UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

IMPLEMENTACIÓN DE SERVICIOS PARA OPTIMIZAR EL USO DE LA RED E INTERNET EN LA COJUDEQ

TRABAJO MONOGRÁFICO
PARA OBTENER EL GRADO DE
INGENIERO EN REDES

PRESENTA
JEFF SAÚL BARDALES LÓPEZ

SUPERVISORES
DR. JAVIER VÁZQUEZ CASTILO
MSI. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE
MTI VLADIMIR VENIAMIN CABAÑAS VICTORIA

Universidad de Quintana Roo
DCI DIVISIÓN DE CIENCIAS E INGENIERÍA

CHETUMAL QUINTANA ROO, MÉXICO, MAYO DE 2016

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO MONOGRÁFICO ELABORADO BAJO SUPERVISIÓN DEL COMITÉ DE ASESORÍA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

COMITÉ DE TRABAJO MONOGRÁFICO

SUPERVISOR:

DR. JAVIER VÁZQUEZ CASTILLO

SUPERVISOR:

MSI. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE

SUPERVISOR:

MTI. VLADIMIR VENIAMIN CABAÑAS VICTOR

UNIVERSIDAD DE QUINTANA ROO
SERVICIOS ESCOLARES
TITULACIONES

Universidad de Quintana Roo
DCI DIVISIÓN DE CIENCIAS E INGENIERÍA

CHETUMAL QUINTANA ROO, MÉXICO, MAYO DE 2016

Agradecimientos

A toda mi familia que me apoyo en los tiempos difíciles, ya que siempre estuvieron ahí cuando más lo necesite. A mi padres Saúl Bardales Sandoval y Olga Verónica López Romero que me dieron el apoyo cuando me accidenté y a mi amada esposa Ana Griselda Cerón Canul que está siempre a mi lado y apoyarme en todo. A mis asesores por siempre estar pendientes de mi trabajo y preguntar cómo voy con el presente trabajo y como sigo de salud

Contents

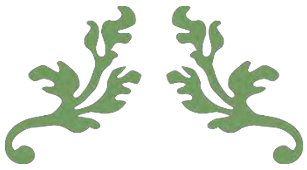
Índice de Ilustraciones

Índice de tablas

Resumen

Hoy en día el contar con un servicio ininterrumpido de internet en horas laborables es algo indispensable. Más aún si se trata en dependencias de gobierno o empresas, las cuales sus sistemas de bases de datos se encuentran en la nube o de dependen de un sistema de servicio remoto. Específicamente, en la Comisión para la Juventud y el Deporte de Quintana Roo (COJUDEQ) se proporciona un servicio de internet para que los trámites administrativos que realiza esta dependencia puedan realizarse de manera eficiente (facturación por los usos de las unidades deportivas, inscripción de atletas a competencias, entre otros). Sin embargo, esto no es del todo correcto, ya que frecuentemente el servicio de internet presenta diversas fallas, lo cual imposibilitaba que los usuarios puedan realizar con éxito sus trámites administrativos.

Es por ello, que en este trabajo monográfico se presenta una serie de acciones que fueron llevadas a cabo para mejorar la calidad en el servicio de Internet en la COJUDEQ. Para ello, fue necesario implementar una serie de diagnósticos del estado de la red actual con el fin de implementar estrategias de mejora en la calidad del servicio. Los diagnósticos fueron llevados a cabo mediante monitoreo de la red para observar el uso que se le estaba dando al servicio de Internet por parte de los usuarios, se realizaron inventarios de equipos de red/comunicaciones para conocer las capacidades tecnológicas con las que contaba dicha institución, se realizó una optimización de vida útil de los equipos de comunicaciones, entre otros. Con las acciones implementadas de este trabajo monográfico se logró extender la vida útil de los equipos de comunicaciones, mejorar la calidad del servicio de Internet, así como también, implementación de acciones de digitalización de información para la mejora del desempeño del sistema de almacenamiento de datos y su organización. El trabajo realizado mostró que haciendo estudios e implementando soluciones tecnológicas se puede impactar en el mejoramiento de la calidad del servicio de Internet y con ello lograr una satisfacción de los usuarios.



CAPÍTULO 1

Capítulo 1

1.1. Definición del Problema

El Internet se ha vuelto un recurso importante para la realización del trabajo cotidiano en la Comisión para la Juventud y el Deporte de Quintana Roo –COJUDEQ, debido a que varios servicios y procesos que se utilizan para las labores diarias están siendo orientados a la nube. Los usuarios de la COJUDEQ, manifestaron su malestar por el pobre desempeño del acceso a Internet afectando su productividad laboral a pesar de contar con cuatro módems con salida de ancho de banda de 4 Mbps cada uno, que prestan servicio a 150 personas aproximadamente. Como parte del Área de Informática encargada de dar soporte a este servicio, se observaba el uso excesivo y sin control de Internet, por lo que las aplicaciones de productividad se veían afectadas por falta de recursos hacia Internet. Se hace evidente el mal servicio que se tenía al interior de la Institución, al tener largos tiempos de espera para tener respuesta de los servicios críticos, ocasionando que se pierda tiempo valioso para realizar el trabajo de las áreas. Además, el Área de Informática carecía de la documentación técnica y de servicio requerida para realizar una reparación, mantenimientos preventivos, detectar un fallo y otros servicios como gestión de garantías, de la red y planeación.

Se hace evidente que la red creció de manera exponencial y rebasó al Área de Informática y por ello no se hicieron las adecuaciones pertinentes a la red de datos por lo que no cuenta con una instalación de aplicaciones y servicios de red que permita optimizar el funcionamiento de equipos y que a su vez permita que sea más fácil la administración.

1.2. Justificación

La implementación de servicios de monitoreo, restricción y acceso a la red, es necesaria para obtener una mayor eficiencia en el aprovechamiento del recurso de Internet con el fin de lograr que las personas realicen el trabajo en tiempo y forma sin descuidar los aspectos de seguridad, de igual forma, se requieren procedimientos que permitan reducir los tiempos de respuesta solicitados por los usuarios en la atención de servicios.

La carencia de documentación en el área de Tecnologías de Información y Comunicaciones, dificulta la toma de decisiones y el trabajo cotidiano de gestión, mantenimiento y solución de problemas.

La COJUDEQ no cuenta con un documento que indique cuáles son las políticas y procedimientos generales que deben de realizarse en el área de TICs en donde se plasmen las normas y responsabilidades a seguir.

1.3. El Objetivo General

Mejorar el rendimiento y seguridad de la red de la COJUDEQ a través de la gestión de servicios informáticos.

1.4. Objetivos Particulares:

- Priorizar servicios y procesos.
- Establecer políticas de uso de la red.
- Evaluar tecnologías de gestión de Calidad y Servicio (QoS).
- Evaluar tecnologías de gestión de la seguridad y de acceso.
- Evaluar tecnologías de monitoreo de la red.
- Reducir los tiempos de solicitud de servicio que demanden los usuarios.
- Prolongar la vida útil de los equipos de comunicaciones.
- Incrementar la seguridad.
- Realizar una lista de cotejo que sirva de guía para el funcionamiento básico de las máquinas de trabajo.
- Monitorear la red de Internet para tomar decisiones e implementar soluciones para su uso óptimo.

CAPÍTULO 2

Capítulo 2

En este capítulo hablaremos sobre las tecnologías tanto de software como de hardware que usamos para solucionar los problemas con los que contábamos como es la asignación de direcciones IP, para dar internet (cuidando tanto el hardware como los equipos de climatización) y servicio de escaneo en una de las áreas más importante de cualquier dependencia. Al igual explicamos porque no sea realizado migraciones de sistemas que se podrían considerar importantes. Más que una lista de cotejo tenemos una serie de procedimientos que con el tiempo y experiencia hemos implementado p que el equipo funcione correctamente y el usuario pueda realizar su trabajo sin complicaciones.

Equipo en reparación

- Recepción de equipo.
- Recepción de oficio solicitando la reparación (requerimiento o el fallo).
- Creación de papeleta del equipo (detalles de problema, observaciones, fecha de ingreso, inventario, área asignada, etc).
- Resolución (formateo, limpieza, diagnostico e incluso remplazo o reparación de hardware)
- Entrega del equipo o baja del mismo.

Habilitación de equipos (debido a reparación o equipos nuevos)

- Instalación de sistema operativo (Windows 7 pro) con sus actualizaciones al día.
- Asignación de dirección IP
- Instalación de ofimática (Microsoft Office 2010 pro) con sus actualizaciones al día.
- Instalación de software multimedia (VLC, CCCP).
- Instalación de utilerías (JAVA, winrar, .net).
- Instalación de antivirus.
- En algunos equipos requieren de aplicaciones para sistemas específicos los cuales no se detallaran.

2.1. Actualización de hardware y software

2.1.1. Análisis.

Como parte de la estrategia del plan Digital del Estado de Quintana Roo 2012-2016, en donde indica la mejora en la prestación de los servicios de red, se procedió al levantamiento de inventario con que contaba en la COJUDEQ en ese periodo. Además se establecieron las estrategias para el remplazo de hardware y software para proporcionar el servicio de Internet.

2.1.2. Problemática.

Anteriormente se usaba software basado en Windows para proporcionar el servicio de Internet como era el *kerio 7.2* pero éste presentaba problemas con frecuencia con el mismo sistema Windows (Múltiples puertas de enlace, IP inválida, etc-). También existían equipos mal instalados o dañados, mal configurados, cables de red en mal estado entre otros.

2.1.3. Solución.

Se remplazó el *Gateway Kerio* el cual estaba instalado en un Windows 7, en un servidor DELL PowerEdge debido a que presentaba además de los problemas descritos anteriormente muchos otros problemas relacionados con la red. Sin embargo al revisar y modificar la configuración en múltiples ocasiones el problema no se resolvía, todos estos problemas generaban a que no funcionara el servicio de Internet. Se instaló inicialmente el servicio de *untangle* pero nos marcaba conflictos con páginas basadas en servicios de Windows. Como es Hotmail y algunas páginas de gobierno. Decidió sustituirse por *endian* pero debido a su naturaleza cerrada de la plataforma era muy complicado automatizar procesos como apagado incluso administrar servicios como es el DHCP, otro causa del abandona de estas 2 plataformas (*untangle y endian*) es la limitación en su configuración ya que existen sus versiones de paga, donde los servicios que son gratis son considerados Lite con limitantes y restricciones.

Actualmente se está utilizando el *pfSense* que es un Firewall Open Source el cual está basado en UNIX conocida por ser una plataforma muy robusta

2.2. Dispositivos invitados y dispositivos dinámicos

2.2.1. Análisis

Ofrecer un servicio de Internet a los dispositivos dinámicos, procurando que fuera sencilla y transparente su conexión para el usuario final. Como dispositivos dinámicos nos referimos aquellos que no están en un lugar fijo conocidos como BYOD – *Bring Your Own Device* que son propiedad de los usuarios y no de la COJUDEQ.

2.2.2. Problemática

Una gran cantidad de usuarios requieren el uso del Internet debido a la naturaleza de la dependencia, y una de las primeras cuestiones fue el de controlar la cantidad de asignaciones de configuraciones de red (IP), tiempo de asignación y quienes se pueden conectar.

2.2.3. Solución

La herramienta *pfSense* cuenta con un servidor DHCP, fácil de configurar e implementar, pero existía la necesidad de personalizar aún más la asignación dinámica de configuraciones, por ejemplo por tiempo variable dependiendo del dispositivo o el usuario. Se recurrió a la implementación de un servidor Debian con el DHCP Server (ISC DHCPd versión 4.1.1) incluido, se usa la distribución de Linux Debian debido a que es estable con bastante documentación y soporta múltiples aplicaciones. Así como una comunidad de usuarios que pueden ayudar con la resolución de problemas.

Debido a la velocidad con la se realizan en muchas ocasiones la demanda para la asignación de la configuración IP, desde el contacto por parte del usuario pasando por la lectura de la dirección MAC de la interface a conectar, la asignación de la IP, liberación, permiso y alta en servidor DHCP, se decidió usar el administrador Webmin, que presenta varias ventajas:

- Es gráfico (basado en Web)
- Se pueden configurar varios servicios además de DHCP como DNS, Apache, compartir archivos, entre otros.

A continuación se muestra el diagrama de flujo de cómo se realiza una asignación de IP a un

dispositivo. En el caso de que ya está aprobado que el dispositivo estará en nuestra red.

Ilustración 1Proceso de asignación de dirección IP a un nuevo dispositivo en el servidor DHCP

En la imagen anterior se describe a grandes rasgos el proceso que se realiza para dar de alta un nuevo dispositivo en el servidor DHCP.

En la siguiente figura se muestra el proceso para que una dirección IP pueda acceder a Internet:

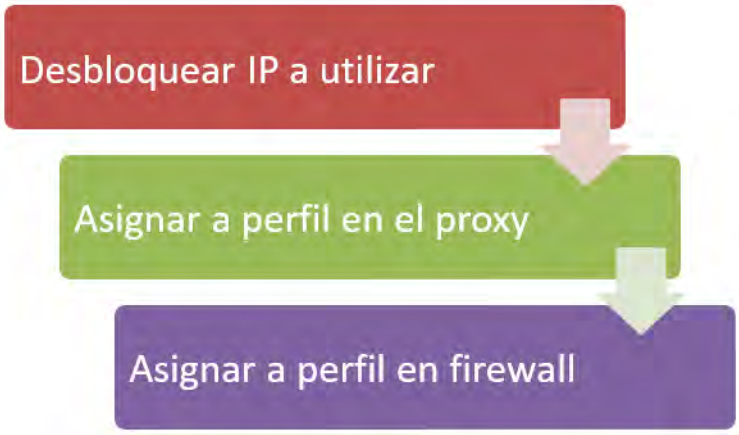


Ilustración 2Proceso para dar Internet a un IP

2.3. Extender tiempo de vida de equipos de climatización y servicio de Internet.

2.3.1. Análisis

Dar servicios de Internet conlleva tener equipos en buen estado, esto se logra con una climatización y evitar desgastes excesivos tanto de los equipo de climatización como de los que proveen el servicio de Internet.

2.3.2. Problemática

Hace aproximadamente 2 año sufrimos daños en los equipos de aire acondicionado del área donde se encuentra el servidor (SITE) esto generó que el servidor fallara constantemente debido al calentamiento y generaba calor en las áreas próximas, así como generando ruido excesivo por la razón de tener que dejar abierto las áreas para evitar el sobre calentamiento de los mismo. Traduciendo en servicio de Internet intermitente y en el malestar de los usuarios.

2.3.3. Solución

Para dar solución se requirió del uso de un equipo *timer*, un router WRT54G de Linksys con un firmware DD-WRT, la creación de unos scripts para automatizar el apagado de los diferentes servidores y algunas líneas de comando en la parte del servidor XenServer para automatizar la parte del encendido de la misma.

Donde el *timer* enciende el *router* Linksys ya previamente configurado y este proveerá del servicio de internet por la noche y parte de la madrugada, evitando que el servidor y los equipos de climatización queden encendidos, debido a que este router no genera mucho calor, los scripts apagaran los servidores a una hora establecida y el clima se programa para su apagado 2 horas después de la salida. La combinación de todo esto genera ampliar la vida de los climas y servidores.

2.4. Digitalización de área contable

2.4.1. Análisis

La digitalización de documentos para ser usados de diferentes maneras, es en la actualidad para el área contable de suma importancia, pero ¿qué pasa si la configuración es demasiado tardada y puede presentar problemas debido a la cantidad de restricciones de los equipo interesados?

2.4.2. Problemática

Restricciones, configuración compleja y la intermitencia en la digitalización fueron algunos de los problemas que se generaron al momento de recibir una impresora Kyocera km-3050, requería que se instalara una carpeta compartida en cada uno de los equipos interesados en utilizar el servicio. Debido a la cantidad de equipos y de documentos a digitalizar no era una opción viable y debido a la naturaleza de los equipos todos requerían de contraseñas, donde el mismo Windows restringía el uso de la carpeta por el nivel de permisos que era necesario establecer.

2.4.3. Solución

La solución a este problema fue crear un medio compartido donde la impresora envía todo lo que escanea y luego los usuarios pueden copiar, cortar y borrar lo digitalizado accediendo a este medio como una unidad de red. Todo esto se conllevo a la implementación de un servidor FreeNAS (FreeNAS-8.3.1-RELEASE-x64 (r13452)), donde se usó FTP, CIFS, Sharing y permisos. También se automatizaron procesos para borrar archivos que no sean PDF, Limpiar la unidad todos los días, crear un archivo de advertencia con la ayuda del cron e incluso el apagado automático de este servidor.

2.5. Solución para el óptimo desempeño lógico de los equipos de cómputo.

2.5.1. Análisis

Hoy en día es de gran importancia la compatibilidad entre las aplicaciones, páginas e incluso hardware, todo esto se logra a través del software. Donde una mala implementación del

mismo puede tener consecuencias importantes.

2.5.2. Problemática

Software obsoleto, aplicaciones desactualizadas e incluso software no deseado es uno de los grandes problemas con los que nos enfrentamos. Ya que éstos nos presentan desde problemas con formatos, hasta alteración en el contenido de páginas y documentos, e incluso mal desempeño en el hardware de los equipos.

2.5.3. Solución

Software actualizado, es una de las claves para que exista una armonía entre el desempeño de las maquinas, siempre teniendo cuidado de la procedencia de las aplicaciones, siendo que se bajan siempre de las paginas oficiales, en el caso de la navegación usamos navegadores compatibles con las mayoría de las paginas como es Firefox, en el caso de antivirus usamos el Avast o en su caso AVG, así como usamos versiones actualizadas de JAVA, en el caso del que la persona requiera una versión diferente por algún sistema que necesite, se usara la versión requerida. En el caso de las librerías de .NET de Microsoft usamos la versión 4.5, debido a que es la que cumple con los requerimientos de algunos sistemas que se utilizan. La versión de Windows que utilizamos es la Microsoft Windows 7 Professional y Microsoft Office 2013 Professional en el caso de la ofimática.

2.6. ¿Por qué no actualizamos a la última versión de pfSense?

2.6.1. Análisis

La necesidad de un servicio de Internet óptimo para trabajar, es de gran importancia por eso se utilizan herramientas de software que ayuden a optimizar y controlar el servicio de Internet como son el Firewall y los Proxy.

2.6.2. Problemática

En muchas ocasiones no es posible actualizar una versión ya sea por algún *bug* que no está relacionada a problemas con configuración o por alguna incompatibilidad con el hardware actual, en las siguientes líneas describiremos brevemente porqué aún no actualizamos a la versión más reciente la 2.2.1 (publicada 2015-03-13)

La versión que actualmente está funcionando es la 2.1 publicada el 2013-09-15, y es la compatible con nuestro servidor.

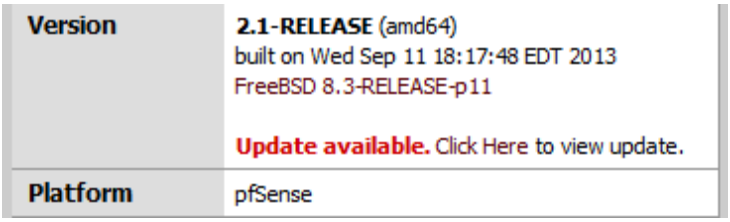


Ilustración 3 Versión en uso del pfSense

¿Por qué razón no actualizamos desde el mismo servidor? Sencillo, porque las instrucciones y las configuraciones no son siempre las mismas entre versiones antiguas o versiones superiores, tuvimos el caso que teníamos la versión 2.0 y tuvimos problemas con actualizar a la versión 2.1, los problemas más comunes fueron la compatibilidad con la configuración de los servicios como proxy por ejemplo, los alias e incluso con aplicaciones de monitoreo como *ntop*.

¿Por qué razón no instalamos desde cero? Las versiones posteriores de la 2.1 (2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5) presentaron problemas con las interfaces virtuales de red creadas con el Citrix XenServer, siendo que te deja configurar pero al momento de reiniciar te mostraba un *kernel panic*, investigando un poco el problema estaba relacionado con la versión de *kernel* del FreeBSD en el cual se basaba.

La versión 2.2 no fue instalada por la fecha en que fue publicada, sin embargo se pretendió migrar desde 0 a la versión 2.2.1, el problema que mostró fue una denegación de servicio debido al proxy (squid) ya sea transparente o no, al momento de asignar una política de Limiter a cualquier regla en el Firewall, donde los host contenidos en esa política eran los afectado los otros no, este problema ya fue documentado en los foros de pfSense, se podría trabajar sin el Limiter pero cualquiera podría bajar a toda la velocidad disponible. Nada recomendable.

Existe actualmente la versión 2.2.2 que fue publicada el 2015-04-15, pero aun no realizamos las pruebas necesarias para ver si el problema se resolvió. En la página de detalles de las correcciones y cambios no encontramos información sobre si se corrigió el problema

mencionado.

Ilustración 4 Versión actual de pfSense

Mensaje del servidor pfSense 2.2.1

```
A new version is now available

Current version: 2.2.1-RELEASE
       Built On: Fri Mar 13 08:16:49 CDT 2015
    New version: 2.2.2-RELEASE

  Update source: https://updates.pfsense.org/_updaters/amd64
```

Ilustración 5 Mensaje de actualización del pfSense

A continuación mostramos una tabla de con las versiones de pfSense

pfSense Version	Config Rev	pfSense Branch	FreeBSD Version	FreeBSD Branch	Release Date	Release Status
1.2	3.0	RELENG_1_2	6.2-RELEASE-p11	RELENG_6_2	2008-02-25	No longer supported
1.2.1	3.0	RELENG_1_2	7.0-RELEASE-p7	RELENG_7_0	2008-12-26	No longer supported
1.2.2	3.0	RELENG_1_2	7.0-RELEASE-p8	RELENG_7_0	2009-01-09	No longer supported
1.2.3	3.0	RELENG_1_2	7.2-RELEASE-p5	RELENG_7_2	2009-12-10	No longer supported
2.0	8.0	RELENG_2_0	8.1-RELEASE-p4	RELENG_8_1	2011-09-17	No longer supported
2.0.1	8.0	RELENG_2_0	8.1-RELEASE-p6	RELENG_8_1	2011-12-20	No longer supported
2.0.2	8.0	RELENG_2_0	8.1-RELEASE-p13	RELENG_8_1	2011-12-21	No longer supported
2.0.3	8.0	RELENG_2_0	8.1-RELEASE-p13	RELENG_8_1	2013-04-15	No longer supported
2.1	9.8	RELENG_2_1	8.3-RELEASE- p11	RELENG_8_3	2013-09-15	Previous stable release
2.1.1	10.1	RELENG_2_1	8.3-RELEASE-p14	RELENG_8_3	2014-04-04	Previous stable release
2.1.2	10.1	RELENG_2_1	8.3-RELEASE-p14	RELENG_8_3	2014-04-10	Previous stable release
2.1.3	10.1	RELENG_2_1	8.3-RELEASE-p16	RELENG_8_3	2014-05-02	Previous stable release
2.1.4	10.1	RELENG_2_1	8.3-RELEASE-p16	RELENG_8_3	2014-06-25	Previous stable release
2.1.5	10.1	RELENG_2_1	8.3-RELEASE-p16	RELENG_8_3	2014-08-27	Previous stable release Includes
						fixes/enhancements from after 2.1.4
2.2	11.6	RELENG_2_2	10.1-RELEASE- p4	releng/10.1	2015-01-23	Previous stable supported release
2.2.1	11.7	RELENG_2_2	10.1-RELEASE- p6	releng/10.1	TBD	Current stable maintenance/security release
2.2.2	TBD, >=11.7	RELENG_2_2	TBD, >= 10.1-RELEASE-p6	releng/10.1	TBD	Next stable maintenance/security release
2.3	TBD, >=11.7	master	TBD	TBD	TBD	Future release

Tabla 1 Tabla oficial de publicaciones de pfSense

2.6.3. Solución

Actualmente estamos trabajando en la implementación del nuevo sistema de pfSense desde 0 de la versión 2.2.2, pero aun no realizamos las pruebas necesarias para ver si se corrigió el problema con la denegación del servicio debido a Limiter y el SQUID.

CONCLUSIONES

Capítulo 3 CONCLUSIONES

Como leímos anteriormente existen varias maneras de mantener una red lo más sana posible y optimizar los recursos que se tienen, desde el cuidado del desgaste físico de los climas y equipos de cómputo, hasta el uso del internet, incluso el ahorro al momento de administrar grandes cantidades de información generada por un área crucial como es el área financiera. Claro, todo esto pasando por la implementación de servicios y equipos.

Para la digitalización se utilizó la herramienta FreeNAS, que es rápida y confiable. Debido a que cuenta con varias tecnologías que ayudaron a resolver el problema de digitalización masiva del área de recursos financieros, ya que combinamos FTP, restricciones, SMB e incluso programación de tareas. Todo con un sistema basado en Unix, lo cual nos garantiza que no fallara en momentos importantes.

Una cosa importante a tener en cuenta es mantener un correcto inventario lógico de los equipos administrados ya que de ahí se toman muchas decisiones al momento de dar permisos y privilegios, no es lo mismo un jefe de departamento a una asistente, las necesidades y los compromisos son distintos.

Espero que con este trabajo se tomen en cuenta muchas cosas que mayormente están asociadas al software propietario o software especializado de gran precio, un claro ejemplo, el control de ancho de banda con ayuda del *Limiter* de *pfSense* o comprar servidores especializados en almacenamiento de Red (NAS).

Otra cosa que aprendimos es el compromiso de otorgar un buen servicio a pesar de no ser de nuestra área de responsabilidad, por ejemplo hay muchos problemas que son generados por factores externos ajenos a nuestra red, como podría ser un envenenamiento de servidor DNS, sin embargo tiene que ser resuelto para poder seguir dando el servicio esperado.

Muchas herramientas y utilerías son proporcionadas por el mismo software que usamos como son los monitores de procesos, de Internet, etc. Pero lo que realmente hay que tomar en cuenta al momento de usarlas es que hay que saber usarlas y cuáles son sus limitaciones.

REFERENCIAS

REFERENCIAS

Andreasson, O. (2006). *Iptables Tutorial 1.2.2*. [online] Linuxsecurity.com. Available at: http://www.linuxsecurity.com/resource_files/firewalls/IPTables-Tutorial/iptables-tutorial.html [Accessed 20 Feb. 2012].

Burm.net, (2015). *XenServer Tips and Tricks â€“ Auto Start Your VM | Burm.net*. [online] Available at: http://burm.net/2012/01/28/xenserver-tips-and-tricks-auto-start-your-vm/ [Accessed 28 May 2015].

Dd-wrt.com, (2009). *Tutorial de instalacón para WRT54G v4 - DD-WRT Wiki*. [online] Available at: http://www.dd-wrt.com/wiki/index.php/Tutorial_de_instalaci%C3%B3n_para_WRT54G_v4 [Accessed 12 Oct. 2012].

Desde Linux, (2010). *Cron & crontab, explicados*. [online] Available at: http://blog.desdelinux.net/cron-crontab-explicados/ [Accessed 28 May 2015].

Forum.pfsense.org, (2015). *NTOP wont Start after Upgrade to 5.0.1_1 v2.4*. [online] Available at: https://forum.pfsense.org/index.php?PHPSESSID=4ain15njqj81h0l000vpk4qvk6&topic=76358.0 [Accessed 13 Mar. 2015].

Forum.pfsense.org, (2015). *Traffic Shaper: Limiter*. [online] Available at: https://forum.pfsense.org/index.php?topic=91299.0 [Accessed 23 Apr. 2015].

Freenas.org, (2013). [online] Available at: http://www.freenas.org/images/resources/freenas8.3.1/freenas8.3.1_guide.html [Accessed 20 Apr. 2013].

Squidworks.net, (2015). *PFSense 2.0 â€“ Limiting users Upload and Download Speeds by Limiting Bandwidth.*. [online] Available at: http://www.squidworks.net/2012/08/pfsense-2-0-limiting-users-upload-and-download-speeds-by-limiting-bandwidth/ [Accessed 28 May 2015].

Sysadmin.compxtreme.ro, (2012). *Autostart VM in free version of XenServer 6.x | SysAdmin*. [online] Available at: http://sysadmin.compxtreme.ro/autostart-vm-in-free-version-of-

xenserver-6-x/ [Accessed 28 May 2015].

The Linux Daily, (2010). *Automatically Start a Script at Linux Bootup*. [online] Available at: http://www.thelinuxdaily.com/2010/01/automatically-start-a-script-at-linux-bootup/ [Accessed 6 Mar. 2013].

Tuxjm.net, (2012). *Configuraciones basicas de squidGuard*. [online] Available at: http://tuxjm.net/docs/Manual_de_Instalacion_de_Servidor_Proxy_Web_con_Ubuntu_Server_y_Squid/html-multiples/ch05s02.html [Accessed 28 May 2015].

REFERENCIAS LIBROS ELECTRÓNICOS

Buechler, C. and Pingle, J. (2009). *pfSense*. [s.l.]: Reed Media Services.

Williamson, M. (2011). *PfSense 2 cookbook*. Birmingham, UK: Packt.

GLOSARIO

GLOSARIO

Bandwidth: Transferencia máxima de una red o dispositivo. Se expresa en cantidad de datos por tiempo dado. (por ejemplo: 256Kbps = 256 Kilobits por segundo).

BSD: erkeley Software Distribution o BSD (en español, «distribución de software berkeley») fue un sistema operativo derivado del sistema Unix nacido a partir de los aportes realizados a ese sistema por la Universidad de California en Berkeley.

Cliente: En una red se llama cliente al PC o a la estación de trabajo que recibe servicios de otro ordenador llamado servidor.

Debian: Debian o Proyecto Debian1 (en inglés: Debian Project2) es una comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo GNU basado en software libre. El sistema se encuentra precompilado, empaquetado y en un formato deb para múltiples arquitecturas de computador y para varios núcleos.

DHCP: DHCP es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Dirección IP: el número que identifica a cada dispositivo dentro de una red con protocolo IP.

Dirección MAC: En las redes de computadoras, la dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

DNS: El Sistema de nombres de dominio (DNS) es la herramienta principal de resolución de nombres que se utiliza en Internet. Se encarga de la resolución entre nombres de host y direcciones de Internet.

Firewall: Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall. Un firewall puede ayudar a impedir que hackers o software malintencionado (como gusanos) obtengan acceso al equipo a través de una red o de Internet. Un firewall también puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos.

FreeNAS: FreeNAS es un sistema operativo basado en FreeBSD que proporciona servicios de almacenamiento en red. NAS son las siglas en inglés de Almacenamiento Conectado en Red (Network Attached Storage). Este sistema operativo gratuito, open-source y software libre (basado en licencia BSD) permite convertir una computadora personal en un soporte de almacenamiento accesible desde red, por ejemplo para almacenamientos masivos de información, música, backups, etc.

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Host: Nombre de un ordenador en una red.

Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Limiter: La característica limiters establece Tuberias Dummynet. Dummynet fue diseñado para simular cualquier tipo de conexión de red. Varios tipos de conexiones se pueden simular son acceso telefónico, T1, un T1 ejecutar a través de microondas, o una conexión por satélite a la Luna. Un efecto secundario de ser capaz de simular cualquier tipo de conexión de red es que también se pueden utilizar para limitar la cantidad de ancho de ancho de banda de un host o grupo de hosts.

Linux: GNU/**Linux** es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix denominado **Linux** con el sistema GNU . Su desarrollo es uno de los ejemplos más prominentes de software libre.

Login: Programa encargado de la validación de un usuario a la entrada al sistema. Primero pide el nombre del usuario y después comprueba que el password sea el asignado a este.

M**icrosoft Windows**: Microsoft Windows es una familia de sistemas operativos para las computadoras personales compatibles IBM. Es el sistema operativo más común, principalmente debido a que viene preínstalado en la mayoría de las computadoras vendidas en el mercado.

Ntop: ntop es una herramienta que permite monitorizar en tiempo real una red. Es útil para controlar los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto y para ayudarnos a detectar malas configuraciones de algún equipo, o a nivel de servicio.

Opera: Opera es un navegador web creado por la empresa noruega Opera Software. Usa el motor de renderizado Blink. Tiene versiones para computadoras de escritorio, teléfonos móviles y tabletas.

Permisos: Todos los archivos en UNIX/Linux tienen definido un conjunto de permisos que permiten establecer los derechos de lectura, escritura o ejecución para el dueño del archivo, el grupo al que pertenece y los demás usuarios.

PfSEnse: pfSense es una distribución personalizada de FreeBSD adaptado para su uso como Firewall y Router. Se caracteriza por ser de código abierto, puede ser instalado en una gran variedad de ordenadores, y además cuenta con una interfaz web sencilla para su configuración.

Proxy: Un proxy, o servidor proxy, en una red informática, es un servidor, que sirve de intermediario en las peticiones de recursos que realiza un cliente a otro servidor.

RAM: Memoria de acceso aleatorio. Es una memoria volátil, que pierde su contenido cuando se desconecta la alimentación. Se suele utilizar para almacenar datos temporales o resultados intermedios.

Red Hat: Red Hat es una distribución Linux creada por Red Hat , que llegó a ser una de las más populares en los entornos de usuarios domésticos hasta el 22 de septiembre de 2003 cuando lo proyectos Fedora y Red Hat se fusionaron. La versión 1.0 fue presentada el 3 de noviembre de 1994.

root: Persona o personas encargadas de la administración del sistema. Tiene TODO el privilegio para hacer y deshacer, por lo que su uso para tareas que no sean absolutamente necesarias es muy peligroso.

Shell: La shell es el intérprete de comandos que se establece entre nosotros y el kernel. Hay muchos tipos de shell cada uno con sus propias características, sin embargo el estándar en GNU/Linux es el shell bash ya que es el que forma parte del proyecto GNU.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

SSH: SSH (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.
TCP/IP: el conjunto de protocolos de red en la que se basa Internet o intranet.

XenServer: Citrix XenServer es una plataforma líder para administración de hipervisor y virtualización de servidores que reduce el costo total de la propiedad de infraestructuras de virtualización de servidores, nubes y escritorios.

ANEXOS

ANEXO 1 Firewall

Descripción del Firewall

Un Firewall es un equipo que permite o deniega servicios en una red. El firewall usado es pfSense el cual es basado en FreeBSD.

Detalles del Firewall

El pfSense se empezó a usar como remplazo a las 2 plataformas (endian y untangle) dando muy buen resultado, siendo que este Firewall tiene una curva de aprendizaje mayor para su implementación. Debido que toda la configuración del Firewall se basa en Alias (IP, Ports, URL), se pueden generar grupos de alias, esto ahorra tiempo al momento de configurar.

Ilustración 6 Etiquetas de Alias

Por ejemplo este es un alias que almacena otros alias, la cual permitir el acceso a varias áreas al mismo tiempo.

Ilustración 7 Este es una Alias que almacena otros Alias

En la parte de las reglas debemos determinar las acciones (block, pass, reject), la interfase (LAN), la versión del TCP/IP(4 y 6), el protocolo TCP, UDP, ICMP, etc.

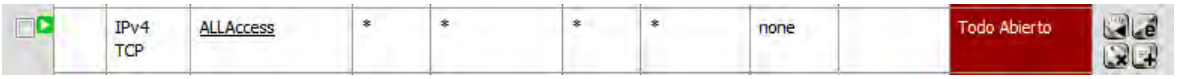


Ilustración 8 Permitimos todos los puertos al Alias ALLAccess

Una de las ventajas que tenemos con este Firewall es que podemos bloquear un sitio con la ayuda del DNS, dándole un nombre FQDN.

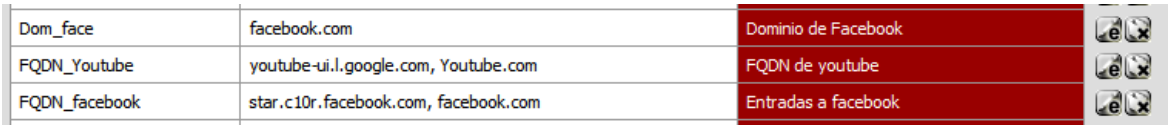


Ilustración 9 Alias con Bloqueo por Dominio

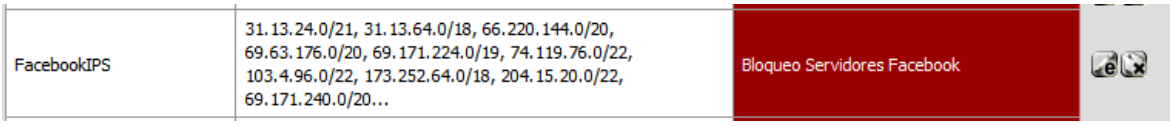
Las direcciones IP resueltas por el DNS Interno se van agregando, en el caso de Facebook, cada que un usuario intenta entrar a Facebook, el Firewall resuelve una IP y la manda dentro de una tabla que luego usa para bloquear o permitir.

En este caso lo utilizamos en youtube.

	IPv4+6 TCP/UDP	LAN net	*	FacebookIPS	*	*	none		Bloqueo Facebook
	IPv4+6 TCP/UDP	LAN net	*	FQDN Youtube	*	*	none		Bloqueo Facebook

Ilustración 10 Bloqueo de Facebook y Youtube en el Firewall

Las IPS contenidas en el alias FacebookIPS son proporcionadas por el servicio de he.net, el cual es una herramienta que explicaremos más tarde.



FacebookIPS	31.13.24.0/21, 31.13.64.0/18, 66.220.144.0/20, 69.63.176.0/20, 69.171.224.0/19, 74.119.76.0/22, 103.4.96.0/22, 173.252.64.0/18, 204.15.20.0/22, 69.171.240.0/20...	Bloqueo Servidores Facebook

Ilustración 11 Direcciones IP de Facebook proporcionados por he.net

El origen destino puerto etc., incluso se puede limitar la velocidad del Internet con el Traffic Shaper: Limiter, más adelante explicaremos en que consiste el Limiter.

Ilustración 12 Sección de Limiter del Traffic Shaper

PfSense cuenta con gráficas generadas con RRD Graphs que muestran un monitor el sistema.

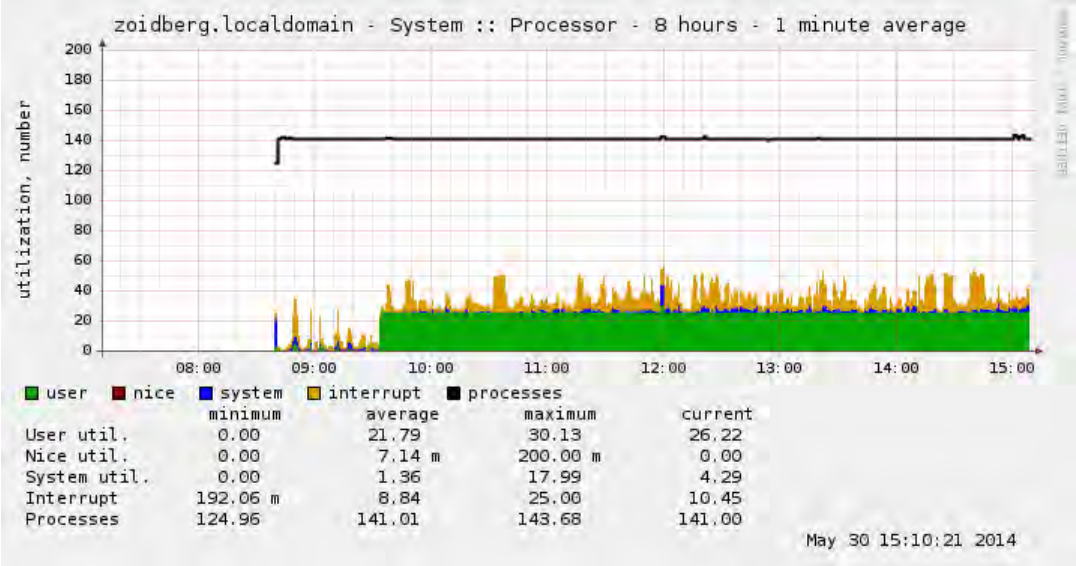


Ilustración 13 Gráfica del Uso del Sistema

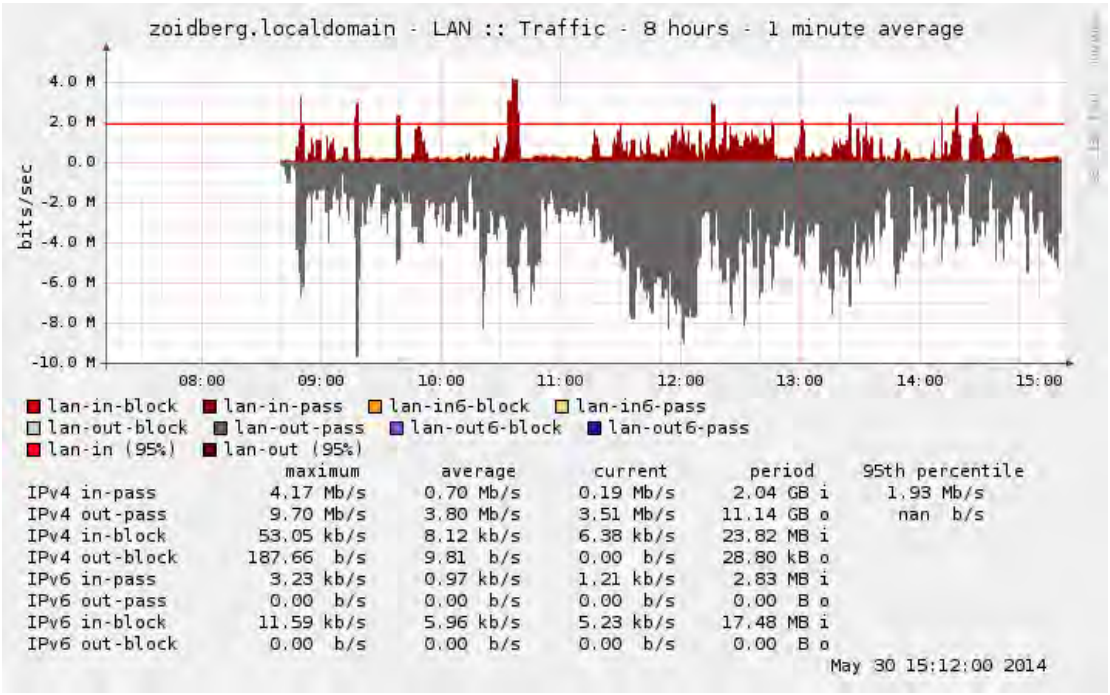


Ilustración 14 Gráfica del Tráfico del pfSense

pfSense cuenta con varios paquetes a ser instalados como es el cron, ntop, lightsquid, squid, squidguard y muchos más que actualmente están siendo usados.

El uso del *cron* es un comando que permite realizar una acción a un momento específico (hora, fecha), incluso diario si así se desea. El cron lo estamos realizando para automatizar el apagado del Firewall.

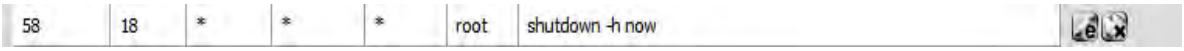


Ilustración 15 Usando cron desde la Aplicación del pfSense

A grandes rasgos lo que realiza es ejecutar el comando *shutdown-h now a las 18:58 hrs (6:58 pm),* todo con privilegio de *root*.

Squid es un servidor proxy-caché que usamos con la ayuda del *squidguard* para permitir o denegar páginas. No estamos cacheando nada de información sólo usamos para bloquear contenido no apropiado.

Se determinan los grupos a los que se aplicaran los permisos de que páginas están ALLOW o DENY. Estas páginas fueron determinas con la ayuda de una BLACKLIST proporcionada por shallalist.de.

Ilustración 16 Grupo de IPs con Privilegios

Luego aplicamos que categorías (listas donde se guardan sitios) vamos a bloquear o permitir

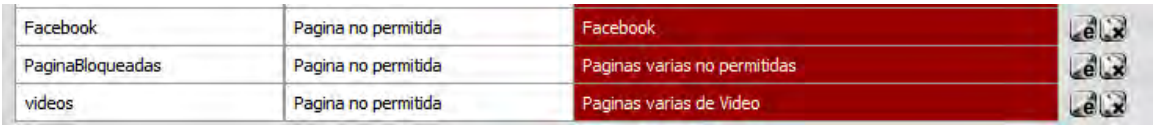


Ilustración 17 Categorías personalizadas de squidGuard con páginas no permitidas

Donde recordemos que siempre es la lectura de arriba hacia abajo donde arriba se colocan de preferencia los permitidos y abajo los denegados.

pfSense cuenta con herramientas que nos ayudan a determinar que esta está pasando en el servidor. Como un LOG de sistema.

Jul 11 09:03:51	ntop[27614]: THREADMGMT[t34470729152]: RRD: Throughput data collection: Thread starting [p27614]
Jul 11 09:03:51	ntop[27614]: THREADMGMT[t34470729152]: RRD: Throughput data collection: Thread running [p27614]
Jul 11 15:08:18	php: /index.php: Successful login for user 'admin' from: 192.168.5.34
Jul 11 15:08:18	php: /index.php: Successful login for user 'admin' from: 192.168.5.34
Jul 11 15:10:10	sshd[95680]: Accepted keyboard-interactive/pam for root from 192.168.5.34 port 53681 ssh2
Jul 11 17:00:35	php: /index.php: Successful login for user 'admin' from: 192.168.5.34
Jul 11 17:00:35	php: /index.php: Successful login for user 'admin' from: 192.168.5.34
Jul 11 17:16:31	php: /index.php: Successful login for user 'admin' from: 192.168.5.34
Jul 11 17:16:31	php: /index.php: Successful login for user 'admin' from: 192.168.5.34

Ilustración 18 Log de Sistema pfSense

LOG de Firewall

Ilustración 19 Log del Firewall

PfSense es un Firewall que tiene muchos paquetes y herramientas, el cual podrían ayudarnos a dar soluciones a muchos problemas. Podemos crear DHCP, VPN, portal cautivo, balanceo de cargas, NAS, redirección de DNS y se complementa con muchos paquetes como son el SQUID, cron, herramientas de Reportes, etc. sólo es cuestión de ajustar a las necesidades.

ANEXO 2 Semi-automatización de servicios de encendido y apagado de servidores.

Descripción de la implementación.

Se describirá el proceso y los comandos usados para prender y apagar los diferentes servicios, así como se mencionaran los diferentes equipos usados para lograr este objetivo.

Detalles de la implementación

Se realizó el proceso semiautomático de apagado y prendido de equipos de comunicaciones con el fin de seguir proporcionando el servicio de Internet en las instalaciones, sin generar un calor excesivo, usando *scripts* en el sistema para el apagado y un *timer* para prender un router linksys que será el que proporcione el servicio en horas no pico.

En las oficinas de la COJUDEQ tenemos definidos los siguientes horarios en donde se describe que equipos funcionaran y en que horario durante la semana laboral Lunes a Viernes

Horario	Proceso	Tip	Equi
5:00 AM	Encendido	Automático	Router Linksys WRT54G
8:30 AM	Encendido	Manual	Servidor Dell PowerEdge
8:30 AM	Apagado	Automático	Router Linksys WRT54G
8:42 AM	Encendido	Automático	Máquinas Virtuales Citrix en Servidor DELL
7:00 PM	Apagado	Automático	Servidor Dell PowerEdge
7:02 PM	Encendido	Automático	Router Linksys WRT54G
2:30 AM	Apagado	Automático	Router Linksys WRT54G

Tabla 2 Horario semanal (Lunes-Viernes)

Horario correspondiente a fines de semana

Horario	Proceso	Tipo	Equi
5:02 AM	Encendido	Automático	Router Linksys WRT54G
11:00 PM	Apagado	Automático	Router Linksys WRT54G

Tabla 3Horario de Fin de Semana

Como nota lo único que no se pudo realizar de forma automática es el encendido del servidor Citrix debido a que no cuenta con la función de *Wake On LAN*, éste lo realiza una persona al llegar a la oficina.

A continuación se describe el proceso de encendido de las máquinas virtuales en Citrix Xen Server en Servidor DELL PowerEdge1

Por default ninguna máquina virtual enciende automáticamente al iniciar el *Xenserver*, es necesario desde la consola del xenserver configurar el *auto_power.*

Paso 1 – Revisamos ID del pool

```
xe pool-list
9195976a-c1ee-523a-1a43-c5f5cd28d6e8
```

Paso 2 – Listamos las máquinas virtuales, para poder tomar los uuid, lo cual nos servirá para automatizar el encendido de las máquinas virtuales.

```
xe vm-list
uuid ( RO): b2a97761-588b-8bb9-92cc-d60980f7455f
name-label ( RW): Debian 6 server
power-state ( RO): halted
```

Paso 3 Establecemos el *auto_power del pool en true*, para que inicie automáticamente, para eso utilizaremos el *uuid* obtenido con anterioridad con *xe pool-list*

```
xe pool-param-set uuid=9195976a-c1ee-523a-1a43-c5f5cd28d6e8 other-config:auto_poweron=true
```

Paso 4 – establecemos el *auto_power* de la máquina virtual en true, para que inicie automáticamente, para eso utilizaremos el *uuid* obtenido con anterioridad con *xe vm-list*

```
xe vm-param-set uuid=b2a97761-588b-8bb9-92cc-d60980f7455f other-config:auto_poweron=true
```

Si por alguna razón queremos evitar que una máquina virtual inicie automáticamente basta con poner false al final en *auto_poweron*

```
xe vm-param-set uuid=b2a97761-588b-8bb9-92cc-d60980f7455f other-config:auto_poweron=false
```

En esta parte describiremos el proceso para apagado automático del servidor DELL PowerEdge 9150, igualmente que el encendido también se aplica en el Citrix Xenserver.

Creación de archivo a ejecutar.

```
[root@xenserver-cojudeq ~]# touch /etc/init.d/shutdown.sh
```

Edición de archivo a ejecutar

```
[root@xenserver-cojudeq ~]# nano /etc/init.d/shutdown.sh
```

Creando el Script a ejecutar

```
#!/bin/bash shutdown -h -P 19:00 &
```

Hay que recordar que guardamos con “o” y salimos con “x”. Estableciendo Permisos para archivo

```
[root@xenserver-cojudeq ~]# chmod 755 /etc/init.d/shutdown.sh
```

Detalles del permiso 755

Octal	Permisos	Pertenece
7	rwx	Usuario
5	rx	Grupo
5	rx	Otro

Tabla 4 Permisos de archivos

Existen otras formas de darle el permiso por ejemplo: chmod +x archivo.sh, pero la forma octal (755) es la que considero menos complicada.

Creando Enlace Simbólico en /etc/rc2.d/

```
[root@xenserver-cojudeq ~]# ln -s /etc/init.d/shutdown.sh /etc/rc2.d/S88apagad
```

Que es /etc/rc2.d/, es el nivel de ejecución del script donde este nivel se considera el inicio del sistema. El nombre S88apagado significa que Script iniciara (Start) con prioridad 88 y el apagado es la descripción.

Ejecutando para probar el Script *Shutdown.sh*

```
[root@xenserver-cojudeq ~]# /etc/init.d/shutdown.sh
```

Verificamos que cargo el Script:

```
[root@xenserver-cojudeq ~]# /etc/init.d/shutdown.sh
```

Daría como resultado:

```
29500 pts/1    00:00:00  shutdown
```

Lo anterior fue desde el punto del servidor DELL que es que contiene el Citrix, ahora describiremos como es que se logra dar el servicio de Internet una vez apagado el servidor Citrix.

Tenemos un equipo APC que cuenta con la función de TIMER que a determinada hora en este caso 07:02 P.M. enciende el equipo Linksys WRT54G que es el que da el servicio de Internet este mismo equipo apaga el equipo a las 02:00 AM del siguiente día y lo encienda nuevamente a las 5:00 am y lo apaga a las 08:30 AM.

Ilustración 20 Equipo APC encargado de realizar el encendido del equipo Linksys

Ilustración 21 Equipo Linksys para

ANEXO 3 Herramientas de apoyo para la resolución de problemas.

Descripción General

Mostraremos a grandes rasgos el uso de algunas herramientas que facilitan la resolución de problemas relacionados con el tráfico que se realiza.

Detalles de las herramientas

Hablaremos un poco de *Ntop*, la cual es una herramienta que permite monitorizar en tiempo real una red. Es útil para saber los dispositivos y aplicaciones que están consumiendo recursos de red en un instante concreto y para ayudarnos a detectar malas configuraciones de algún equipo.

A que nos referimos con malas configuración, ya sea que tenga muchos privilegios, descubrió alguna página o sitio que no esté bloqueado y el cual haga uso de excesivo del Internet o está usando alguna herramienta no permitida.

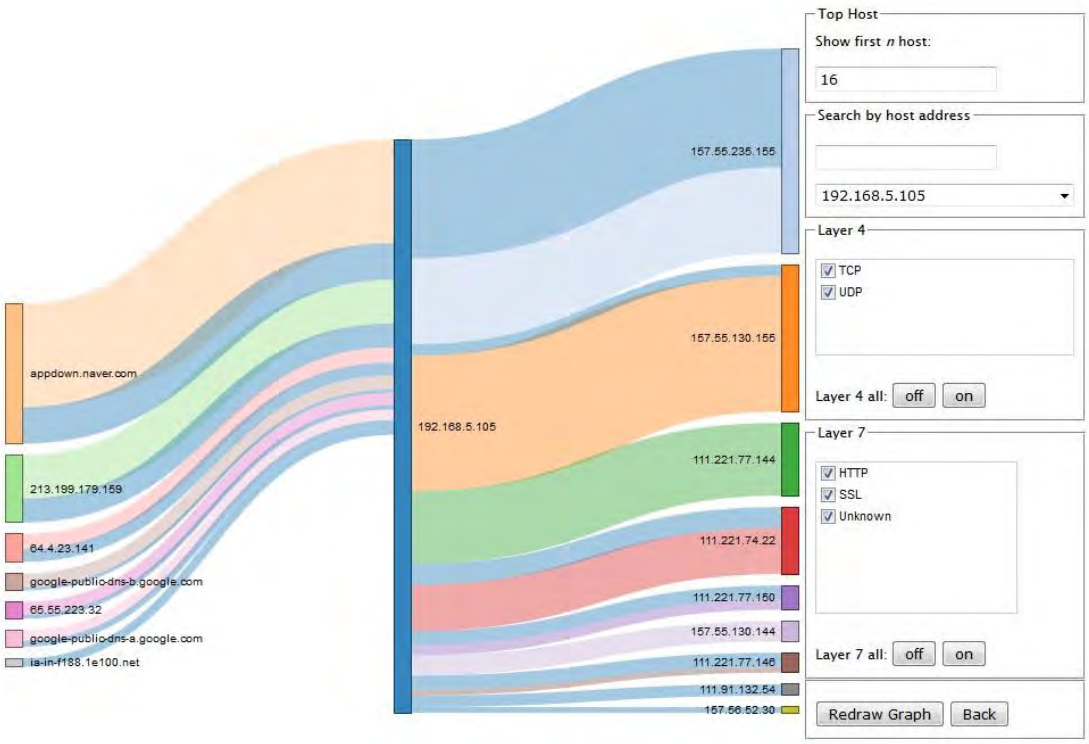


Ilustración 22 Tráfico Generado por equipo de Red

Ntop nos proporciona esta información pero no sabes muy bien a dónde va la información si no tenemos otra herramienta que nos diga quién es el sitio accedido, pero tenemos la IP, en este caso usaremos la herramienta proporcionada por *Hurricane Electric.*

Hurricane Electric es un sitio web donde podemos encontrar información sobre IP, dominios, etc.; con esta herramienta nos apoyaremos para bloquear o permitir correctamente un servicio o dominio.

Como podemos ver tenemos información sobre la página de la universidad (www.uqroo.mx), sin embargo podemos obtener más información como es IP (192.100.164.38).

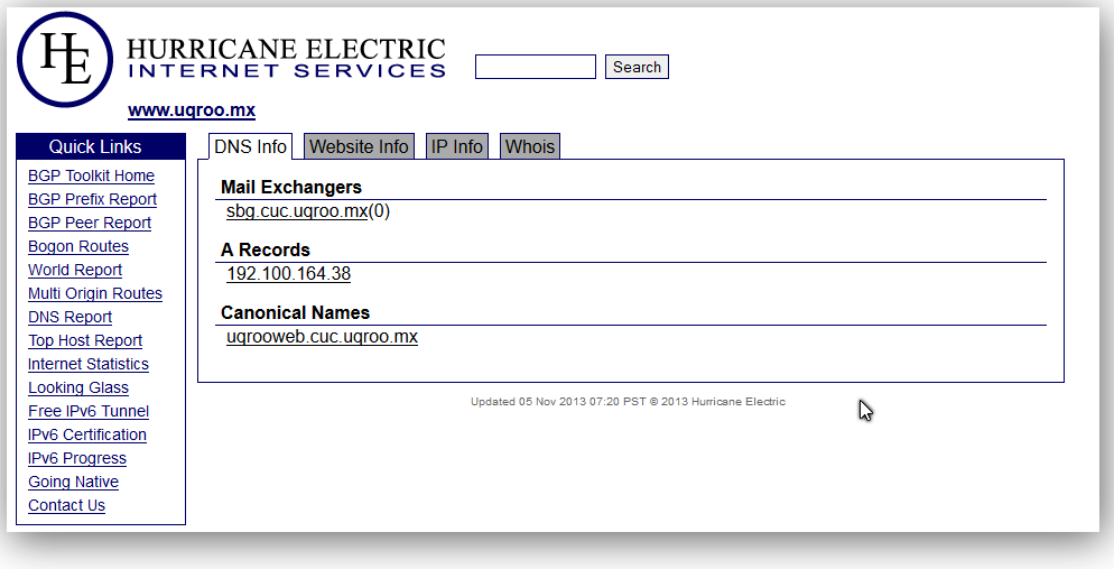


Ilustración 23 : Captura de Pantalla de la página he.net

Si damos clic en la IP obtenemos más información. Como es el *Origin AS (Autonomous System -AS8151*), la RED (192.100.164.0/24) y la descripción que mayormente encontramos a quien pertenece la IP, eso sólo en la pestaña IP Info. (Como se puede apreciar en la siguiente figura).

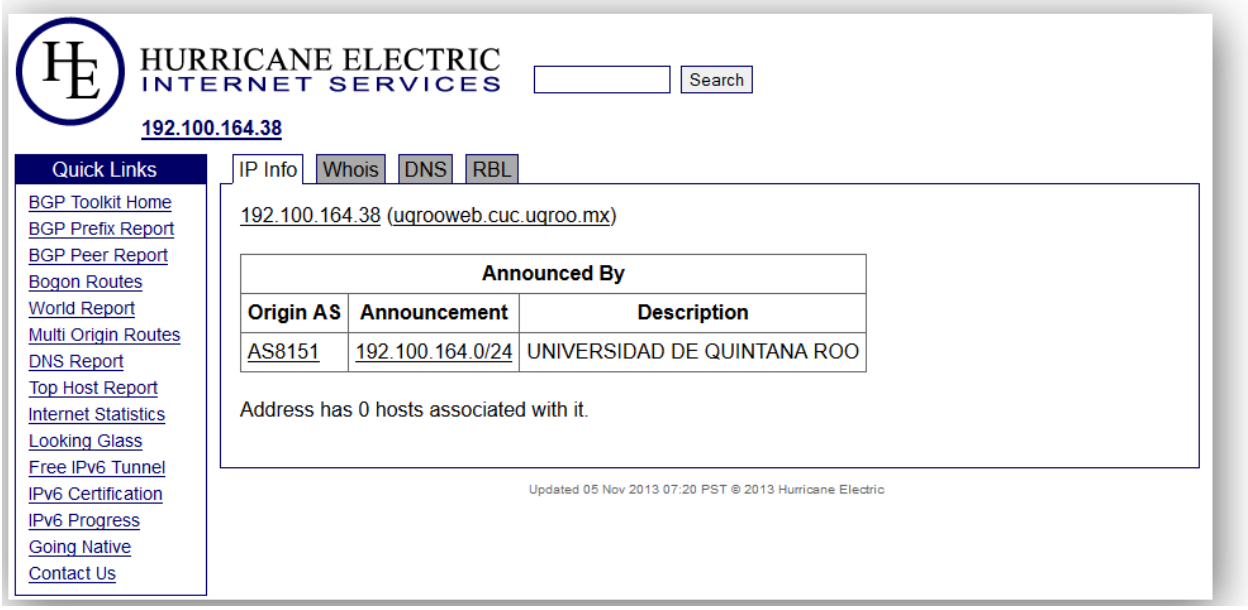


Ilustración 24 Captura de Pantalla de la página he.net Sección IP Info

En la pestaña *Whois* encontramos más detalles sobre la IP

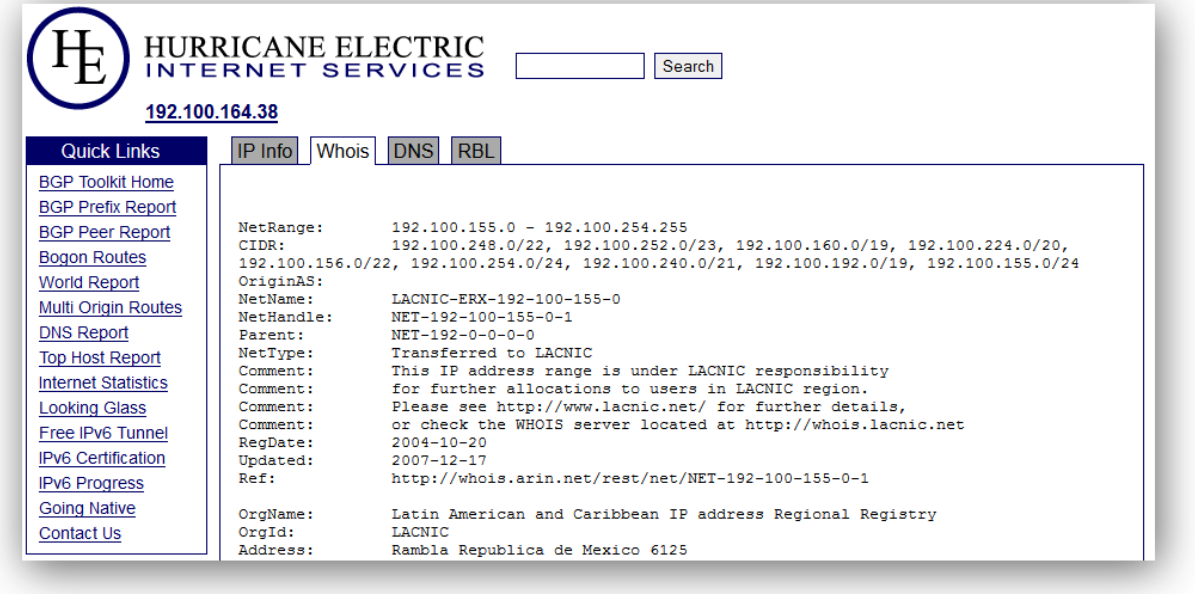


Ilustración 25 Captura de Pantalla de la página he.net sección whois

Una parte interesante es la pestaña RBL (*Realtime Blackhole List*), que se podría considerar como grupo de servidores con listas de sitios que se consideran spam.

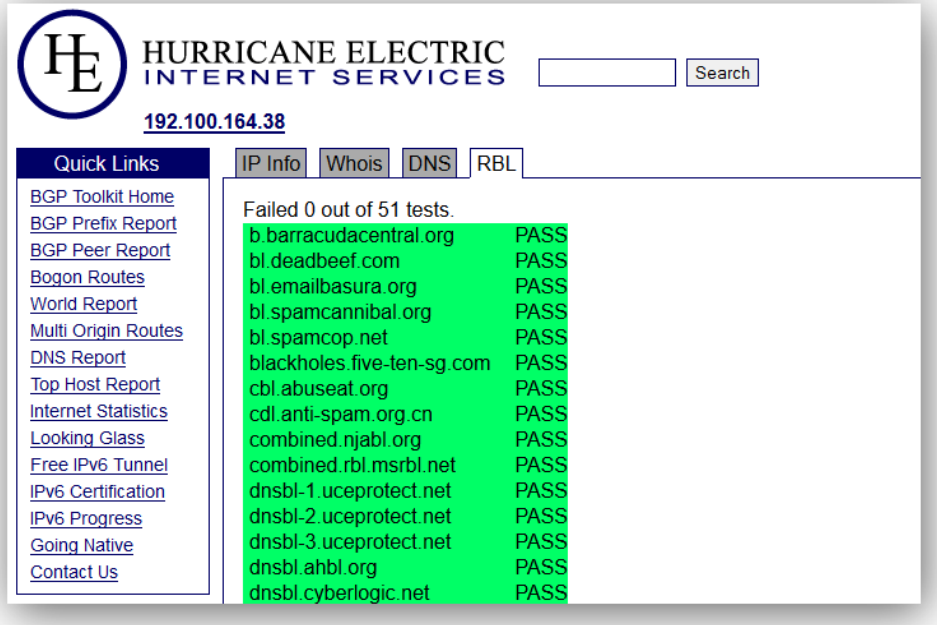


Ilustración 26 Captura de Pantalla de la página he.net Sección RBL

Otra cosa que podemos tomar en cuenta sólo en carácter informativo es la parte de Origin AS (AS8151), de la compañía a Uninet S.A. de C.V.

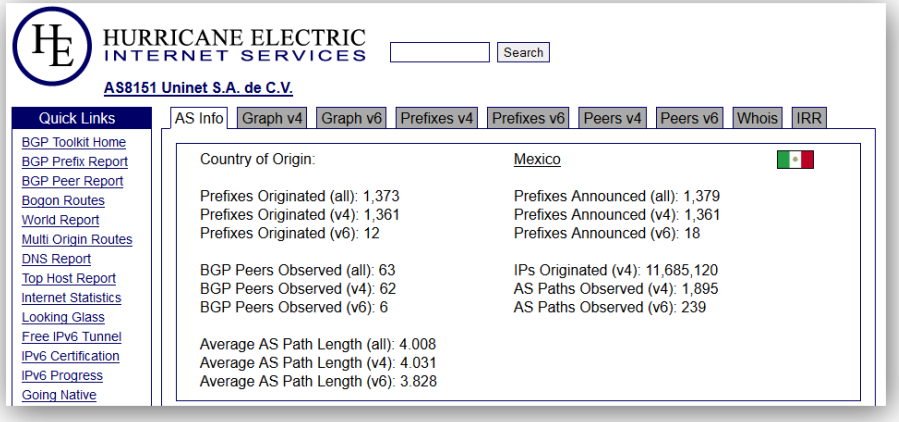


Ilustración 27 Información sobre la AS

En la siguiente ilustración se puede observar la ruta de Propagación IPv4.

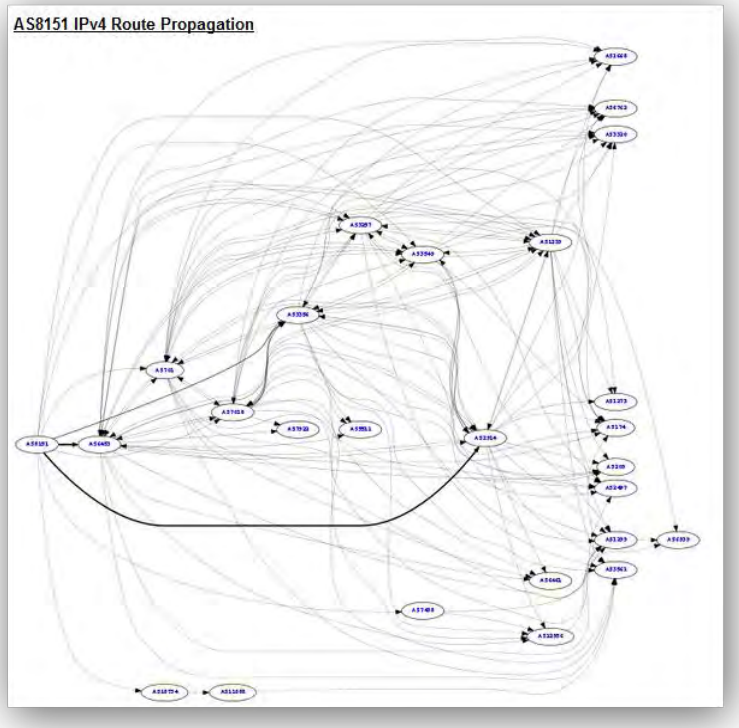


Ilustración 28 Ruta de Propagación IPv4

También nos muestra una ruta de propagación con IPv6

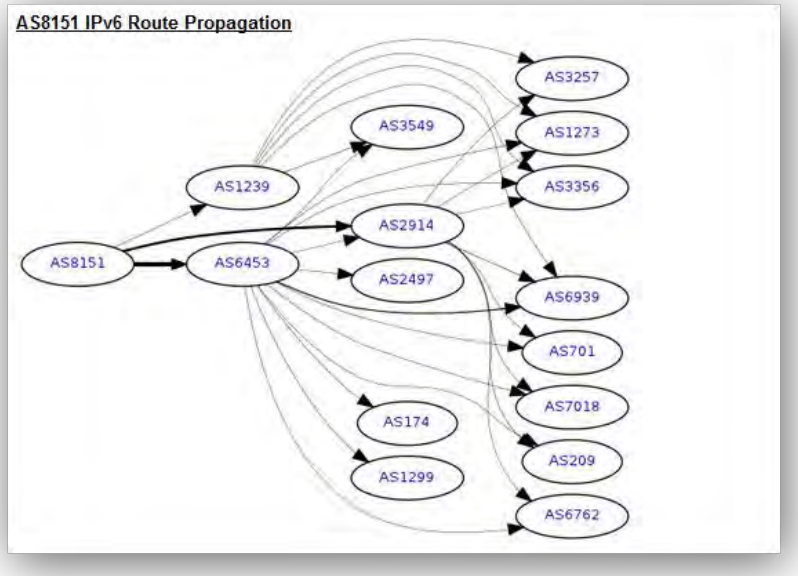


Ilustración 29 Ruta de Propagación IPv6

Hay más información en la página como son las redes que tiene asignadas

192.100.159.0/24	Cent. de Invest. en Quimaca Aplicada
192.100.161.0/24	Universidad Autonoma de Baja California Sur
192.100.162.0/24	Universidad Autonoma de Nayarit
192.100.163.0/24	Universidad Autonoma de Campeche
192.100.164.0/24	UNIVERSIDAD DE QUINTANA ROO
192.100.166.0/24	Instituto Tecnologico de Sonora
192.100.170.0/24	Universidad Tecnologica de la Mixteca
192.100.172.0/24	Instituto Nacional de Astrofisica, Optica y Electronica
192.100.178.0/24	Colegio de Postgraduados

Tabla 5 : Redes Asignadas

En el caso que no sepamos qué tipo de dispositivo está consumiendo el tráfico, existen otras herramientas de mucha utilidad para identificar el fabricante de una tarjeta de red y así poder determinar que dispositivo es, puede ser una PC, Laptop o Teléfono.

La primera página que usaremos será hwaddress.com, donde colocaremos los 3 octetos del fabricante (3C:74:37)

Prefix	Address space	Company
3C:74:37	3C:74:37:00:00:00 - 3C:74:37:FF:FF:FF	RIM

Ilustración 30 Determinando tipo de dispositivo por MAC Address

Observamos que pertenece a RIM (*Research In Motion* Limited) entonces sabemos que es un blackberry puede ser un Teléfono o una Tableta de esta marca. Esta información servirá para determinar si está permitido o no para usar nuestro servicio.

ANEXO 4 Solución de digitalización para el área de recursos financieros

Descripción de la solución de digitalización

Dar la solución a uno de los problemas más comunes e importante como es la digitalización de documentos con la ayuda de servidor FreeNAS el cual esta denominado como almacenamiento de código abierto tiene una licencia BSD, se utilizaron diferentes herramientas con la que cuenta como es CIFS, FTP, permisos y restricciones.

Detalles de la solución de digitalización.

Se implementó un servicio de FTP con el servicio CIFS anteriormente conocido como SMB, el servicio FTP y CIFS es implementado en un servidor FreeNAS debido a que existe mucha documentación, es robusto (no falla en el momento que más se le necesita), originalmente se basó en un sistema Open Source de nombre FreeBSD en su versión 6.0, actualmente la versión para descargar es la 9.2.1.5, pero la implementada es la versión FreeNAS-8.3.1-RELEASE-x64 (r13452)

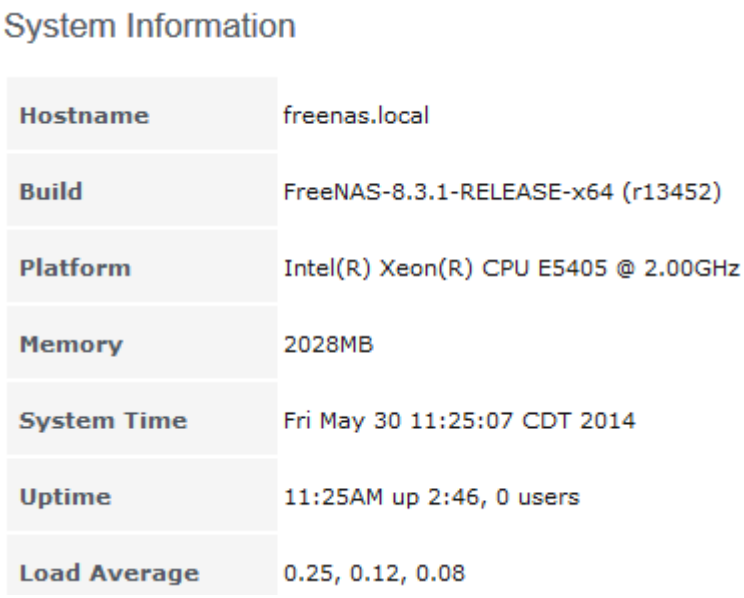


Ilustración 31 Información del Sistema FreeNAS

En este sistema se utilizan 2 disco duros, 1 donde se encuentra la instalación de FreeNAS y 1 donde se guarda la información digitalizada.

Esta es la partición donde se enviarán los datos a digitalizar.

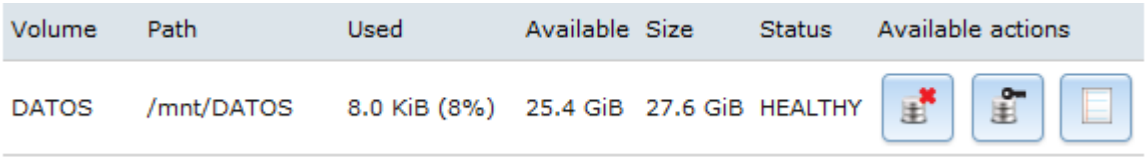


Ilustración 32 Disco Duro donde se almacena las digitalización del scanner

Tenemos dado permisos al disco duro.

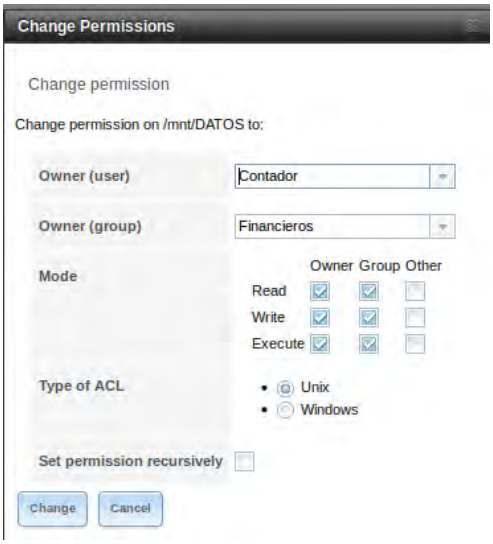


Ilustración 33 Permisos al disco Duro

En este disco duro guardamos la información que genera el scanner con ayuda del servicio del FTP con el que cuenta el scanner.

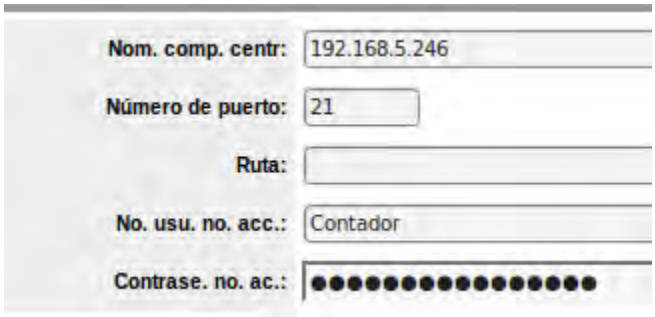


Ilustración 34 Configuración FTP en el Scanner

Pero tenemos una serie de tareas programadas con ayuda del *cron*, el cual apoya a mantener la información del disco

Borra todos menos PDFs	00	Every hour	Everyday	Every month	Everyday	root	find /mnt/DATOS -not -name '*.pdf' -exec rm/-f {} \;

Ilustración 35 Ejemplo de tarea programada: Eliminar archivos con excepción de archivos PDF

Apagado a las 6:55 pm	05	09	Everyday	Every month	Everyday	root	shutdown -h 18:55 "apagado Automatico" &

Ilustración 36 Ejemplo de tarea programada: Apagado automático

En equipos clientes tenemos el disco Duro “Datos” compartidos como una unidad de red y la tenemos restringida por IP de los Clientes aparte del credencial que se necesita para lograr conectar, por cuestiones de seguridad no pondré captura de pantalla de esto.

Describiendo brevemente el FreeNAS tiene FTP y CIFS/SMB, el scanner guarda información en el disco DATOS del FreeNAS por el FTP y los clientes acceden a la información con una Unidad de RED proporcionada por el CIFS/SMB

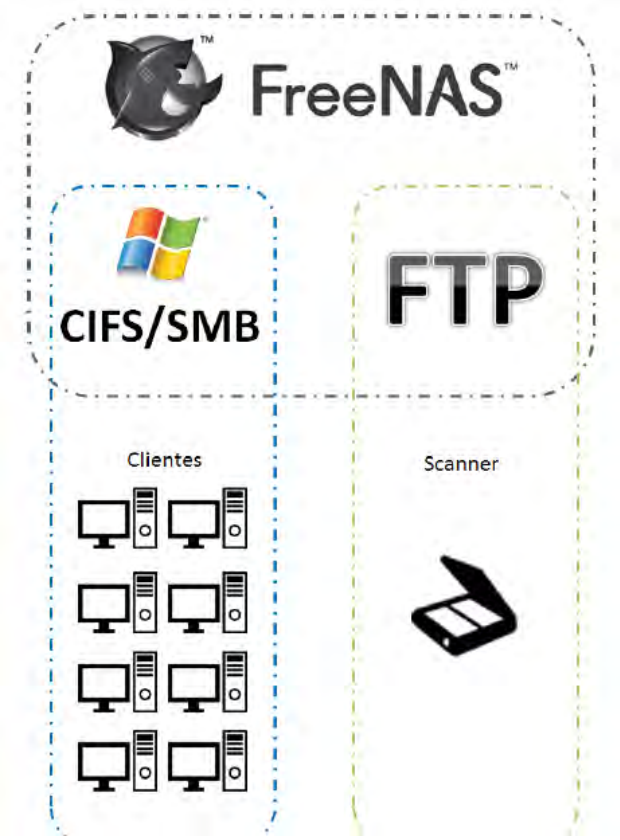


Ilustración 37 Diagrama de Funcionamiento del FreeNAS

Como comentamos los usuarios obtienen la información guardada por el scanner por la unidad de red

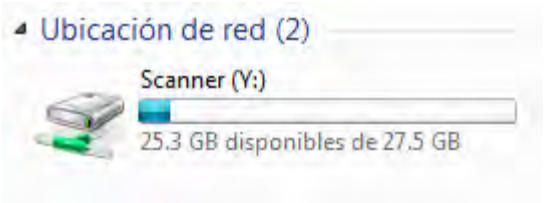


Ilustración 38 Unidad de Red

Vemos como el escanear está guardando la información digitalizada (doc04087920150522170054.pdf)

Ilustración 39 Ejemplo de documento creado en por el scanner

Como vemos este método tal vez parezca más complicado que con *smb* por cliente, la situación es que la cantidad de clientes en esta área es de 16 y ellos cambian sus contraseñas lo que lo hace poco práctico ya que por cada cambio que ellos realicen en sus contraseñas hay que cambiar la configuración dentro del escáner.

ANEXO 5 Uso del administrador de máquinas virtuales Citrix XenCenter

Descripción general

En este apartado hablaremos sobre el uso del XenCenter a grandes rasgos es el administrador grafico para Windows para el Citrix XenServer, hablaremos en ámbito general.

Detalles del uso del XenCenter

Se debe agregar un servidor nuevo una vez instalado la aplicación, dar la IP y dar la contraseña que se estableció al instalar el XenServer.

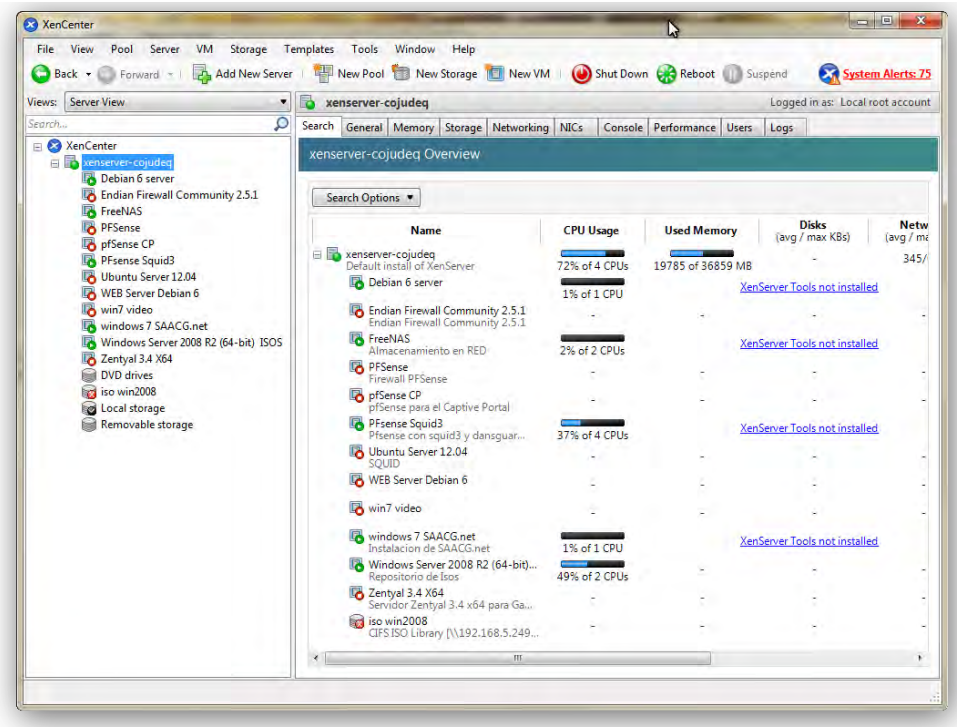


Ilustración 40 Captura del Citrix XenCenter

La lista de los diferentes servidores que hubiéramos vinculado.

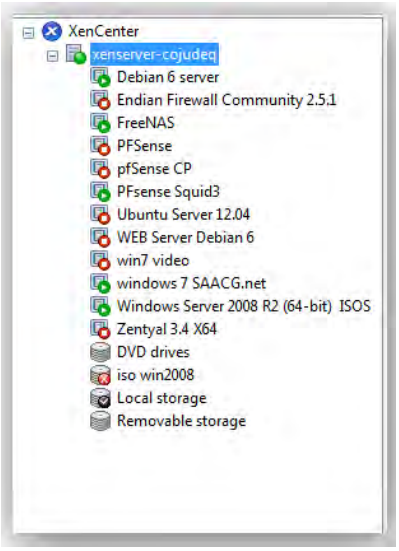


Ilustración 41 Servidor vinculado con sus máquinas virtuales

En la anterior imagen se aprecian unos pequeños iconos de color verde, esto nos indica que son los que están en funcionamiento en ese momento.

Propiedades Generales del Servidor Seleccionado(Ilustración 42 y 43), como es versión del XenServer, información sobre la licencia, IP de administración Memoria, etc.

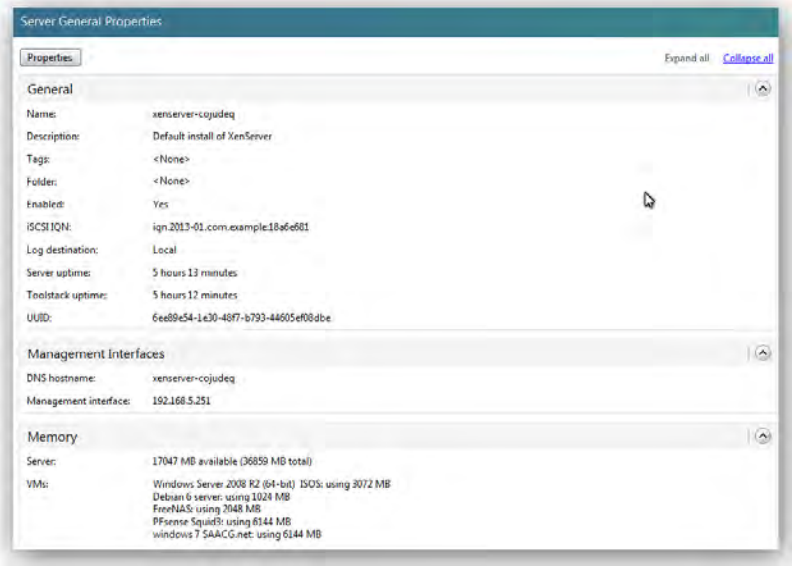


Ilustración 42 Propiedades Generales del Servidor Xen

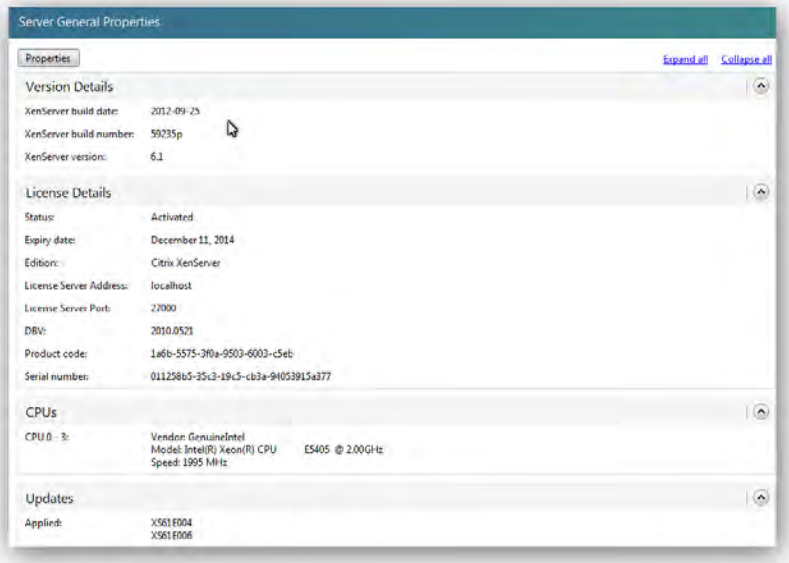


Ilustración 43 Propiedades Generales del Servidor Xen

Una parte importante del XenCenter es la pestaña de las consolas. Ahí podrás hacer cosas que no es posible realizar desde la interface gráfica. En esta parte es donde configuramos aquellas opciones que no están disponibles desde la interface gráfica como el auto *poweron* o *shutdown* personalizados. Los cuales ya hablamos anteriormente.

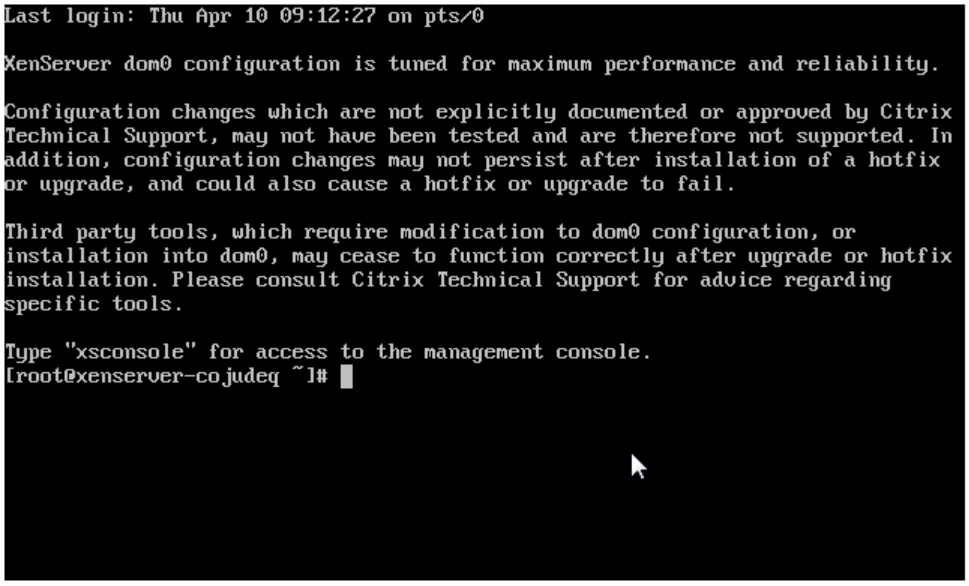


Ilustración 44 Página Inicial de la Consola del XenServer

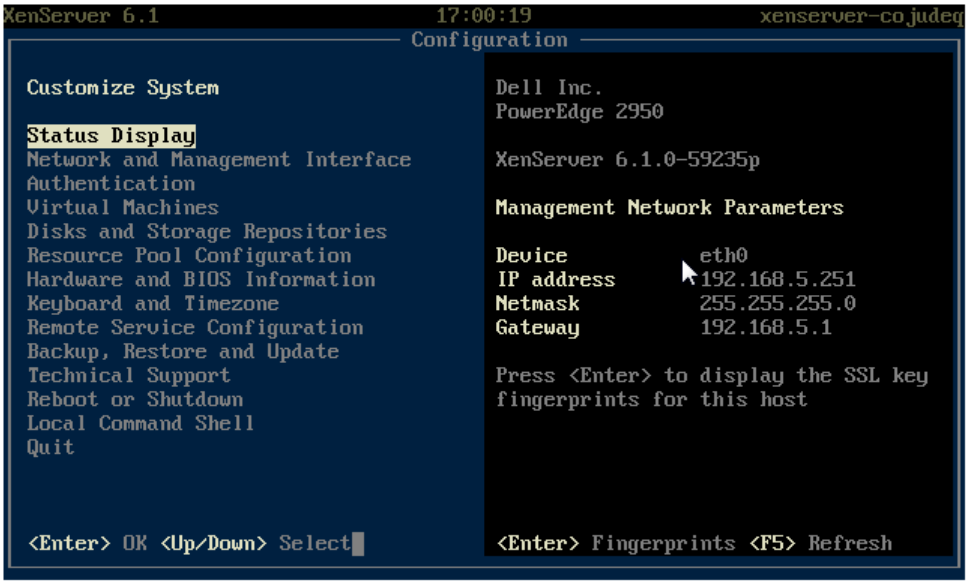


Ilustración 45 Management Console

Anexo 6: Creando una máquina virtual desde el XenCenter

Descripción de la creación de máquina virtual desde el XenCenter

Mostraremos el proceso de creación de una máquina virtual, en este caso de una versión de FreeNAS, desde escoger el medio de instalación hasta establecer la RAM y Procesadores Virtuales.

A continuación se detalla la creación de máquina virtual desde el XenCenter

Creación de una máquina virtual con el XenCenter

En este apartado describimos el proceso de creación de una nueva máquina virtual con XenCenter. Lo primero es desplegar el menú con clic derecho sobre el servidor que queremos crear la nueva máquina virtual (New VM…)

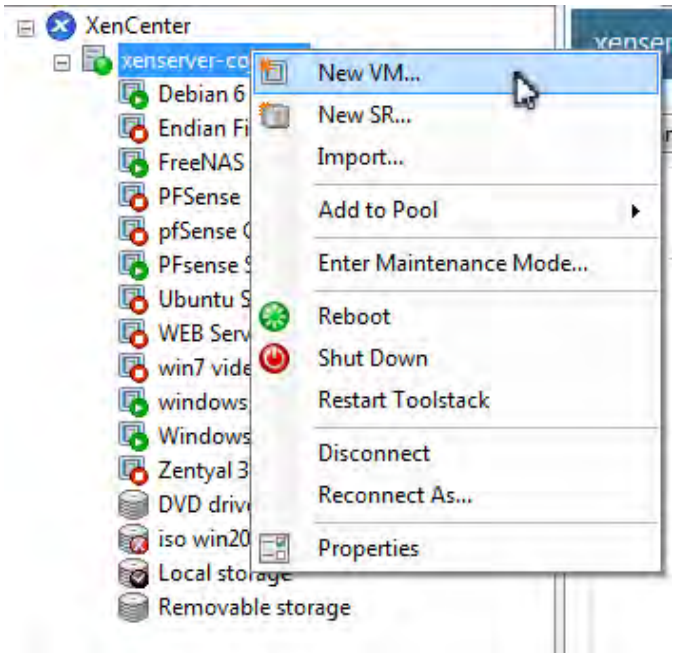


Ilustración 46 Menú del XenServer vinculado desde el XenCenter

En la ventana escogeremos el **template**, por cuestiones prácticas se tomará **el template Other Install media** y una ahí se instala la versión de FreeNAS (versión 8.3.1 x64).

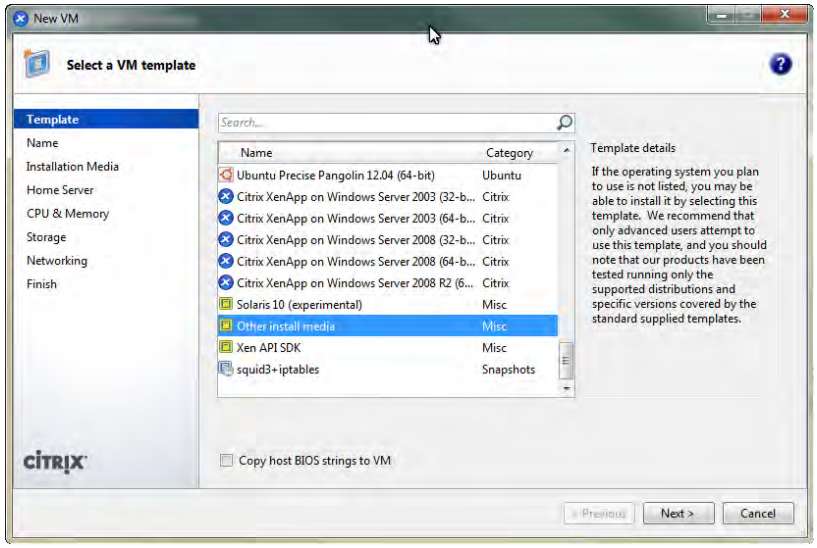


Ilustración 47 Eligiendo el Template para la Instalación

Le pondremos un nombre y una descripción de tal forma que podamos diferenciarlo de las demás.

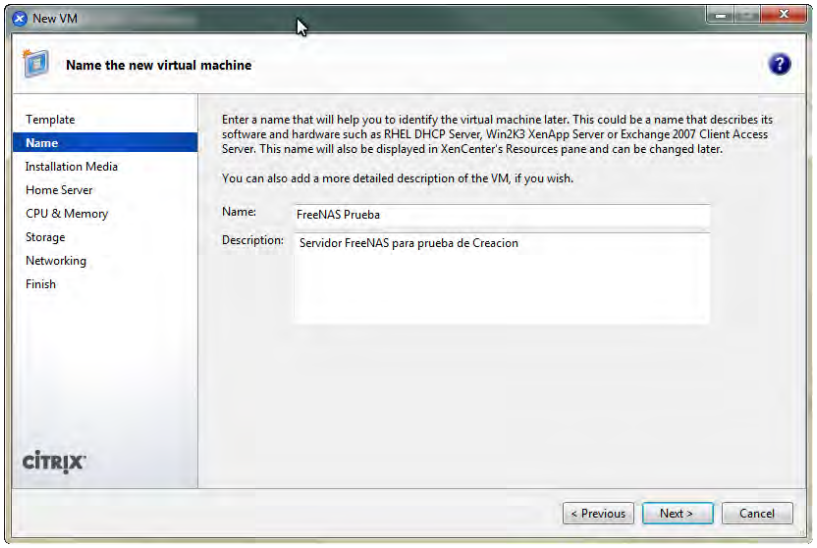


Ilustración 48 Nombre para la nueva instalación

Escogeremos la versión FreeNAS (FreeNAS-8.3.1-RELEASE-x64) como una nota **iso win2008** es un repositorio (Storage Repository) creado en el servidor Windows Server 2008 R2 (64 bits) ISOS en el cual se almacenan imágenes ISO para poder ser usado en la creación de las máquinas virtuales.

Esta es la máquina virtual con la creamos el repositorio de imágenes ISO

Ilustración 49 Eligiendo el repositorio

Escogeremos con que servidor trabajaremos

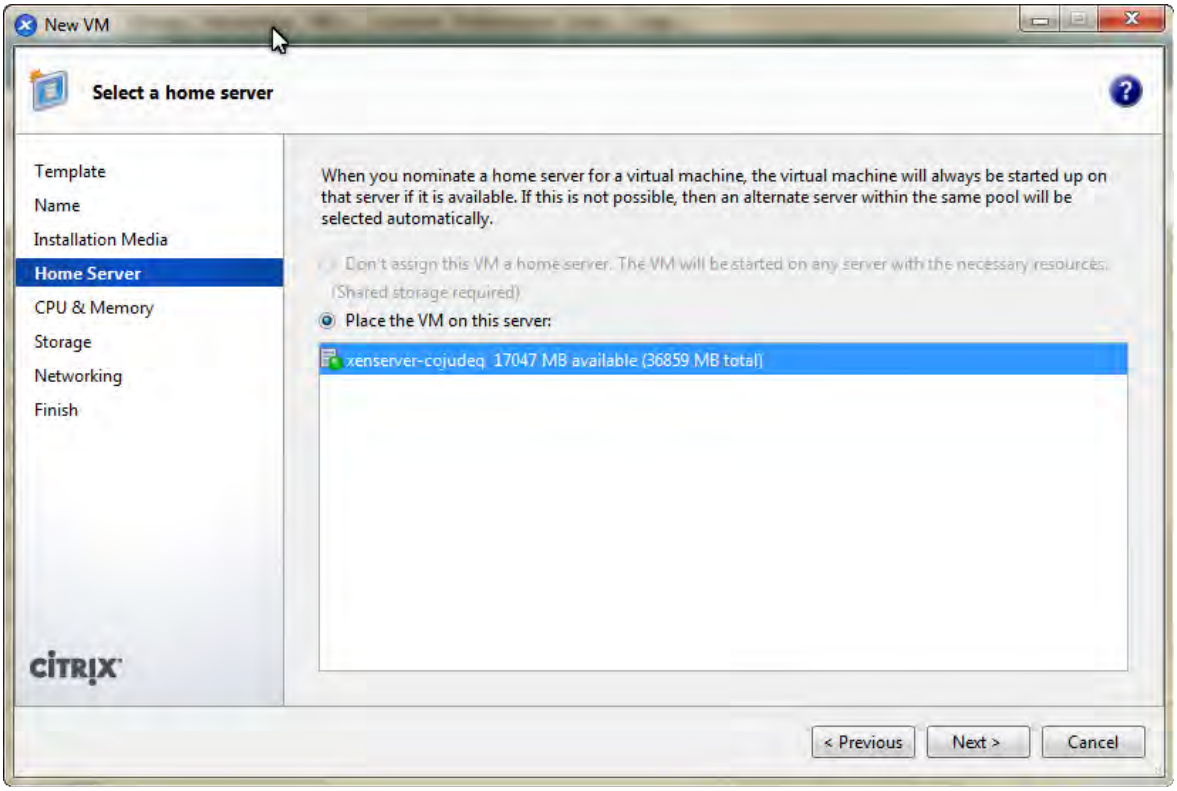


Ilustración 50 Escogiendo el Servidor vinculado

El número de núcleos virtuales, el procesador Xeon que contiene el servidor es de 4 núcleos, así como la memoria el cual contiene 36 GB pero actualmente sólo contamos con 17 para ser usados, como mostraba la ventana anterior.

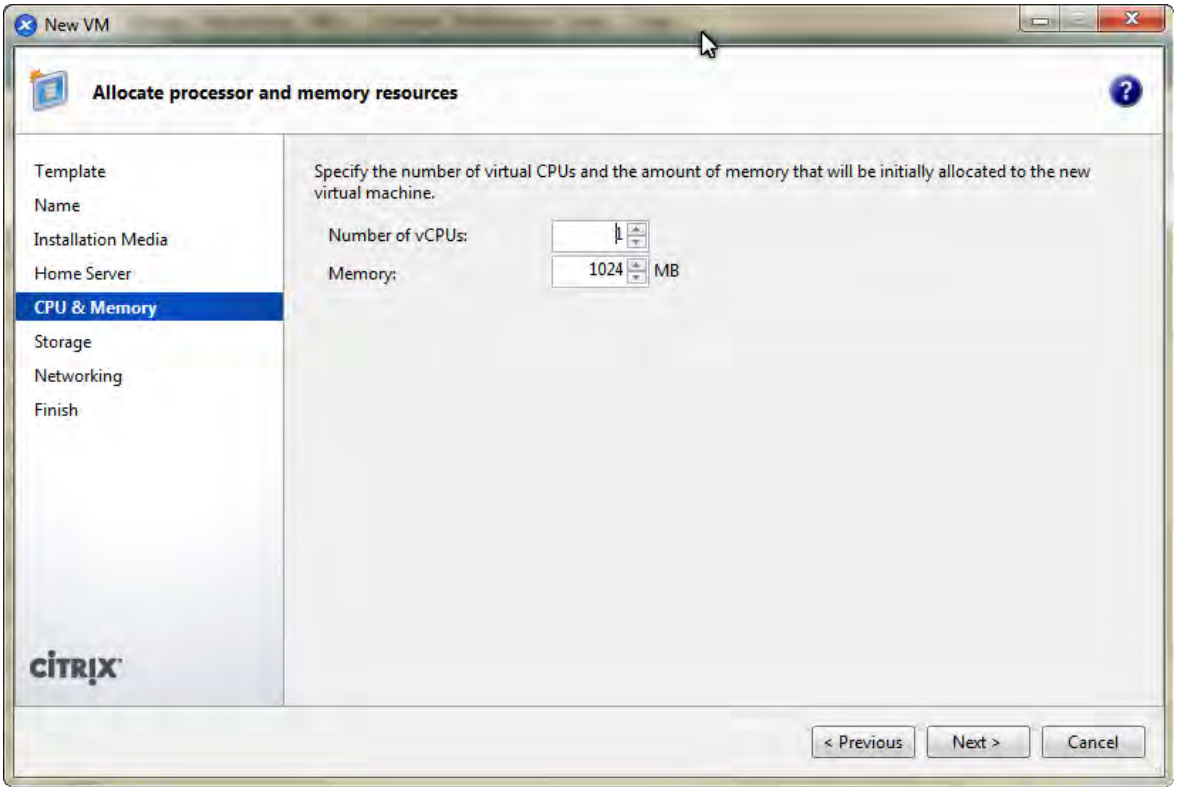


Ilustración 51 Asignando memorias y procesador

Le asignamos el espacio en disco duro (un disco duro virtual) en donde cual servirá solo para instalar el FreeNAS, más adelante tendremos que agregar más discos duros virtuales para dar servicio de almacenamiento.

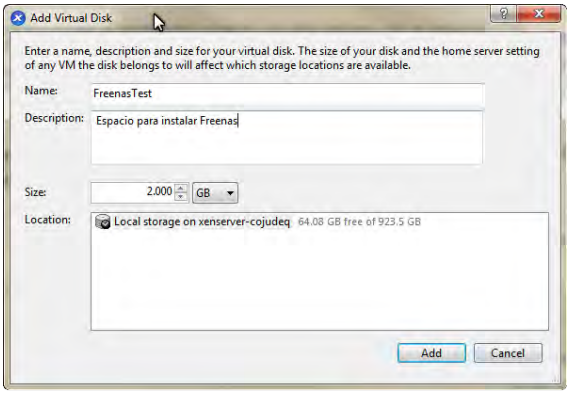


Ilustración 52 Asignando disco duro

El número de Interfaces con las cuales trabajaremos.

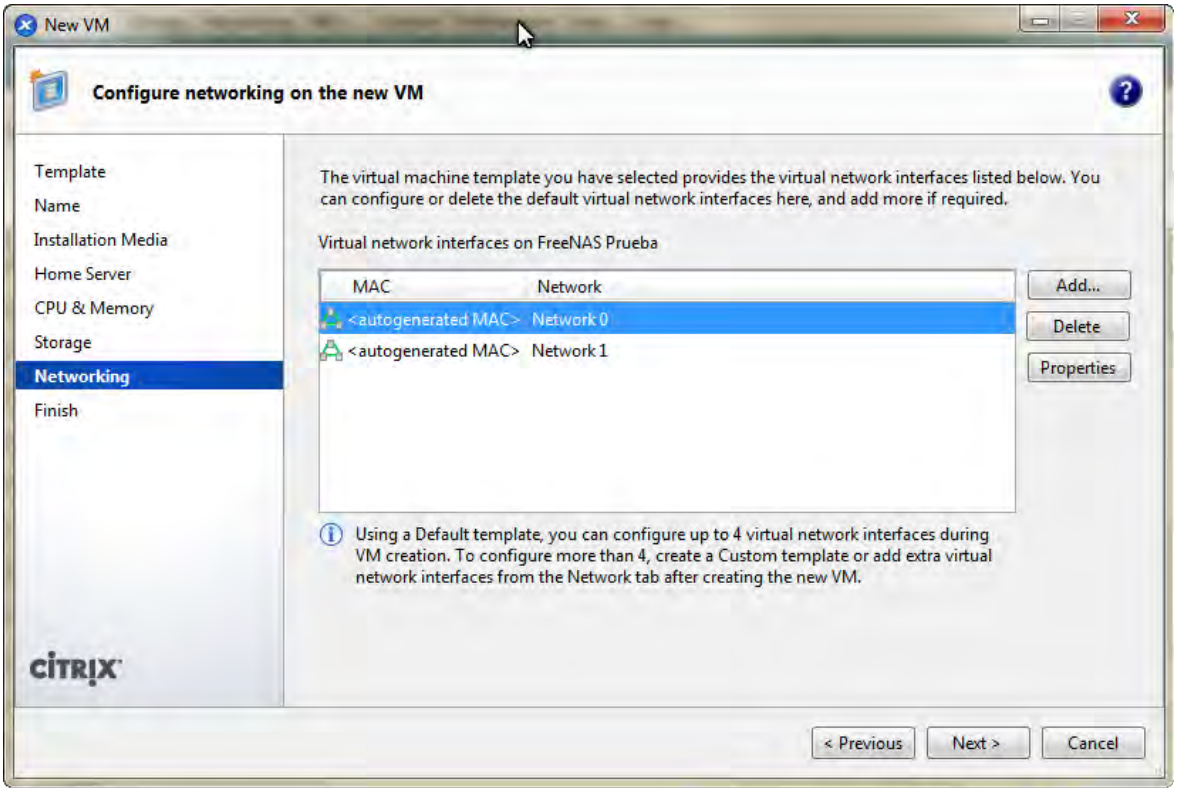


Ilustración 53 Asignando interfaces de Red

Al finalizar nos aparece un resumen de todo lo realizado.

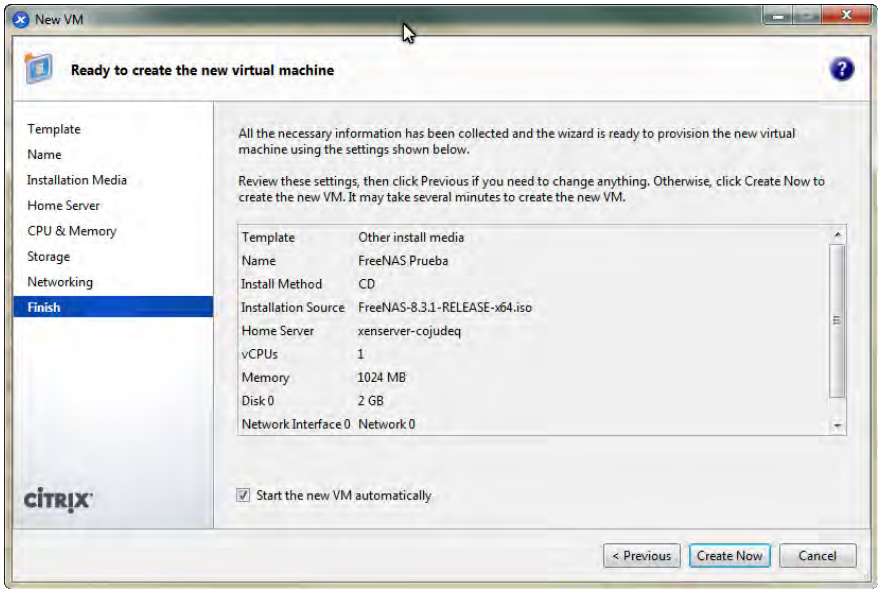


Ilustración 54 Resumen de lo realizado

Al dar en **Create Now** esperamos unos segundos, aparece aun lado en listado la nueva máquina virtual

Ilustración 55 Máquina virtual generada

Al hacer clic en la máquina creada, aparecerán las pestañas para información y manipulación.

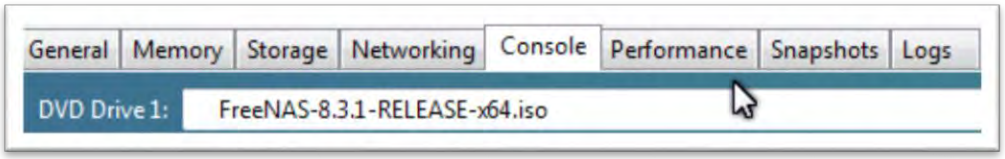


Ilustración 56 Pestaña consola de la máquina virtual generada

Como observamos al seleccionar la imagen ISO del FreeNAS, es montada a una unidad de DVD virtual.

En la ventana de consola aparece la pantalla de instalación como si estuviéramos frente al monitor. Todas las máquinas virtuales tienen consola.

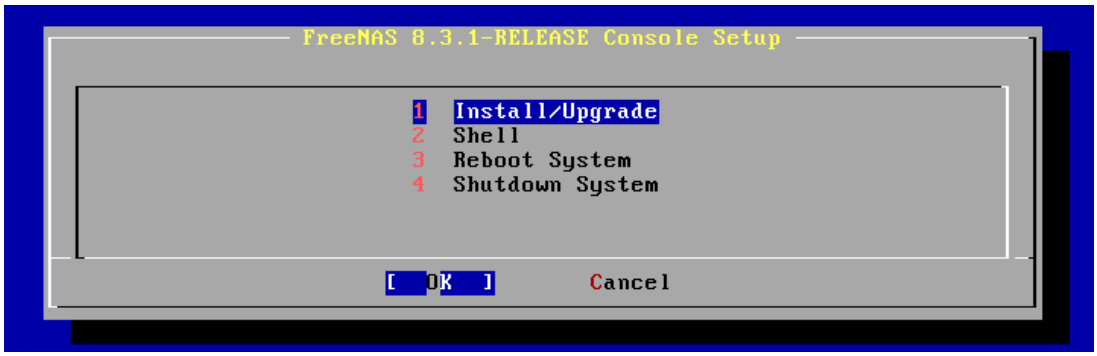


Ilustración 57 Instalación inicial de freeNAS mostrada desde la consola

Después se continúa con la instalación según el servidor o sistema a instalar. Es de gran importancia que los repositorios donde están las imágenes ISO sean accesibles.

Anexo 7: Servidor Debian 6 con servicio de DHCP

Descripción general

Asignación de direcciones automáticas con el servicio de DHCP a equipos permitidos, así como asignaciones de direcciones estáticas a equipos determinados, siendo que el servicio DHCP proporcionado por el pfSense es bueno pero inflexible, ya que tiene todo establecido y no te permite configuraciones personalizadas.

Detalles del Servidor DHCP

Un servicio de DHCP implementado en Debian 6.0 para tener un mejor control y flexibilidad al momento de la asignación de configuraciones y denegación de dispositivos conectados a la red.

Se escoge como sistema el Debian 6.0 debido a que existe mucha documentación referente a la implementación de servicios, así como es una plataforma Open Source el cual no requiere de licencias y tiene una reputación de ser de los sistemas más estables para la implementación de servicios. Esto también está pensado para que un futuro se pueda implementar otros servicios en esta plataforma como podría ser el gestor Nagios o un BIND, junto con este servicio de DHCP se instala el administrador sistema Webmin, el cual consiste en una interface web en donde se pueden instalar, administrar y manipular los servicio y ficheros del servidor de manera remota (vía web), debido a la gran importancia que tiene Debian existen paquetes ya listo para éste.

Ilustración 58 Menú principal de página webmin

Ilustración 59 Paquete .deb descargado para Debian 6

Se instala este servicio debido a se puede administrar de manera remota el servicio de *DHCP*.

Ilustración 60 Server instalados en el Debian 6

Pero por cuestiones prácticas es una excelente aplicación para manipular el fichero de configuración del DHCP para de manera rápida asignar o denegar el servicio de DHCP.

Ilustración 61 Botón de edición manual

Debido a que la interface web contiene muchas partes que hay que llenar para terminar un proceso de asignación o denegación.

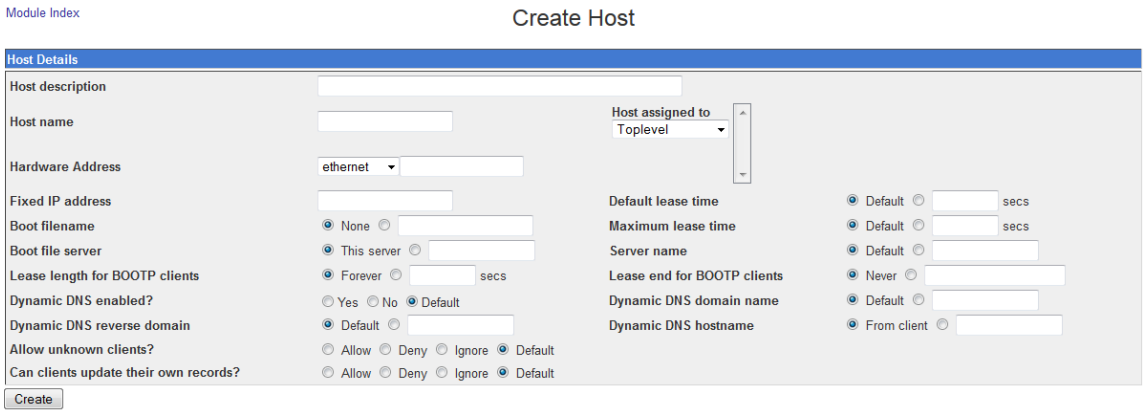


Ilustración 62 Modo gráfico para crear una IP en el DHCP

De manera manual sólo hay que poner unas cuantas líneas, guardar:

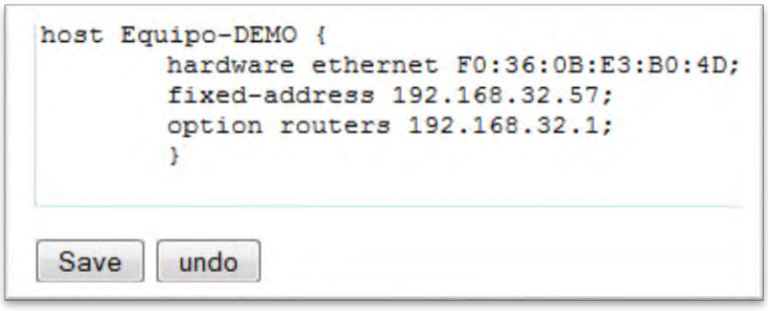


Ilustración 63 Creando una asignación en DHCP

Por último después de haber guardado aplicar los cambios, el cual detendrá y reiniciará el servicio ya con la nueva configuración:

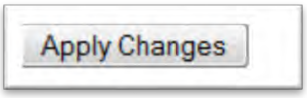


Ilustración 64 Botón para aplicar los cambios

Si existe algún problema ya sea una dirección MAC repetida, con mala estructura de las sentencias o sintaxis errónea al momento de aplicar, nos marcara un error.

Anexo 8: Gráficas y Estadísticas de pfSense

Descripción general

Una de las partes más importantes de un sistema es el uso de las gráficas y estadísticas para saber que está sucediendo tanto en el mismo como el servicio que se provea.

Detalles de gráficas y estadísticas de pfSense

Las gráficas que se mostraran consisten en las generadas por el *ntop*, las RRD del propio pfSense.

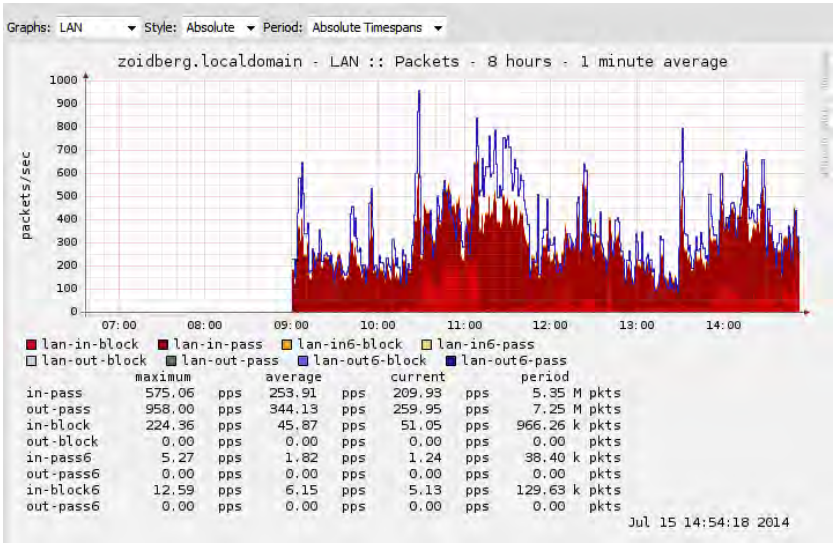


Ilustración 65 Gráfica del tráfico de paquetes en 6 horas

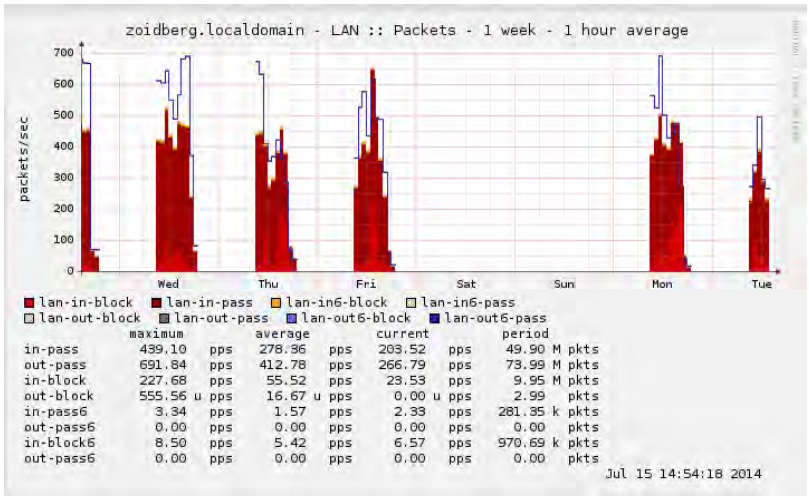


Ilustración 66 Gráfica del tráfico de paquetes por semanas

Con la Ilustración 66 podemos ver que el día sábado y domingo no se ofrece el servicio de Internet con el pfSense si no con un router linksys que se explicó anteriormente.

La siguiente gráfica muestra el tráfico de paquetes por mes:

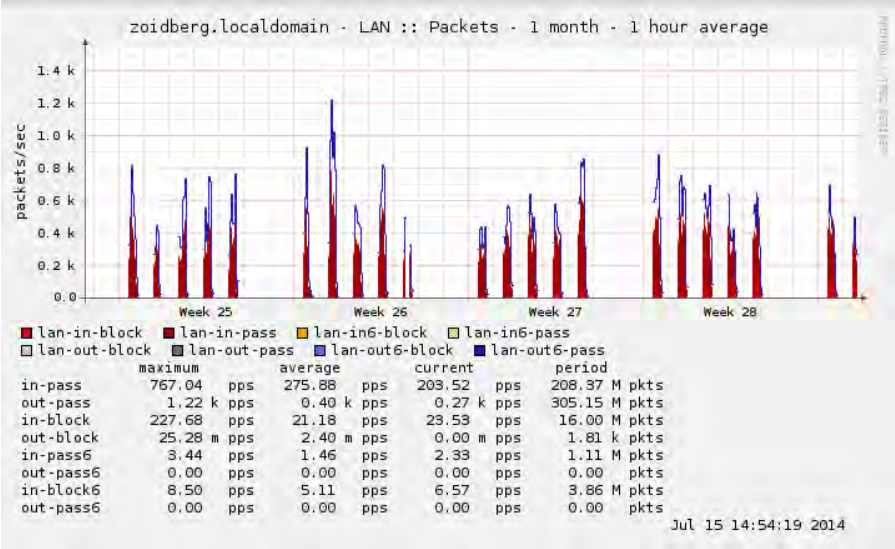


Ilustración 67 Gráfica del tráfico de paquetes por mes

Como vemos en la Ilustración 67 que corresponde al tráfico de paquetes por mes, observamos que los días con menos tráfico son miércoles y jueves y los días con mayor demanda son los días lunes y martes.

Las siguientes Ilustraciones (68 y 69) consisten en el tráfico monitoreado en la interface LAN, en donde el análisis consiste en 7 horas de tráfico (9:00 hrs a 15:00 hrs) vemos que el máximo de tráfico de salida (bajada desde vista del usuario) en IPv4 es de 10.43 Mb/s y el máximo de entrada (subida desde vista del usuario) es 1.10 Mb/s, pero el promedio es salida (bajada desde vista del usuario) promedio en IPv4 es de 3.31 Mb/s y el máximo de entrada (subida desde vista del usuario) es 0.29 Mb/s, como vemos en este periodo de 7 horas se bajaron un 8.84 GB por parte de los usuarios y se subieron 782.4 MB.

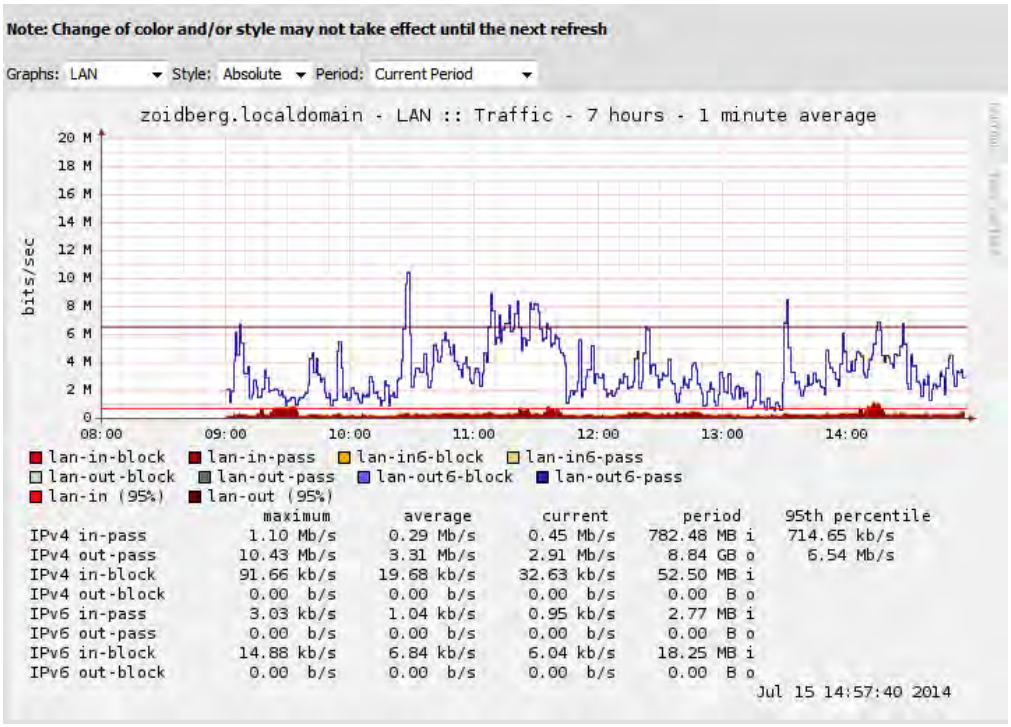


Ilustración 68 Gráfica de 7 horas (9:00 hrs a 15:00 hrs) de Tráfico

Esta gráfica (Ilustración 68) es por 1 mes, vemos que el máximo de tráfico de salida (bajada desde vista del usuario) en IPv4 es de 9.67 Mb/s y el máximo de entrada (subida desde vista del usuario) es 1.06 Mb/s, pero el promedio es salida (bajada desde vista del usuario) promedio en IPv4 es de 4.10 Mb/s y el máximo de entrada (subida desde vista del usuario) es 0.31 Mb/s, como vemos en este periodo de 1 mes se bajaron un 212.28 GB por parte de los usuarios y se subieron 15.93 GB.

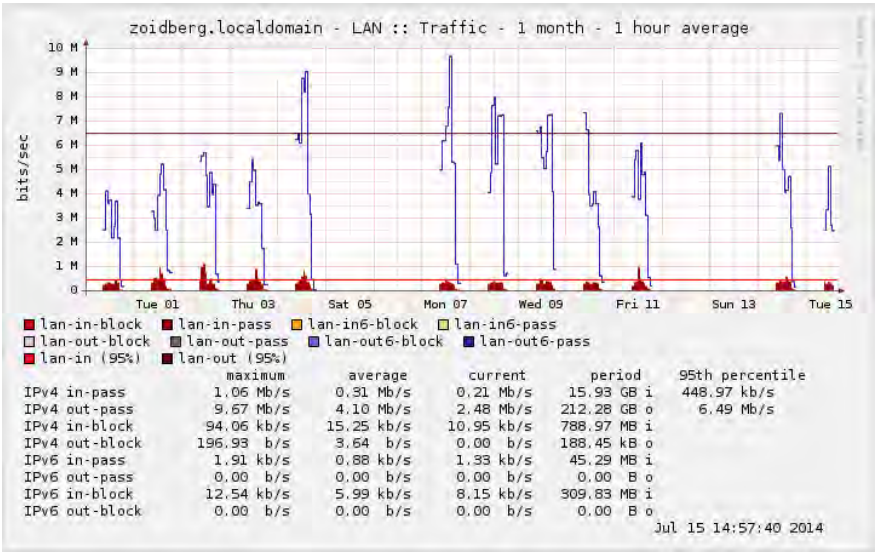


Ilustración 69 Gráfica por mes

Otra parte importante es el LOG del sistema donde podemos ver casi todo lo que sucede

con el pfSense.

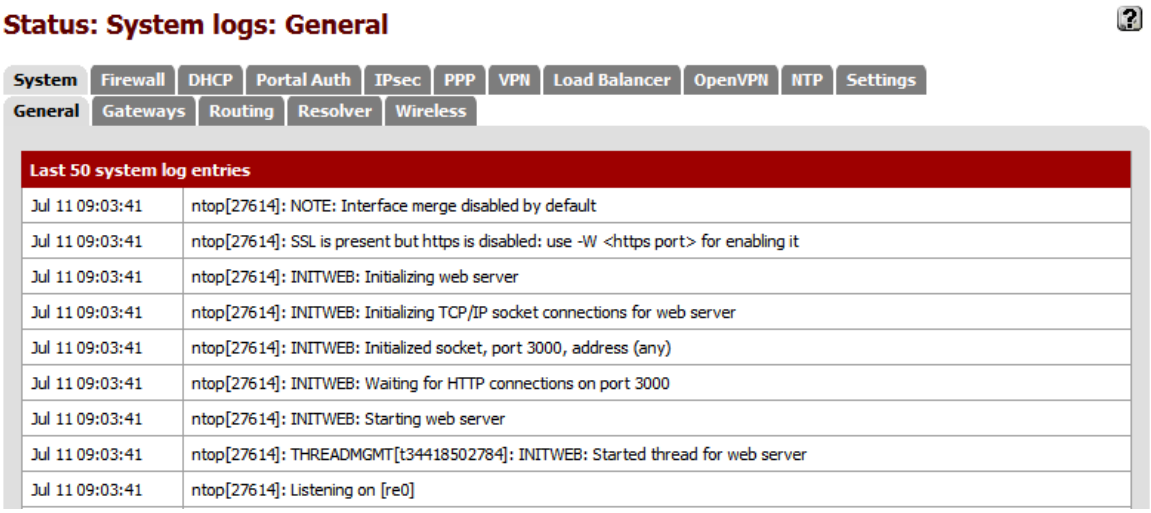


Ilustración 70 Log general del Firewall

Otra parte de importancia para saber si algún dispositivo está abusando o que está visitando el dispositivo es el *log* del *firewall.*

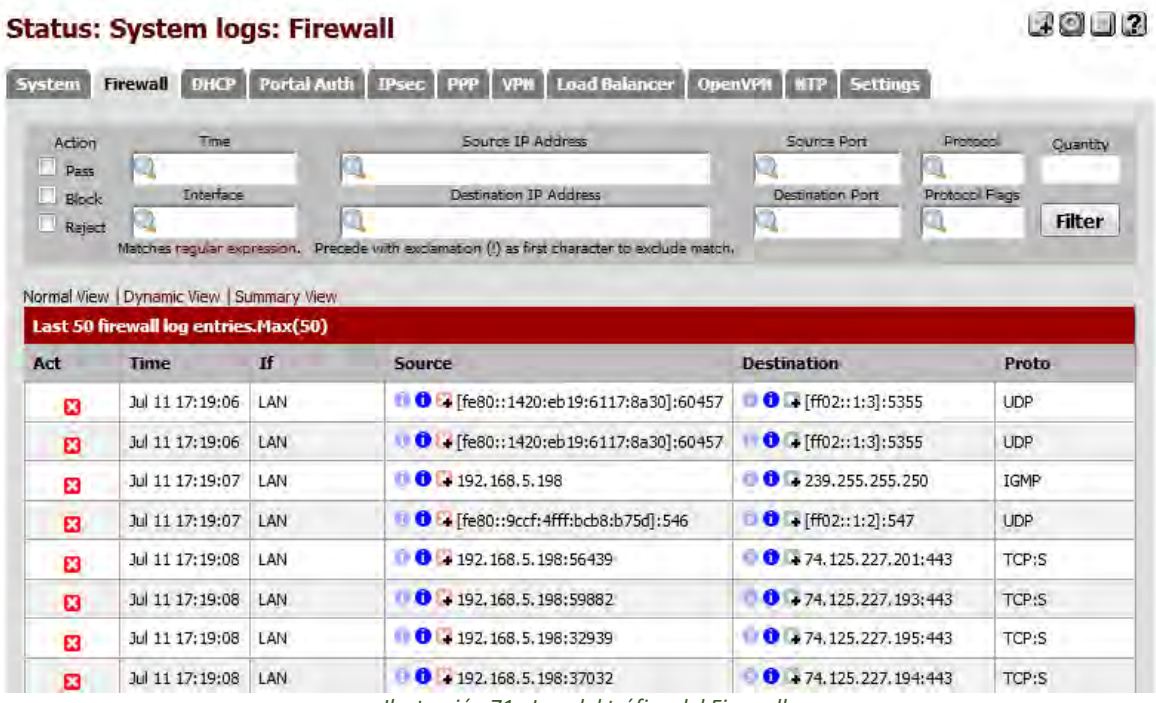


Ilustración 71 : Log del tráfico del Firewall

Si observamos en la imagen la IP 192.168.5.198 tiene un destino 74.125.227.201, por un puerto seguro (443).

La IP 74.125.227.201 es de del dominio de Google, este reconocimiento se puede realiza desde la página tcpiputils.com (http://www.tcpiputils.com/browse/ip- address/74.125.227.201).

Ilustración 72 Información proporcionada por tcpiputils

También podemos usar otra página con la que hablamos anteriormente he.net (http://bgp.he.net/ip/74.125.227.201#_ipinfo).

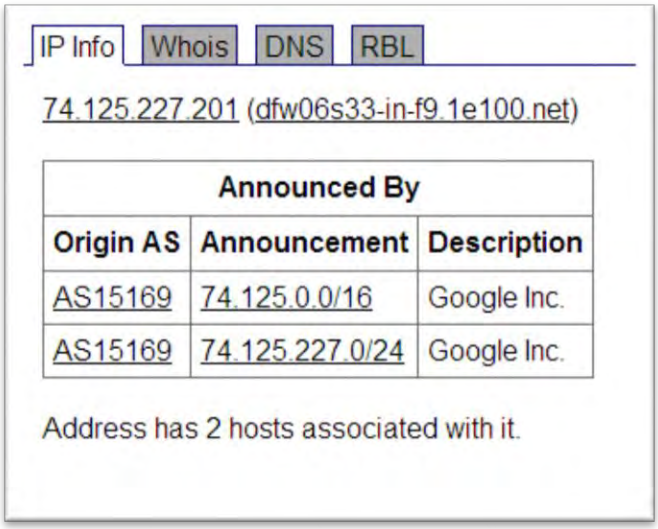


Ilustración 73 Información proporcionada por he.net

Ahora hablaremos un poco de las gráficas generadas con el *ntop, l*a gráfica (Ilustración 73) de los protocolos, como observamos nos muestra los protocolos que se usan en la red, en gráfica de pastel para comprender un poquito mejor, donde observamos claramente que los más requerido es HTTP seguido de SSL.

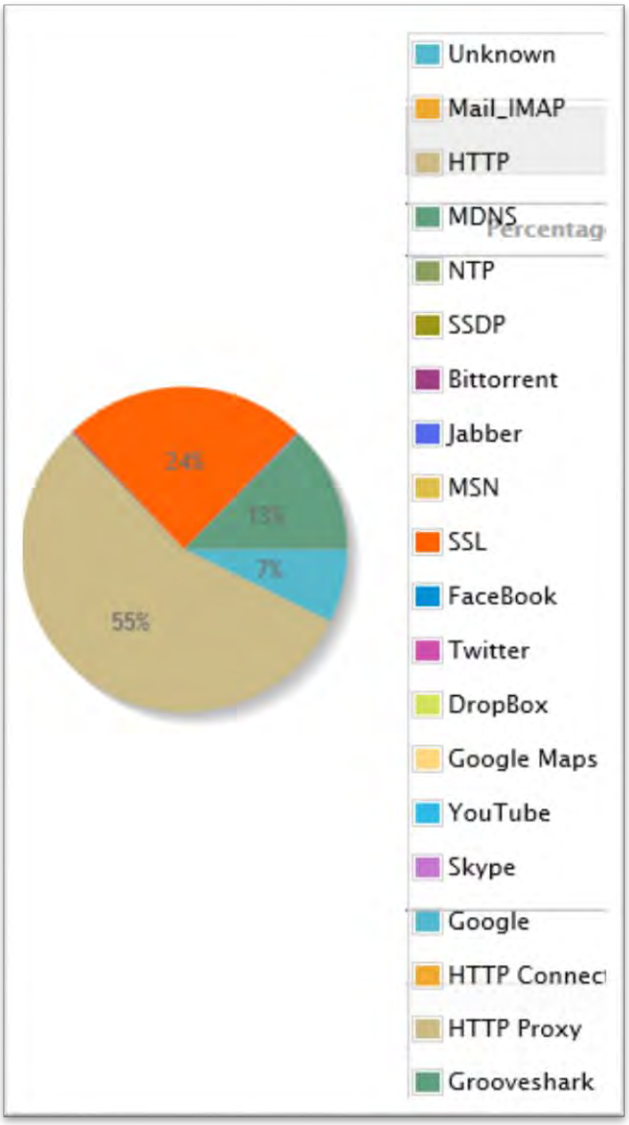


Ilustración 74 Gráfico de Pastel de protocolos generada por el Ntop

Otra gráfica (Ilustración 75) es la Hosts World Map que es de utilidad para saber si algún equipo está haciendo uso de alguna aplicación no autorizada que mayormente se conecte a servidores de Rusia o China.

Ilustración 75 Gráfica de Host World Map generado por el Ntop

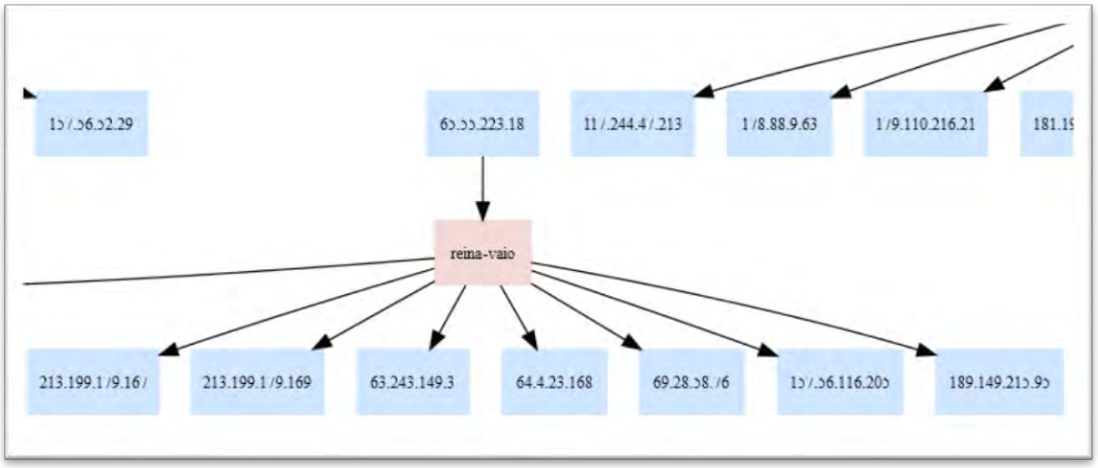


Ilustración 76 Gráfica de Comunicación entre Direcciones IP

Esta gráfica (ilustración 76) nos sirve para ver que IPs están siendo visitadas con más frecuencias, con esto podemos saber si hay un sitio de películas o una página no permitida está siendo visitada incluso si se está descargando algo desde servidores como mega o 4shared.

Anexo 9: Fechas de instalación de sistemas

Descripción general

La estabilidad es una de las características de los diferentes servidores con los que sean trabajados.

Detalles de la fecha de instalación de sistemas

Usaremos un comando *ls* y un *tail (ls -lct /etc | tail -1 | awk '{print $6, $7, $8}')* que determina la fecha del archivo más antiguo en la carpeta */etc*, con esto determinamos la fecha de instalación del sistema. Servidor Debian 6.0

```
root@debianserver:~#  ls -lct /etc | tail -1 | awk '{print $6, $7, $8}'
may 24 2012
```

Este servidor(Debian 6) podríamos decir que es el más antiguo, es más antiguo que el servidor Xen, debido a que el servidor Xen fue migrado de una instalación anterior.

Firewall pfSense:

```
$8}' [2.1-RELEASE][root@zoidberg.localdomain]/root(1): ls -lct /etc | tail -1 | awk '{print $6, $7, Oct
28 2013
```

Este servidor fue actualizado debido a que la versión 2.0.3 contenía algunos *bugs.*

Servidor FreeNAS

```
[root@freenas] ~# ls -lct /etc | tail -1 | awk '{print $6, $7, $8}' Mar
16 2013
```

Esta versión sólo se ha instalado una vez y no se ha actualizado debido a que la versión actual nos es suficiente para las tareas diarias.

Servidor Citrix XenServer.

```
[root@xenserver-cojudeq ~]# ls -lct /etc | tail -1 | awk '{print $6, $7, $8}'
Jan 22 2013
```

Como vemos la versión fue instalado en Enero del 2013 más de un año a la fecha actual esto demuestra la estabilidad del sistema Citrix XenServer. Se realizó una nueva instalación del XenServer debido a que la versión anterior que se utilizaba la 5.6 presentaba incompatibilidad con algunas versiones nuevas de los sistemas operativos que utilizamos para las instalaciones.

Anexo 10: Herramientas lógicas para diagnóstico de hardware

Descripción general

El uso de herramientas o utilidades por software para resolver problemas comunes es algo que debería hacerse antes de brindar un diagnóstico, ya que al no realizarlo podemos caer en el inconveniente de que el problema no quede resuelto, generando atrasos en la entrega de los equipos o gasto innecesario de piezas. Por eso se describirán algunas herramientas que aunque sencillas son de gran utilidad al momento de determinar algún problema.

Detalles de Herramientas lógicas para diagnóstico de hardware

Uno de los problemas comunes que se puede presentar en una computadora es que los archivos se corrompan, no se puedan copiar, que se reinicie el equipo sin previo aviso, que se congele el sistema e incluso se pierda información al momento de guardar algún archivos con los que estemos trabajando.

HD Tune 2.55.

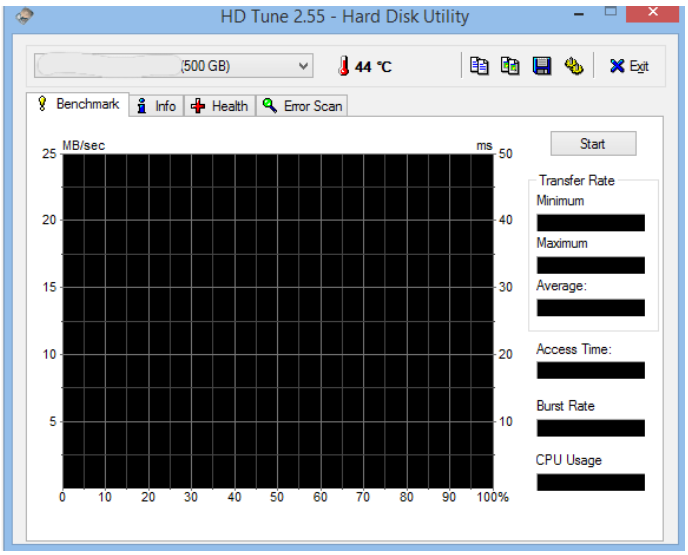


Ilustración 77 Pantalla Principal de HD Tune 2.55

Que es una utilidad que permite saber la salud del disco duro, escanear los sectores del disco y ver información del S.M.A.R.T y que notifique la detección de algún problema. La siguiente ilustración muestra al *HD Tune 2.55* una vez que terminó el análisis de un disco duro de 500 GB, donde no marca errores, aparentemente.

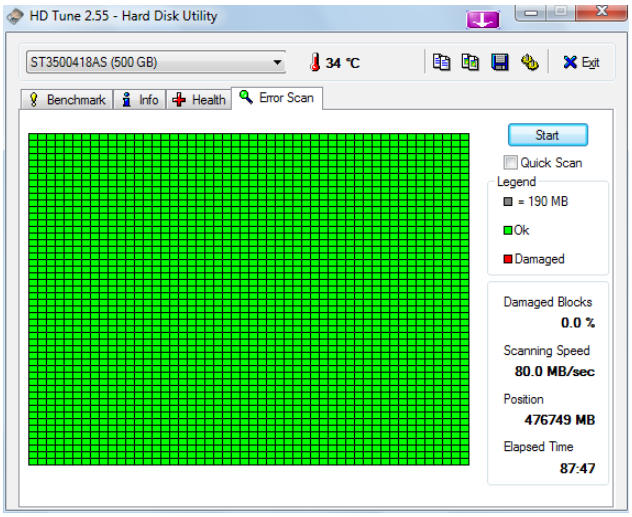


Ilustración 78 Error Scan del HD Tune 2.55

Pero si revisamos la parte del Health S.M.A.R.T si se presentan errores. (Ilustración 79).

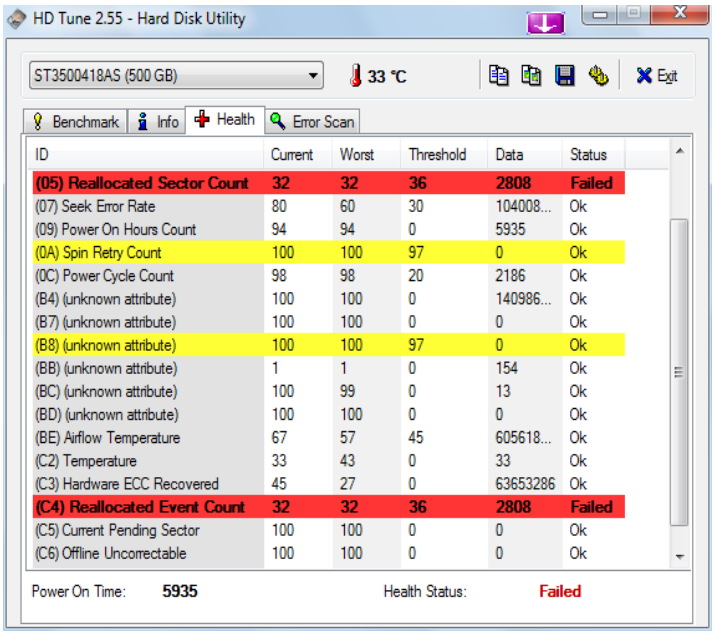


Ilustración 79 Información del S.M.A.R.T. del HD Tune

En la siguiente gráfica vemos un escaneo de un disco duro donde que contiene errores.

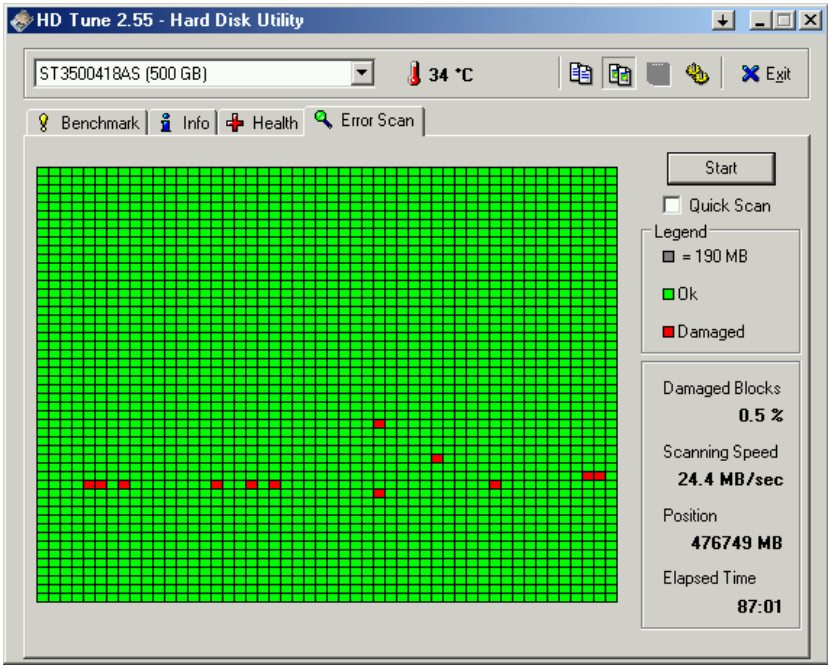


Ilustración 80 Escaneo de disco duro con errores

El caso de este equipo es de mencionarse debido a que el usuario presentaba problemas al trabajar que podrían ser síntomas de una infección por virus pero el problema era el disco duro, un ejemplo de que no siempre es lo que parece.

Memtest86+:

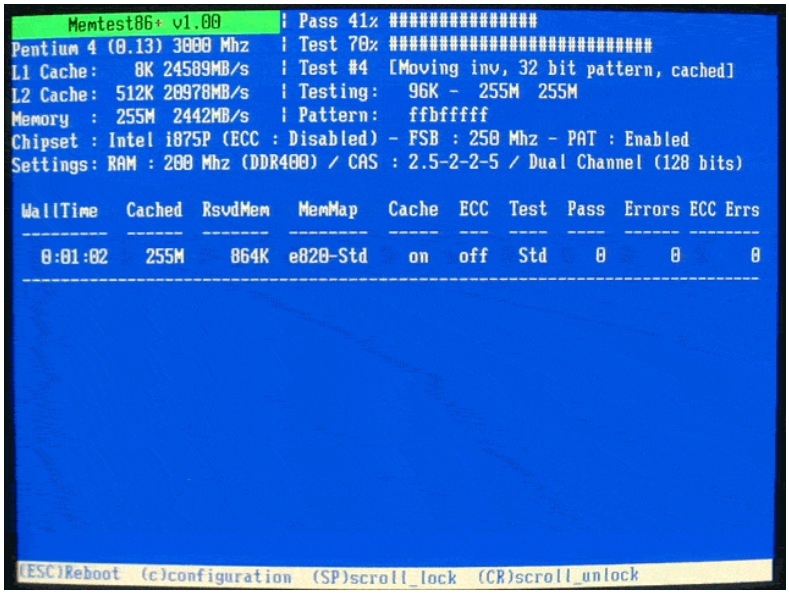


Ilustración 81 Pantalla del funcionamiento del Memtest86+

Memtest86+ escanea la memoria de acceso aleatorio (RAM) en busca de errores aplicándole diferentes pruebas. En el caso de encontrar un fallo aparecerá una leyenda con un error en la parte de abajo.

Hiren's Bootcd

Otra de las herramientas que usamos para rescatar información es *Hiren's Bootcd* pero montado en una memoria usb (Fat32 con MBR) ya que es más fácil de trabajar, este consiste en un conjunto de herramientas de diagnóstico y recuperación, pero lo usamos por la versión de Windows XP Live que contiene, este nos ayuda a recuperar información, cambiar parámetros de las particiones e incluso otras cosas más el cual no entraremos en detalle debido a la sensibilidad de esa información.

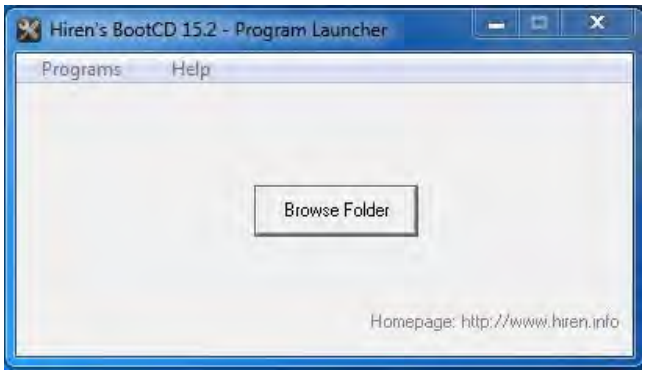


Ilustración 82 Ventana principal del Hiren's

Contiene una versión de Linux especial para diagnóstico y recuperación de información de nombre Parted Magic.

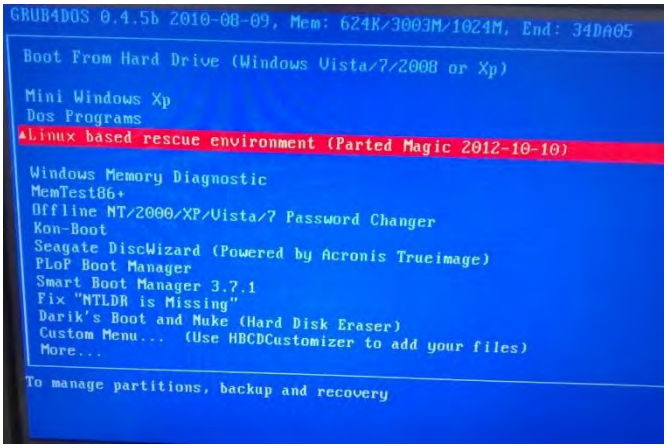


Ilustración 83 Menú en DOS de Hiren's bootCD

Como vemos el paquete Hirenś bootCD tiene muchas herramientas desde recuperación, procesos monitores de conexiones de red, editor de imágenes, editor de texto, etc. Pero estas de las que hablamos son unas des las herramientas que más utilizamos.

DiskGenius

Diskgenius es una utilería para diagnosticar e incluso recuperar información de un disco incluso borrado y dañado físicamente o de manera lógica por software (virus).

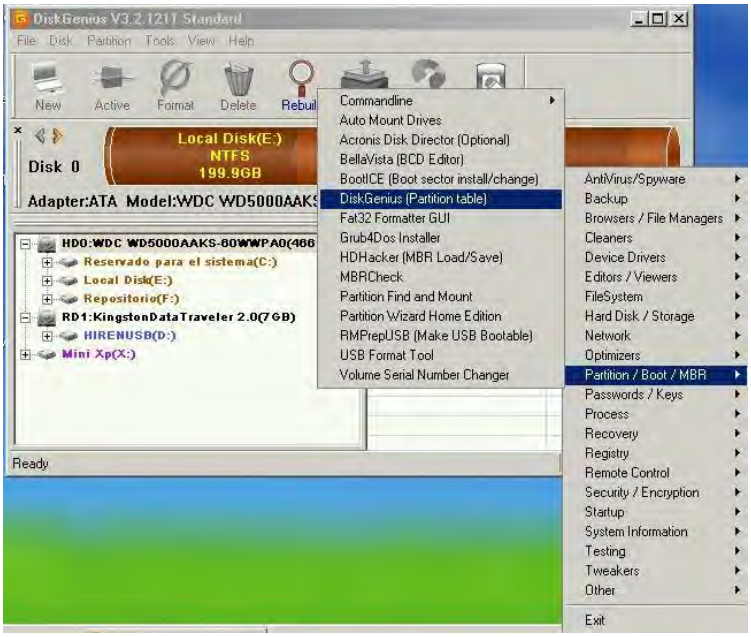


Ilustración 84 Ventana principal de DiskGenius

Anexo 11: Resolución de nombres incorrecta en la red interna por un envenenamiento DNS de un servidor externo

Descripción General

Una parte crucial para cualquier compañía con salida y que trabaja en Internet es la resolución de nombres, para esto se utiliza un servidor *DNS* (*Domain Name System*) el trabajo de este servidor es convertir de nombres comunes a una dirección IP.

Detalles de la resolución del problema

Todo empezó un lunes aproximadamente a las 09:30 A.M, se recibió un reporte de un usuario que reportaba que no podía entrar a la página de Banorte (www.banorte.com), realmente no era un problema de bloqueo, si no otra página a la que entraba pero no por poner mal la dirección si no que la resolución de nombre a IP era a una IP que no correspondía a la www.banorte.com.

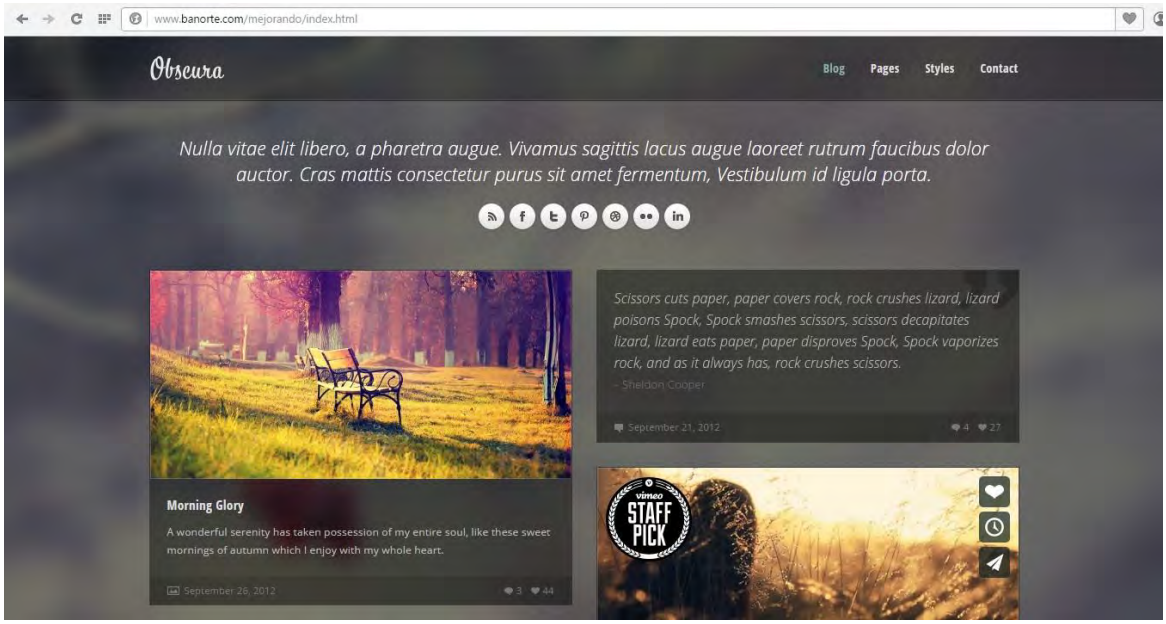


Ilustración 85 Página mostrada al poner Banorte

A través de la línea de comandos de Windows (CMD), usamos un comando llamado *nslookup* que nos sirve para resolver la IP de un dominio en este caso www.banorte.com.
Como vemos obtenemos una IP

```
C:\Users\Soporte>nslookup www.banorte.com
Servidor:  UnKnown
Address:  172.*.*.*

Nombre:  www.banorte.com
Address:  188.166.127.110
```

Pero ¿cómo podemos saber si pertenece a Banorte? utilizamos la página de HURRICANE ELECTRIC (http://bgp.he.net), obtenemos la siguiente información si observamos, no dice que pertenezca a Banorte(debe decir Banco Mercantil del Norte S.A).

188.166.127.110

Announced By		
Origin AS	**Announcement**	**Description**
AS202018	188.166.64.0/18	Digital Ocean, Inc.

Ilustración 86 Información proporcionada por he.net de la IP 192.100.234.28

Si utilizamos otro servidor DNS para resolver www.banorte.com en este caso el DNS de Google (8.8.8.8) y los de openDNS (208.67.222.222).

```
C:\Users\Soporte>nslookup www.banorte.com 8.8.8.8
Servidor:  google-public-dns-a.google.com
Address:  8.8.8.8

Respuesta no autoritativa:
Nombre:  www.banorte.com
Address:  192.100.234.28

C:\Users\Soporte>nslookup www.banorte.com 208.67.222.222
Servidor:  resolver1.opendns.com
Address:  208.67.222.222

Respuesta no autoritativa:
Nombre:  www.banorte.com
Address:  192.100.234.28
```

Nos resuelve una IP diferente 192.100.234.28, donde esta IP, si pertenece a Banorte, comprobándolo con la página de HURRICANE ELECTRIC.

192.100.234.28

Announced By		
Origin AS	**Announcement**	**Description**
AS11519	192.100.234.0/24	Banco Mercantil del Norte S.A., Institucion de Banca Multiple, Grupo Financiero Banorte

Ilustración 87 Información proporcionada por he.net de la IP 192.100.234.28

Entonces ¿qué está pasando? Al realizar las pruebas desde el servidor hasta el balanceador, sin embargo el servidor está resolviendo correctamente y el que resuelve incorrectamente es el balanceador pero esta información la obtiene de los módems de Infinitum, debido a que no tenemos control sobre los DNS de los modem de Infinitum es decir tuvimos que cambiar el DNS del balanceador a un DNS de Infinitum que si resolviera bien. Utilizamos el 200.33.146.209,

¿Por qué razón seguimos utilizando los DNS de Infinitum? Se debe a que algunos sistemas educativos pertenecen al IPS de TELMEX Y no son correctamente resueltas por DNS fuera de TELMEX como los de Google.

```
C:\Users\Soporte>nslookup www.banorte.com 200.33.146.209
Servidor:  nspue1.uninet.net.mx
Address:  200.33.146.209

Respuesta no autoritativa:
Nombre:  www.banorte.com
Address:  192.100.234.28
```

Al momento de resolver en el navegador ya entra al portal de Banorte.

Ilustración 88 Página correcta de Banorte

No sabemos si el problema fue un ataque al DNS de TELMEX o un error debido al DNS padre del que depende TELMEX.

Realizando una prueba más en un sistema Linux conectado al modem supuestamente con fallas, encontramos, que este modem estaba resolviendo mal las IP. En la siguiente imagen vemos con el comando *ifconfig* ya me resuelve una dirección IP.

```
jeffbardales@escaflowne-CQ45 ~ $ ifconfig
eth0      Link encap:Ethernet  direcciónHW 2c:44:fd:ac:69:82
          Direc. inet:192.168.1.68  Difus.:192.168.1.255  Másc:255.255.255.0
          Dirección inet6: fe80::2e44:fdff:feac:6982/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500 Métrica:1
          Paquetes RX:65 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:160 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:23947 (23.9 KB)  TX bytes:26962 (26.9 KB)
```

Luego ejecutamos *nslookup* desde la consola de Linux, lo cual nos da la IP no deseada (188.166.127.110) eso significa que este modem está resolviendo mal.

```
jeffbardales@escaflowne-CQ45 ~ $ nslookup www.banorte.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Name:   www.banorte.com
Address: 188.166.127.110
```

Realizamos las pruebas con otros servidores DNS donde estos si resuelven correctamente, revisamos el modem si tenía alguna configuración anormal y tenía los parámetros correctos.

jeffbardales@escaflowne-CQ45 ~ $ *nslookup www.banorte.com* 200.33.146.249.

```
Server:         200.33.146.249
Address:        200.33.146.249#53

Non-authoritative answer:
Name:   www.banorte.com
Address: 192.100.234.28

jeffbardales@escaflowne-CQ45 ~ $ nslookup www.banorte.com 200.33.146.241
Server:         200.33.146.241
Address:        200.33.146.241#53

Non-authoritative answer:
Name:   www.banorte.com
Address: 192.100.234.28
```

Antes de terminar las pruebas para ver que servidor DNS de infinitum estaba fallando, el problema dejo de presentarse, al parecer los encargados de los DNS de TELMEX resolvieron el problema. Esto da una idea que no todos están a salvo de un envenenamiento DNS.

```
jeffbardales@escaflowne-CQ45 ~ $ nslookup www.banorte.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name: www.banorte.com
Address: 192.100.234.28
```

Anexo 12: Uso excesivo del ancho de banda de Internet

Descripción General

Como sabrán el uso del Internet, aunque sea limitado en el aspecto de contenido, también tendría que ser limitado en la velocidad de Internet que se proporciona, por eso se realiza esta solución efectiva hasta el momento.

Todos usaban el Internet sin restricción de velocidad siendo que aunque consultaban contenido apropiado, podían consultar el contenido a toda la velocidad disponible al momento, si eran 4 Mb de Internet a 4 Megas o 2 Megas o de ya en el peor de los casos 8 y 9 Megas, esto generaba la frustración que Internet lo consumían unos pocos.

Detalles de la resolución del Problema

Se hizo uso del Limiter una característica que tiene pfSense que no tienen otros o son de paga los módulos. En este apartado explicaremos como se usó y en que consiste el Limiter. Lo que hace el Limiter es establecer un límite de velocidad de internet ya sea para una IP o puedo definir una velocidad para que la comparta todo un segmento.

Hemos establecido varios Limiters con el fin de usar según sea la ocasión.

Ilustración 89 Limiters creados

Limiter bajada1Mb que estamos aplicando a la mayoría de los equipos conectados.

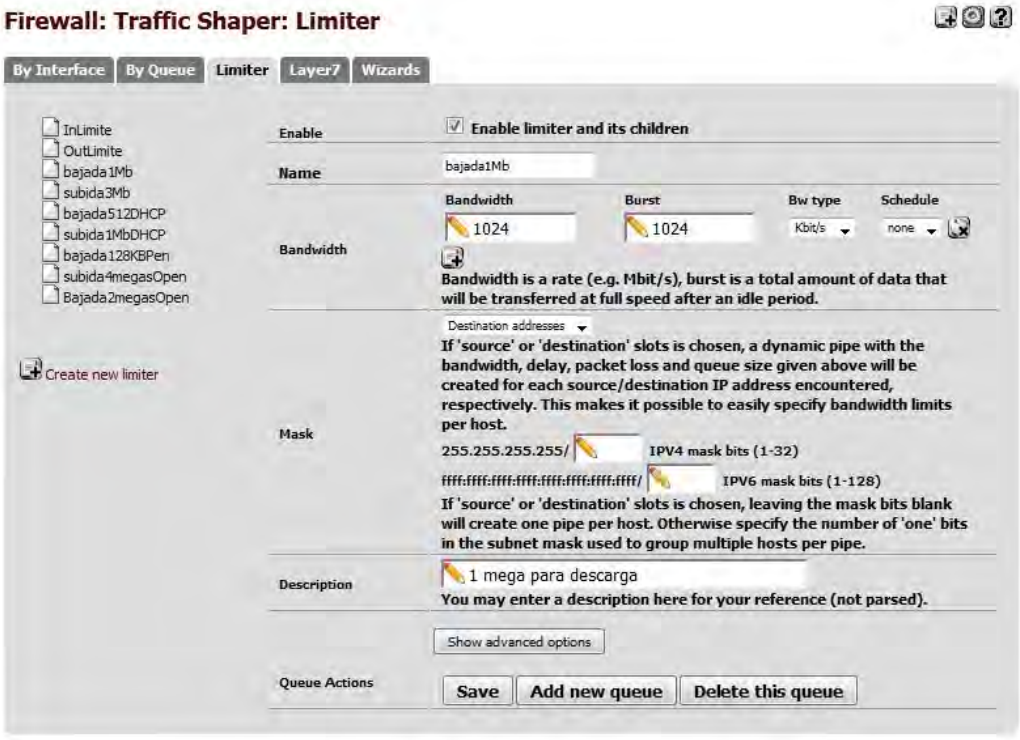


Ilustración 90 Limiter bajada1Mb para la mayoría de los equipos

En el número de posición que el Limiter bajada1Mb tiene es 3, esto nos servirá para monitorear más adelante el Limiter. Estamos aplicando el Limiter **bajada1Mb** a la toda la red.

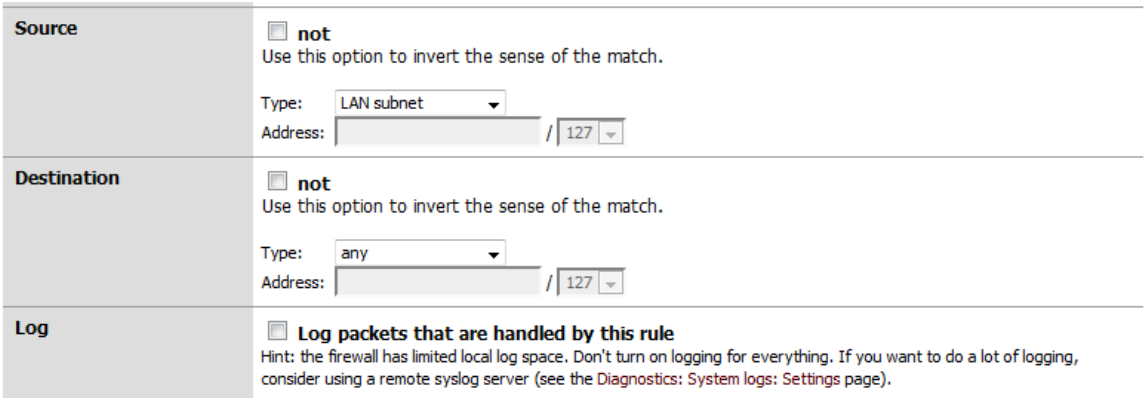


Ilustración 91 Regla donde aplicaremos el Limiter bajada1Mb

En las **Advanced features** de la regla que deseamos aplicar el *limiter* en la parte de in/out donde **in** se refiere a la subida (si lo vemos del punto de vista del usuario) y out es bajada (entra si lo vemos del punto de vista del usuario).

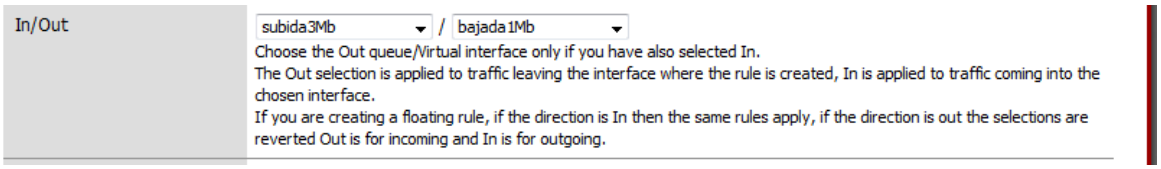


Ilustración 92 Aplicando el Limiter Subida a 3Mb y bajada 1Mb

Explicado en un gráfico.

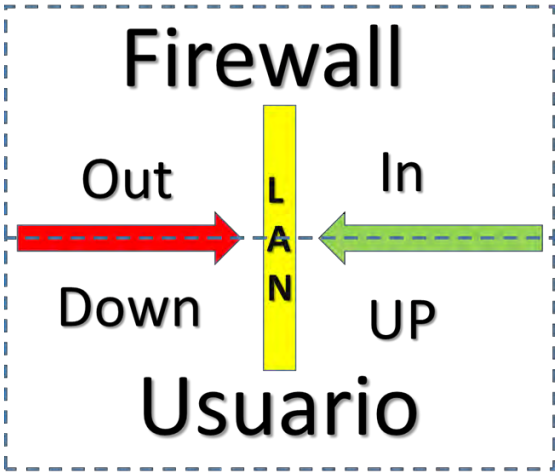


Ilustración 93 Explicación del In y Out

Desde el punto de vista del usuario, *Out* es lo que descarga y el *In* es la subida para el usuario. Es la parte del Out donde tenemos que aplicar el Limiter que administrara la velocidad que requerimos, en este ejemplo estamos dando 1 *Mb* de descarga para cada uno de las IP dentro mi segmento a menos que diga lo contrario.

Como podemos ver a continuación en la información del *Limiter* observamos que el 3 está funcionando que es el que aplica de 1024 Mbits (1 MB de descarga).

Diagnostics: Limiter Info

```
Limiters:
00001:   1.000 Mbit/s    0 ms burst 1048576
q131073  50 sl. 0 flows (1 buckets) sched 65537 weight 0 lmax 0 pri 0 droptail
 sched 65537 type FIFO flags 0x0 0 buckets 0 active
00002: 512.000 Kbit/s    0 ms burst 524288
q131074  50 sl. 0 flows (1 buckets) sched 65538 weight 0 lmax 0 pri 0 droptail
 sched 65538 type FIFO flags 0x0 0 buckets 0 active
00003:   1.024 Mbit/s    0 ms burst 1048576
q131075  50 sl. 0 flows (1 buckets) sched 65539 weight 0 lmax 0 pri 0 droptail
 sched 65539 type FIFO flags 0x1 256 buckets 38 active
    mask:  0x00 0x00000000/0x0000 -> 0xffffffff/0x0000
BKT Prot ___Source IP/port____ ____Dest. IP/port____ Tot_pkt/bytes Pkt/Byte Drp
  5 ip           0.0.0.0/0        192.168.5.85/0       21     2483  0    0   0
  9 ip           0.0.0.0/0        192.168.5.89/0       18     5979  0    0   0
 11 ip           0.0.0.0/0        192.168.5.91/0     1449  1107685  0    0   0
 30 ip           0.0.0.0/0       54.230.80.210/0        2       80  0    0   0
 40 ip           0.0.0.0/0       192.168.5.120/0       10      901  0    0   0
 41 ip           0.0.0.0/0       192.168.5.121/0       18     1410  0    0   0
 42 ip           0.0.0.0/0       192.168.5.122/0      207   101742  0    0   0
 44 ip           0.0.0.0/0       192.168.5.124/0    22602 31729975  0    0  74
 47 ip           0.0.0.0/0       192.168.5.127/0     5025  7520896  0    0   4
 49 ip           0.0.0.0/0        192.168.5.97/0      212   214914  0    0   0
 52 ip           0.0.0.0/0       192.168.5.100/0       81    12850  0    0   0
 66 ip           0.0.0.0/0        192.168.5.18/0     1072   739212  0    0   0
 67 ip           0.0.0.0/0        192.168.5.19/0        2      104  0    0   0
 70 ip           0.0.0.0/0        192.168.5.22/0     2832  1891581  0    0  17
 74 ip           0.0.0.0/0        192.168.5.26/0       28     4881  0    0   0
 77 ip           0.0.0.0/0        192.168.5.29/0       18     2039  0    0   0
 79 ip           0.0.0.0/0        192.168.5.31/0       21     2316  0    0   0
 84 ip           0.0.0.0/0         192.168.5.4/0       31     5145  0    0   0
 88 ip           0.0.0.0/0         192.168.5.8/0      847   112799  0    0   0
 89 ip           0.0.0.0/0         192.168.5.9/0       16      688  0    0   0
 98 ip           0.0.0.0/0       192.168.5.50/0       486   494180  0    0   0
106 ip           0.0.0.0/0       192.168.5.58/0       414   223512  0    0   0
111 ip           0.0.0.0/0       192.168.5.63/0      1320  1543517 32 44104  32
115 ip           0.0.0.0/0       192.168.5.35/0       525   221347  0    0   0
117 ip           0.0.0.0/0       192.168.5.37/0      1145   614336  0    0   0
124 ip           0.0.0.0/0       192.168.5.44/0         9      753  0    0   0
```

Ilustración 94 Limiter Info mostrando el uso del Limiter bajada1Mb

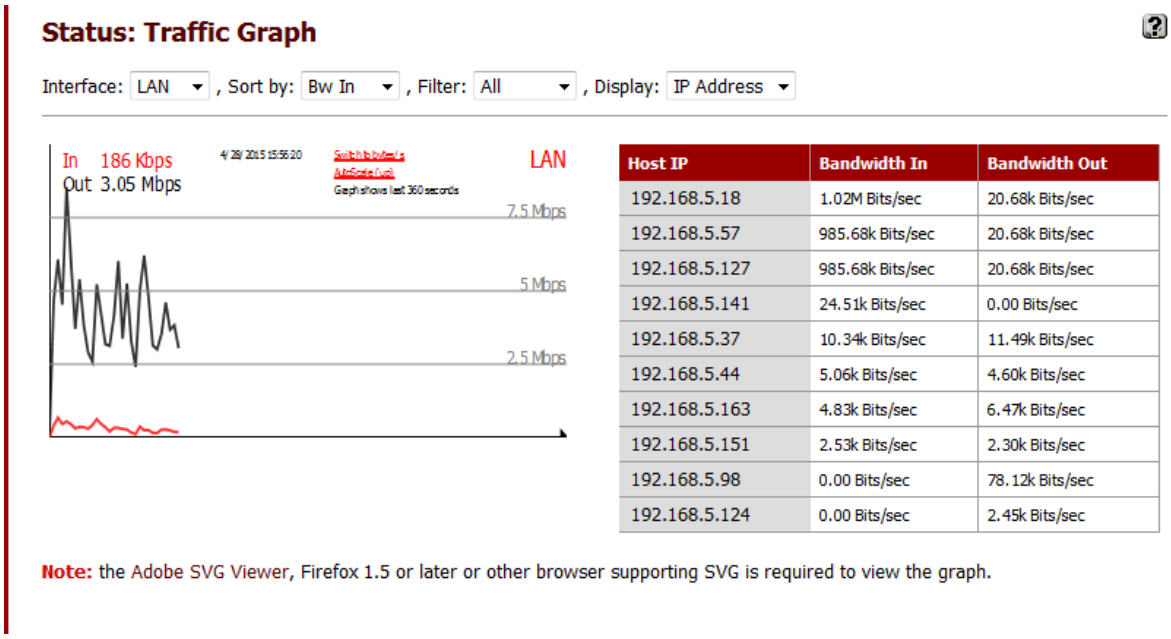


Ilustración 95 Gráfica del Tráfico con el Limiter bajada1Mb funcionando

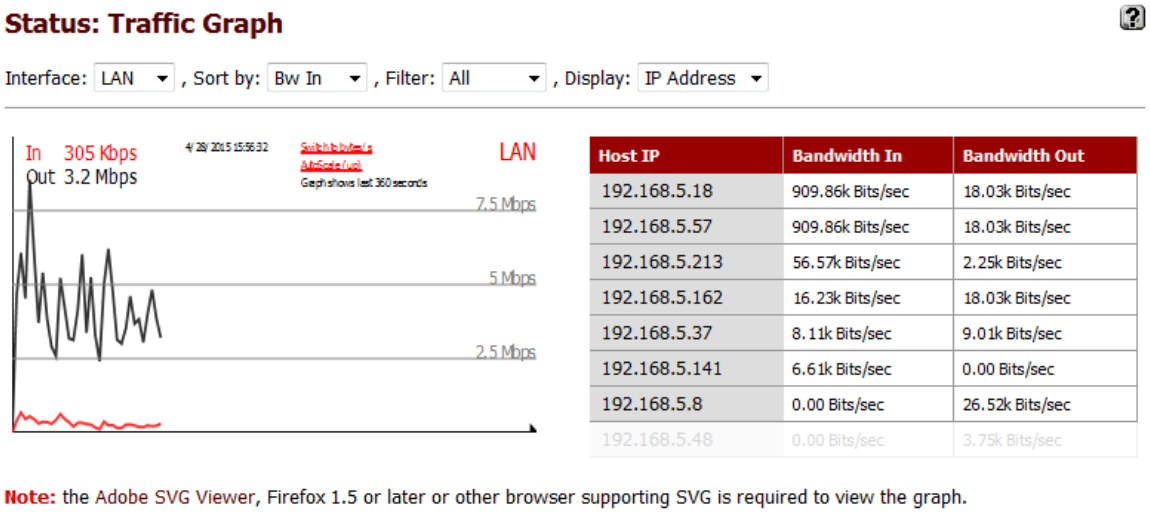


Ilustración 96 Gráfica del Tráfico con el Limiter bajada1Mb funcionando

Las ilustraciones 95 y 96 muestran como estamos limitando la velocidad de internet y puede ser aplicado con cualquier velocidad. Tanto en la bajada como en la subida, pero es más útil en la parte de descarga ya que así evitamos que sólo unos cuantos usuarios consuman el Internet.