt;br /&gt;
2197             It filters the actual content of pages based on many ↩
                    methods including phrase matching, PICS filtering ↩
                    and URL filtering.&lt;br /&gt;
2198             It does not purely filter based on a banned list of ↩
                    sites like lesser totally commercial filters.&lt;br ↩
                    /&gt;
2199             For all non-commercial its free, without cost.&lt;br /&↩
                    gt;
2200             For all commercial use visit dansguardian website to ↩
                    get a licence.]]></descr>
```

```
2201        <category>Services</category>
2202        <config_file>http://www.pfsense.com/packages/config/↩
                dansguardian/dansguardian.xml</config_file>
2203        <pkginfolink>http://forum.pfsense.org/index.php/topic↩
                ,43786.0.html</pkginfolink>
2204        <depends_on_package_base_url>http://files.pfsense.org/↩
                packages/amd64/8/All/</depends_on_package_base_url>
2205        <depends_on_package>dansguardian-2.12.0.3.tbz</↩
                depends_on_package>
2206        <depends_on_package>ca_root_nss-3.14.1.tbz</↩
                depends_on_package>
2207        <depends_on_package_pbi>dansguardian-2.12.0.3-amd64.pbi</↩
                depends_on_package_pbi>
2208        <version>2.12.0.3 pkg v.0.1.8</version>
2209        <status>beta</status>
2210        <required_version>2.0</required_version>
2211        <configurationfile>dansguardian.xml</configurationfile>
2212        <build_port_path>/usr/ports/www/dansguardian-devel</↩
                build_port_path>
2213        <build_port_path>/usr/ports/www/ca_root_nss</build_port_path>
2214        <build_options>dansguardian-devel_UNSET=APACHE;dansguardian-↩
                devel_SET=TRICKLE CLAMD ICAP NTLM SSL</build_options>
2215      </package>
2216      <phpsysinfo>
2217        <config>
2218          <hidepicklist/>
2219          <sensorprogram/>
2220          <showmountpoint>on</showmountpoint>
2221          <showinodes>on</showinodes>
2222          <loadbar>on</loadbar>
2223          <showerrors/>
2224        </config>
2225      </phpsysinfo>
2226      <bandwidthd>
2227        <config>
2228          <enable>on</enable>
2229          <active_interface>wan</active_interface>
2230          <subnets_custom>10.1.0.0/16</subnets_custom>
2231          <skipintervals/>
2232          <graphcutoff/>
2233          <promiscuous>on</promiscuous>
2234          <outputcdf/>
2235          <recovercdf>on</recovercdf>
2236          <filter/>
2237          <drawgraphs>on</drawgraphs>
2238          <meta_refresh/>
2239          <graph_log_info/>
```

```
2240        </config>
2241      </bandwidthd>
2242      <tab>
2243        <text>General</text>
2244        <url>/pkg_edit.php?xml=squid.xml&amp;id=0</url>
2245        <active/>
2246      </tab>
2247      <dansguardian>
2248        <config>
2249          <interface>lo0</interface>
2250          <daemon_options>softrestart</daemon_options>
2251        </config>
2252      </dansguardian>
2253      <dansguardianconfig>
2254        <config>
2255          <auth_plugin/>
2256          <scan_options>scancleancache,createlistcachefiles,↩
                deletedownloadedtempfiles</scan_options>
2257          <weightedphrasemode>2</weightedphrasemode>
2258          <preservecase>0</preservecase>
2259          <phrasefiltermode>2</phrasefiltermode>
2260          <cron>day</cron>
2261        </config>
2262      </dansguardianconfig>
2263      <dansguardianlog>
2264        <config>
2265          <report_level>3</report_level>
2266          <report_language>ukenglish</report_language>
2267          <report_options>showweightedfound,usecustombannedimage,↩
                nonstandarddelimiter</report_options>
2268          <logging_options>logconnectionhandlingerrors</↩
                logging_options>
2269          <loglevel>2</loglevel>
2270          <logexceptionhits>2</logexceptionhits>
2271          <logfileformat>1</logfileformat>
2272        </config>
2273      </dansguardianlog>
2274      <dansguardianphraseacl>
2275        <config>
2276          <name>Default</name>
2277          <description><![CDATA[Default Phrase access list setup]]></↩
                description>
2278          <banned_enabled>on</banned_enabled>
2279          <weighted_enabled>on</weighted_enabled>
2280          <exception_enabled>on</exception_enabled>
2281              </dansguardianphraseacl>
2282      <dansguardiansiteacl>
```

```
2283        <config>
2284          <name>Default</name>
2285          <description><![CDATA[Default Site access list setup]]></↩
                description>
2286          <exceptionsite_enabled>on</exceptionsite_enabled>
2287          <bannedsite_enabled>on</bannedsite_enabled>
2288          <greysite_enabled>on</greysite_enabled>
2289        </config>
2290      </dansguardiansiteacl>
2291      <dansguardianurlacl>
2292        <config>
2293          <name>Default</name>
2294          <description><![CDATA[Default Url access list setup]]></↩
                description>
2295          <bannedurl_enabled>on</bannedurl_enabled>
2296          <exceptionurl_enabled>on</exceptionurl_enabled>
2297          <contenturl_enabled>on</contenturl_enabled>
2298          <greyurl_enabled>on</greyurl_enabled>
2299              </config>
2300      </dansguardianurlacl>
2301      <dansguardianpicsacl>
2302        <config>
2303          <name>Default</name>
2304          <description><![CDATA[Default file access list setup]]></↩
                description>
2305
2306      </dansguardianpicsacl>
2307      <dansguardiansearchacl>
2308        <config>
2309          <name>Default</name>
2310          <description><![CDATA[Default search engine list setup]]></↩
                description>
2311          <searchengineregexplist/>
2312          <banned_searchtermlist/>
2313          <weighted_searchtermlist/>
2314          <exception_searchtermlist/>
2315        </config>
2316      </dansguardiansearchacl>
2317      <dansguardianfileacl>
2318        <config>
2319          <name>Default</name>
2320          <description><![CDATA[Default file access list setup]]></↩
                description>
2321          <exception_enabled>on</exception_enabled>
2322          <banned_enabled>on</banned_enabled>
2323              </config>
2324      </dansguardianheaderacl>
```

```
2325      <dansguardiancontentacl>
2326        <config>
2327          <name>Default</name>
2328          <description><![CDATA[Default content setup]]></description↩
                >
2329      <dansguardiangroups>
2330        <config>
2331          <name>Default</name>
2332          <description><![CDATA[Default dansguardian filtergroup]]></↩
                description>
2333          <picsacl>Default</picsacl>
2334          <phraseacl>Default</phraseacl>
2335          <siteacl>Default</siteacl>
2336          <extensionacl>Default</extensionacl>
2337          <headeracl>Default</headeracl>
2338          <contentacl>Default</contentacl>
2339          <searchacl>Default</searchacl>
2340          <urlacl>Default</urlacl>
2341          <group_options>scancleancache,infectionbypasserrorsonly</↩
                group_options>
2342          <reportinglevel>3</reportinglevel>
2343          <group_name_source>name</group_name_source>
2344          <mode>1</mode>
2345          <report_level>global</report_level>
2346        </config>
2347      </dansguardiangroups>
2348      <dansguardianphraselistsweighted>
2349        <config>
2350          <descr><![CDATA[badwords weighted_dutch]]></descr>
2351          <list>badwords</list>
2352          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                badwords/weighted_dutch</file>
2353        </config>
2354        <config>
2355          <descr><![CDATA[badwords weighted_french]]></descr>
2356          <list>badwords</list>
2357          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                badwords/weighted_french</file>
2358        </config>
2359        <config>
2360          <descr><![CDATA[badwords weighted_german]]></descr>
2361          <list>badwords</list>
2362          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                badwords/weighted_german</file>
2363        </config>
2364        <config>
2365          <descr><![CDATA[badwords weighted_portuguese]]></descr>
```

```
2366          <list>badwords</list>
2367          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  badwords/weighted_portuguese</file>
2368        </config>
2369        <config>
2370          <descr><![CDATA[badwords weighted_spanish]]></descr>
2371          <list>badwords</list>
2372          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  badwords/weighted_spanish</file>
2373        </config>
2374        <config>
2375          <descr><![CDATA[chat weighted]]></descr>
2376          <list>chat</list>
2377          <file>/usr/local/etc/dansguardian/lists/phraselists/chat/↩
                  weighted</file>
2378        </config>
2379        <config>
2380          <descr><![CDATA[chat weighted_italian]]></descr>
2381          <list>chat</list>
2382          <file>/usr/local/etc/dansguardian/lists/phraselists/chat/↩
                  weighted_italian</file>
2383        </config>
2384        <config>
2385          <descr><![CDATA[conspiracy weighted]]></descr>
2386          <list>conspiracy</list>
2387          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  conspiracy/weighted</file>
2388        </config>
2389        <config>
2390          <descr><![CDATA[domainsforsale weighted]]></descr>
2391          <list>domainsforsale</list>
2392          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  domainsforsale/weighted</file>
2393        </config>
2394        <config>
2395          <descr><![CDATA[drugadvocacy weighted]]></descr>
2396          <list>drugadvocacy</list>
2397          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  drugadvocacy/weighted</file>
2398        </config>
2399        <config>
2400          <descr><![CDATA[forums weighted]]></descr>
2401          <list>forums</list>
2402          <file>/usr/local/etc/dansguardian/lists/phraselists/forums/↩
                  weighted</file>
2403        </config>
2404        <config>
```

```
2405          <descr><![CDATA[gambling weighted]]></descr>
2406          <list>gambling</list>
2407          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  gambling/weighted</file>
2408        </config>
2409        <config>
2410          <descr><![CDATA[gambling weighted_portuguese]]></descr>
2411          <list>gambling</list>
2412          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  gambling/weighted_portuguese</file>
2413        </config>
2414        <config>
2415          <descr><![CDATA[games weighted]]></descr>
2416          <list>games</list>
2417          <file>/usr/local/etc/dansguardian/lists/phraselists/games/↩
                  weighted</file>
2418        </config>
2419        <config>
2420          <descr><![CDATA[goodphrases weighted_general]]></descr>
2421          <list>goodphrases</list>
2422          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  goodphrases/weighted_general</file>
2423        </config>
2424        <config>
2425          <descr><![CDATA[goodphrases weighted_general_danish]]></↩
                  descr>
2426          <list>goodphrases</list>
2427          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  goodphrases/weighted_general_danish</file>
2428        </config>
2429        <config>
2430          <descr><![CDATA[goodphrases weighted_general_dutch]]></↩
                  descr>
2431          <list>goodphrases</list>
2432          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  goodphrases/weighted_general_dutch</file>
2433        </config>
2434        <config>
2435          <descr><![CDATA[goodphrases weighted_general_malay]]></↩
                  descr>
2436          <list>goodphrases</list>
2437          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  goodphrases/weighted_general_malay</file>
2438        </config>
2439        <config>
2440          <descr><![CDATA[goodphrases weighted_general_polish]]></↩
                  descr>
```

```
2441          <list>goodphrases</list>
2442          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  goodphrases/weighted_general_polish</file>
2443        </config>
2444        <config>
2445          <descr><![CDATA[goodphrases weighted_general_portuguese]]><↩
                  /descr>
2446          <list>goodphrases</list>
2447          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  goodphrases/weighted_general_portuguese</file>
2448        </config>
2449        <config>
2450          <descr><![CDATA[goodphrases weighted_general_swedish]]></↩
                  descr>
2451          <list>goodphrases</list>
2452          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  goodphrases/weighted_general_swedish</file>
2453        </config>
2454        <config>
2455          <descr><![CDATA[goodphrases weighted_news]]></descr>
2456          <list>goodphrases</list>
2457          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  goodphrases/weighted_news</file>
2458        </config>
2459        <config>
2460          <descr><![CDATA[gore weighted]]></descr>
2461          <list>gore</list>
2462          <file>/usr/local/etc/dansguardian/lists/phraselists/gore/↩
                  weighted</file>
2463        </config>
2464        <config>
2465          <descr><![CDATA[gore weighted_portuguese]]></descr>
2466          <list>gore</list>
2467          <file>/usr/local/etc/dansguardian/lists/phraselists/gore/↩
                  weighted_portuguese</file>
2468        </config>
2469        <config>
2470          <descr><![CDATA[idtheft weighted]]></descr>
2471          <list>idtheft</list>
2472          <file>/usr/local/etc/dansguardian/lists/phraselists/idtheft↩
                  /weighted</file>
2473        </config>
2474        <config>
2475          <descr><![CDATA[illegaldrugs weighted]]></descr>
2476          <list>illegaldrugs</list>
2477          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  illegaldrugs/weighted</file>
```

```
2478        </config>
2479        <config>
2480          <descr><![CDATA[illegaldrugs weighted_portuguese]]></descr>
2481          <list>illegaldrugs</list>
2482          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 illegaldrugs/weighted_portuguese</file>
2483        </config>
2484        <config>
2485          <descr><![CDATA[intolerance weighted]]></descr>
2486          <list>intolerance</list>
2487          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 intolerance/weighted</file>
2488        </config>
2489        <config>
2490          <descr><![CDATA[intolerance weighted_portuguese]]></descr>
2491          <list>intolerance</list>
2492          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 intolerance/weighted_portuguese</file>
2493        </config>
2494        <config>
2495          <descr><![CDATA[legaldrugs weighted]]></descr>
2496          <list>legaldrugs</list>
2497          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 legaldrugs/weighted</file>
2498        </config>
2499        <config>
2500          <descr><![CDATA[malware weighted]]></descr>
2501          <list>malware</list>
2502          <file>/usr/local/etc/dansguardian/lists/phraselists/malware↩
                 /weighted</file>
2503        </config>
2504        <config>
2505          <descr><![CDATA[music weighted]]></descr>
2506          <list>music</list>
2507          <file>/usr/local/etc/dansguardian/lists/phraselists/music/↩
                 weighted</file>
2508        </config>
2509        <config>
2510          <descr><![CDATA[news weighted]]></descr>
2511          <list>news</list>
2512          <file>/usr/local/etc/dansguardian/lists/phraselists/news/↩
                 weighted</file>
2513        </config>
2514        <config>
2515          <descr><![CDATA[nudism weighted]]></descr>
2516          <list>nudism</list>
```

```
2517          <file>/usr/local/etc/dansguardian/lists/phraselists/nudism/↩
                 weighted</file>
2518        </config>
2519        <config>
2520          <descr><![CDATA[peer2peer weighted]]></descr>
2521          <list>peer2peer</list>
2522          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 peer2peer/weighted</file>
2523        </config>
2524        <config>
2525          <descr><![CDATA[personals weighted]]></descr>
2526          <list>personals</list>
2527          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 personals/weighted</file>
2528        </config>
2529        <config>
2530          <descr><![CDATA[personals weighted_portuguese]]></descr>
2531          <list>personals</list>
2532          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 personals/weighted_portuguese</file>
2533        </config>
2534        <config>
2535          <descr><![CDATA[pornography weighted]]></descr>
2536          <list>pornography</list>
2537          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted</file>
2538        </config>
2539        <config>
2540          <descr><![CDATA[pornography weighted_chinese]]></descr>
2541          <list>pornography</list>
2542          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_chinese</file>
2543        </config>
2544        <config>
2545          <descr><![CDATA[pornography weighted_danish]]></descr>
2546          <list>pornography</list>
2547          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_danish</file>
2548        </config>
2549        <config>
2550          <descr><![CDATA[pornography weighted_dutch]]></descr>
2551          <list>pornography</list>
2552          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_dutch</file>
2553        </config>
2554        <config>
2555          <descr><![CDATA[pornography weighted_french]]></descr>
```

```
2556          <list>pornography</list>
2557          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_french</file>
2558        </config>
2559        <config>
2560          <descr><![CDATA[pornography weighted_german]]></descr>
2561          <list>pornography</list>
2562          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_german</file>
2563        </config>
2564        <config>
2565          <descr><![CDATA[pornography weighted_italian]]></descr>
2566          <list>pornography</list>
2567          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_italian</file>
2568        </config>
2569        <config>
2570          <descr><![CDATA[pornography weighted_japanese]]></descr>
2571          <list>pornography</list>
2572          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_japanese</file>
2573        </config>
2574        <config>
2575          <descr><![CDATA[pornography weighted_malay]]></descr>
2576          <list>pornography</list>
2577          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_malay</file>
2578        </config>
2579        <config>
2580          <descr><![CDATA[pornography weighted_norwegian]]></descr>
2581          <list>pornography</list>
2582          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_norwegian</file>
2583        </config>
2584        <config>
2585          <descr><![CDATA[pornography weighted_polish]]></descr>
2586          <list>pornography</list>
2587          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_polish</file>
2588        </config>
2589        <config>
2590          <descr><![CDATA[pornography weighted_portuguese]]></descr>
2591          <list>pornography</list>
2592          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/weighted_portuguese</file>
2593        </config>
2594        <config>
```

```
2595          <descr><![CDATA[pornography weighted_russian]]></descr>
2596          <list>pornography</list>
2597          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_russian</file>
2598        </config>
2599        <config>
2600          <descr><![CDATA[pornography weighted_russian_utf8]]></descr↩
                 >
2601          <list>pornography</list>
2602          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_russian_utf8</file>
2603        </config>
2604        <config>
2605          <descr><![CDATA[pornography weighted_spanish]]></descr>
2606          <list>pornography</list>
2607          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_spanish</file>
2608        </config>
2609        <config>
2610          <descr><![CDATA[pornography weighted_swedish]]></descr>
2611          <list>pornography</list>
2612          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 pornography/weighted_swedish</file>
2613        </config>
2614        <config>
2615          <descr><![CDATA[proxies weighted]]></descr>
2616          <list>proxies</list>
2617          <file>/usr/local/etc/dansguardian/lists/phraselists/proxies↩
                 /weighted</file>
2618        </config>
2619        <config>
2620          <descr><![CDATA[secretsocieties weighted]]></descr>
2621          <list>secretsocieties</list>
2622          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 secretsocieties/weighted</file>
2623        </config>
2624        <config>
2625          <descr><![CDATA[sport weighted]]></descr>
2626          <list>sport</list>
2627          <file>/usr/local/etc/dansguardian/lists/phraselists/sport/↩
                 weighted</file>
2628        </config>
2629        <config>
2630          <descr><![CDATA[translation weighted]]></descr>
2631          <list>translation</list>
2632          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 translation/weighted</file>
```

```
2633        </config>
2634        <config>
2635          <descr><![CDATA[travel weighted]]></descr>
2636          <list>travel</list>
2637          <file>/usr/local/etc/dansguardian/lists/phraselists/travel/↩
                weighted</file>
2638        </config>
2639        <config>
2640          <descr><![CDATA[upstreamfilter weighted]]></descr>
2641          <list>upstreamfilter</list>
2642          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                upstreamfilter/weighted</file>
2643        </config>
2644        <config>
2645          <descr><![CDATA[violence weighted]]></descr>
2646          <list>violence</list>
2647          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                violence/weighted</file>
2648        </config>
2649        <config>
2650          <descr><![CDATA[violence weighted_portuguese]]></descr>
2651          <list>violence</list>
2652          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                violence/weighted_portuguese</file>
2653        </config>
2654        <config>
2655          <descr><![CDATA[warezhacking weighted]]></descr>
2656          <list>warezhacking</list>
2657          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                warezhacking/weighted</file>
2658        </config>
2659        <config>
2660          <descr><![CDATA[weapons weighted]]></descr>
2661          <list>weapons</list>
2662          <file>/usr/local/etc/dansguardian/lists/phraselists/weapons↩
                /weighted</file>
2663        </config>
2664        <config>
2665          <descr><![CDATA[weapons weighted_portuguese]]></descr>
2666          <list>weapons</list>
2667          <file>/usr/local/etc/dansguardian/lists/phraselists/weapons↩
                /weighted_portuguese</file>
2668        </config>
2669        <config>
2670          <descr><![CDATA[webmail weighted]]></descr>
2671          <list>webmail</list>
```

```
2672          <file>/usr/local/etc/dansguardian/lists/phraselists/webmail↩
                  /weighted</file>
2673        </config>
2674      </dansguardianphraselistsweighted>
2675      <dansguardianphraselistsbanned>
2676        <config>
2677          <descr><![CDATA[gambling banned]]></descr>
2678          <list>gambling</list>
2679          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  gambling/banned</file>
2680        </config>
2681        <config>
2682          <descr><![CDATA[gambling banned_portuguese]]></descr>
2683          <list>gambling</list>
2684          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  gambling/banned_portuguese</file>
2685        </config>
2686        <config>
2687          <descr><![CDATA[googlesearches banned]]></descr>
2688          <list>googlesearches</list>
2689          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  googlesearches/banned</file>
2690        </config>
2691        <config>
2692          <descr><![CDATA[illegaldrugs banned]]></descr>
2693          <list>illegaldrugs</list>
2694          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  illegaldrugs/banned</file>
2695        </config>
2696        <config>
2697          <descr><![CDATA[intolerance banned_portuguese]]></descr>
2698          <list>intolerance</list>
2699          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  intolerance/banned_portuguese</file>
2700        </config>
2701        <config>
2702          <descr><![CDATA[pornography banned]]></descr>
2703          <list>pornography</list>
2704          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/banned</file>
2705        </config>
2706        <config>
2707          <descr><![CDATA[pornography banned_portuguese]]></descr>
2708          <list>pornography</list>
2709          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                  pornography/banned_portuguese</file>
2710        </config>
```

```
2711        <config>
2712          <descr><![CDATA[rta banned]]></descr>
2713          <list>rta</list>
2714          <file>/usr/local/etc/dansguardian/lists/phraselists/rta/↩
                 banned</file>
2715        </config>
2716        <config>
2717          <descr><![CDATA[safelabel banned]]></descr>
2718          <list>safelabel</list>
2719          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 safelabel/banned</file>
2720        </config>
2721      </dansguardianphraselistsbanned>
2722      <dansguardianphraselistsexception>
2723        <config>
2724          <descr><![CDATA[goodphrases exception]]></descr>
2725          <list>goodphrases</list>
2726          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 goodphrases/exception</file>
2727        </config>
2728        <config>
2729          <descr><![CDATA[goodphrases exception_email]]></descr>
2730          <list>goodphrases</list>
2731          <file>/usr/local/etc/dansguardian/lists/phraselists/↩
                 goodphrases/exception_email</file>
2732        </config>
2733      </dansguardianphraselistsexception>
2734      <dansguardianblacklistsdomains>
2735        <config>
2736          <descr><![CDATA[ads domains]]></descr>
2737          <list>ads</list>
2738          <file>/usr/local/etc/dansguardian/lists/blacklists/ads/↩
                 domains</file>
2739        </config>
2740      </dansguardianblacklistsdomains>
2741      <dansguardianblacklistsurls>
2742        <config>
2743          <descr><![CDATA[ads urls]]></descr>
2744          <list>ads</list>
2745          <file>/usr/local/etc/dansguardian/lists/blacklists/ads/urls↩
                 </file>
2746        </config>
2747      </dansguardianblacklistsurls>
2748    </installedpackages>
2749    <dhcrelay/>
2750
2751      <allowedip>
```

```
2752        <ip>132.248.x.y</ip>
2753        <sn>32</sn>
2754        <dir>both</dir>
2755        <descr><![CDATA[ibiologia]]></descr>
2756        <bw_up>1000</bw_up>
2757        <bw_down>1000</bw_down>
2758      </allowedip>
2759      <allowedip>
2760        <ip>132.248.x.y</ip>
2761        <sn>32</sn>
2762        <dir>both</dir>
2763        <descr><![CDATA[apoyo.ibiologia]]></descr>
2764        <bw_up>1000</bw_up>
2765        <bw_down>1000</bw_down>
2766      </allowedip>
2767      <allowedip>
2768        <ip>132.248.x.y</ip>
2769        <sn>32</sn>
2770        <dir>both</dir>
2771        <descr><![CDATA[web]]></descr>
2772        <bw_up>1000</bw_up>
2773        <bw_down>1000</bw_down>
2774      </allowedip>
2775      <interface>opt1</interface>
2776      <timeout/>
2777      <idletimeout/>
2778      <freelogins_count/>
2779      <freelogins_resettimeout/>
2780      <auth_method>none</auth_method>
2781      <reauthenticateacct/>
2782      <httpsname/>
2783      <preauthurl/>
2784      <bwdefaultdn/>
2785      <bwdefaultup/>
2786      <certificate/>
2787      <cacertificate/>
2788      <private-key/>
2789      <redirurl/>
2790      <radiusip/>
2791      <radiusip2/>
2792      <radiusport/>
2793      <radiusport2/>
2794      <radiusacctport/>
2795      <radiuskey/>
2796      <radiuskey2/>
2797      <radiusvendor>default</radiusvendor>
2798      <radiussrcip_attribute>wan</radiussrcip_attribute>
```

```
2799        <radmac_format>default</radmac_format>
2800        <page>
2801          /page>
2802        <enable/>
2803      </captiveportal>
2804      <ezshaper>
2805        <step1>
2806          <numberofconnections>5</numberofconnections>
2807        </step1>
2808      </ezshaper>
2809  </pfsense>
```