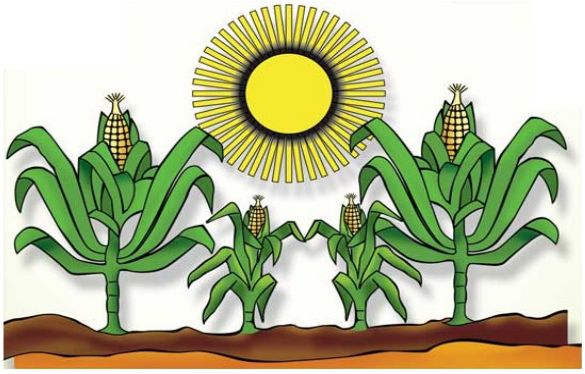
UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACION



ASIGNATURA: Redes II

CATEDRATICO: Ing. Manuel Flores

TEMA: Firewall con Balanceador de carga

INTEGRANTES

APELLIDO	*NOMBRE*	*CARNET*	*% PARTICIPACION*
Avalos	*Julio César*	**A02110311**	**100%**
Campos Nolasco	*Jacquelinne Lissette*	**CN02110850**	**100%**
Alvarado Ramiréz	*Evelin Beatríz*	**AR02110095**	**100%**
Urbina	*Oscar Antonio*	*UM02110703*	**100%**

San Salvador, 30 noviembre de 2013.

Índice de contenido

Introducción

En el presente documento se detalla la forma en la que se procederá en la configuración del Firewall con balanceador de dos enlaces en Internet. Ya que el balanceador sirbe como un equilibrador de carga ya que es una solución de red central encargada de distribuir el tráfico entrante entre al servidor y el mismo contenido de la aplicación . Al equilibrar las solicitudes de aplicaciones a través de múltiples servidores.

Además también Mencionamos los estudios de factibilidad en la implementación de dicho Proyecto las tecnologías involucradas y las etapas de para la implementación del proyecto. y el beneficios que nos traería la implementación del mismo.

Objetivo General.

Configurar el firewall con balanceador de carga entre dos puntos de enlace en Internet, y explicar de manera precisa su funcionamiento.

Objetivos Específicos.

1. Explicar en que consiste el firewall con balanceador de carga.
2. Enumerar las herramientas que se necesitan para realizare.
3. En que casos puede usarse.

Descripción de Proyecto

Este proyecto consiste configurar un firewall con balanceador de carga que permite controlar el trafico que pasa por Internet según las peticiones de los clientes que tenga conectados . Para este proyecto se a realizado la prueba con dos modems 3G teniendo configurada tres computadoras una como servidor y dos como clientes, luego se instalan la aplicaciones iproute, iptables Y Munin.

Iproute: que sirbe en el balanceo asignándole pesos a cada una de las placas existentes dentro de la computadora.

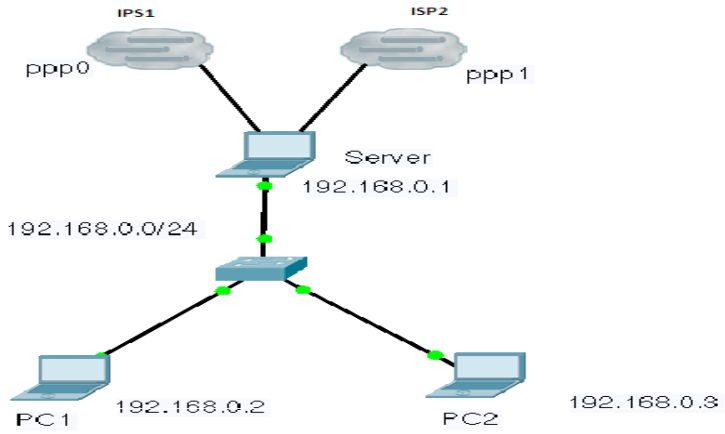
Iptables: una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red.

Munin es una aplicación escrita en perl, de monitorización de sistema de red que nos muestra gráficos a través de una interfaz web.

Tcpdump. Es un herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red

Dicho proyecto se a desarrollado en un lapso de tiempo de dos meses y 15 días, según lo establecido en el cronograma. Utilizando computadoras con sistema operativo Linux en este caso Debian.

Diagrama de Red.



Marco Teórico

Que es un Firewall. Es Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Balance de carga

El balance o balanceo de carga es un concepto usado en informática que se refiere a la técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos. Está íntimamente ligado a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles.
El balance de carga se mantiene gracias a un algoritmo que divide de la manera
más equitativa posible el trabajo, para evitar los así denominados cuellos de botella.

Uno de los principales problemas de los mayores sitios web en Internet es cómo gestionar las solicitudes de un gran número de usuarios. Se trata de un problema de escalabilidad que surge con el continuo crecimiento del número de usuarios activos en el sistema.
Este servicio se puede brindar tanto con un enrutador como con una computadora con dos placas de red y software específico.
Hay balanceadores de carga tipo round-robin (uno a uno) y por pesos (que son capaces de saber cuál de los nodos está más libre y lanzarle la petición). El más conocido es LVS, sin embargo hay otros, como el Red Hat Piranha.

El estudio del balanceo de carga es muy importante para poder distribuir de una forma equitativa la carga computacional entre todos los procesadores disponibles y con ello
conseguir la máxima velocidad de ejecución

Que es un Modems.

es un pequeño Gadget o dispositivo electrónico que permite a un usuario acceder a Internet a través de su PC portátil cuando no dispone de ninguna conexión a Internet o cuando no se encuentra dentro de una zona WiFi.

Cómo funciona
El modem USB 3G, una especie de modem inalámbrico de tipo WiFi, utiliza la red de los operadores de telefonía para conectarse a Internet. Al igual que los teléfonos móviles, el modem USB 3G posee un lugar reservado para una tarjeta SIM. Para que funcione, es necesario que previamente se haya suscrito a un plan en un operador de telefonía.

Herramientas Utilizadas iproute
Enrutamiento IP es un término general para el conjunto de protocolos que determinan el camino que sigue a los datos con el fin de viajar a través de múltiples redes desde su origen hasta su destino. Los datos se dirige

desde su origen hasta su destino a través de una serie de routers , y a través de múltiples redes. Los protocolos de enrutamiento IP permiten a los enrutadores construir una tabla de reenvío que se correlaciona con destinos finales siguientes direcciones hop.

Estos protocolos incluyen :

1. BGP (Border Gateway Protocol)
2. IS-IS (Intermediate System - Sistema Intermedio
3. OSPF (Open Shortest Path First)
4. RIP (Protocolo de Información de Enrutamiento)

Como Funciona.

Cuando un paquete IP se debe desviar , un router utiliza su tabla de reenvío para determinar el siguiente salto para el destino del paquete (en base a la dirección IP de destino en la cabecera del paquete IP) , y reenvía el paquete apropiadamente . El siguiente router entonces repite este proceso utilizando su propia tabla de reenvío , y así sucesivamente hasta que el paquete alcanza su destino . En cada etapa , la dirección IP en la cabecera del paquete es información suficiente para determinar el siguiente salto ; no se requieren cabeceras de protocolo adicionales .

La Internet , con el fin de encaminamiento , se divide en sistemas autónomos (AS) . Un AS es un grupo de routers que están bajo el control de una sola administración y el intercambio de información de enrutamiento utilizando un protocolo de enrutamiento común . Por ejemplo, una intranet corporativa o una red ISP por lo general puede ser considerado como un individuo

además Iproute2 es un paquete de utilidades desarrollado por Alexey Kuznetsov. Este paquete es un conjunto de herramientas muy potentes para administrar interfaces de red y conexiones en sistemas Linux.

Este paquete reemplaza completamente las funcionalidades presentes en
ifconfig, route, y arp y las extiende llegando a tener características similares a las provistas por dispositivos exclusivamente dedicados al ruteo y control de tráfico.

Iptables

iptables es un sistema de firewall vinculado al kernel de linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema ipchains, un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación iptables esta integrado con el kernel, es parte del sistema operativo. ¿Cómo se pone en marcha? Realmente lo que se hace es aplicar reglas. Para ellos se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple

script de shell en el que se van ejecutando las reglas de firewall.

Las reglas de firewall están a nivel de kernel, y al kernel lo que le llega es un paquete (digamos, un marrón ;) y tiene que decidir que hacer con él. El kernel lo que hace es, dependiendo si el paquete es para la propia maquina o para otra maquina, consultar las reglas de firewall y decidir que hacer con el paquete según mande el firewall

se usa para crear, mantener y revisar las tablas de filtrado de paquetes en el kernel de Linux una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros

Munin.

Munin es un programa de monitorización de servidores que genera estadísticas sobre su funcionamiento de los recursos de nuestros servidores, como memoria, disco duro y servicios. Utiliza las herramientas RRDTool para generar gráficas de rendimiento de los parámetros del sistema analizados. Utiliza una interfaz web para mostrar las gráficas generadas, permite trabajar de forma distribuida, mostrando la información de varios servidores.

Características.

- Cuenta con una interfaz [web] que muestra la evolución histórica del uso de recursos.
- Monitorea el uso de recurso de cada máquina, recursos como disco, red, uso de CPU, RAM, Carga (load).
- Es capaz de monitorear indicadores de algunas aplicaciones como tamaño de cola de postfix, procesos de apache, consultas de mysql entre otras.
- Genera gráficas por día, semana, mes y año de cada uno de los indicadores.
- Muestra el mínimo, máximo, media y valor actual de los indicadores en cada período de tiempo.

Ventajas

- Permite determinar con anticipación cuando un recurso estará sobre utilizado o será insuficiente.
- Permite monitorear errores o generar mejoras. Por ejemplo, detectar errores de red que pueden ser causados por la alta carga del servidor.
- Permite medir cuantitativamente el crecimiento del uso de los recursos, de esta manera es posible sustentar la compra de hardware o medir el crecimiento.

Tcpdump.
Es un herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red.
Funciona a nivel de paquetes, lo que significa que captura los paquetes reales
que entran o salen de su equipo.

Permite al usuario capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado.

tcpdump funciona en la mayoría de los sistemas operativos UNIX: Linux, Solaris, BSD, Mac OS X, HP-UX y AIX entre otros. En esos sistemas, tcpdump hace uso de la biblioteca libpcap para capturar los paquetes que circulan por la red y utiliza Un sniffer que es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.

Utilización frecuente de tcpdump

- Para depurar aplicaciones que utilizan la red para comunicar.
- Para depurar la red misma.
- Para capturar y leer datos enviados por otros usuarios u ordenadores. Algunos protocolos como telnet y HTTP no cifran los datos que envían en la red.
- Un usuario que tiene el control de un router a través del cual circula tráfico no cifrado puede usar tcpdump para conseguir contraseñas u otras informaciones.

Lista de actividades.

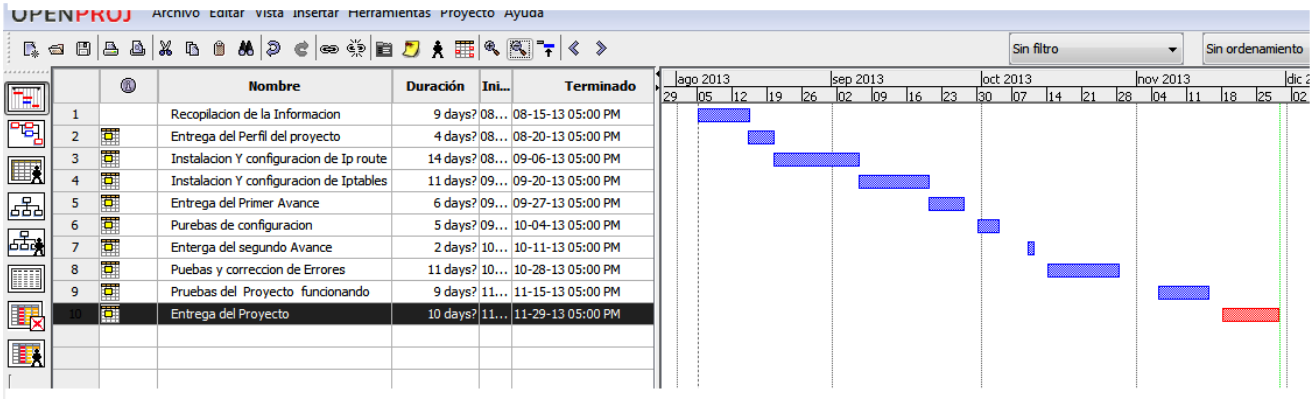
1. Instalar configurar ip route.

2. Instalación y configuración de Iptables

3. pruebas Funcionales del proyecto

4. Entrega del Proyecto.

Cronograma de Actividades.



Factibilidad.

Técnica. Se cuentan con los conocimientos básicos en el funcionamiento de redes informáticas. Y tenemos acceso a las herramientas a utilizar.

Económica. Es factible debido a que no incurriremos en grandes gastos para la implementación del Proyecto.

Económica. Es factible debido a que no incurriremos en grandes gastos para la implementación del Proyecto.

nombre	**Costo económico**
2 módem	$ 60.00
1 router	$12.00
4 computadoras	$1,600
4 empleados	$ 400
Total	**$2,072**

Operativa. Es factible por que consideramos que puede contribuir ha hacer un mejor uso de los recursos en redes cuando este se implementando.

Conclusión

1. Como grupo hemos concluido la importancia que tiene un firewall con balanceador de carga con dos enlaces a internet, el cual nos puede ayudar para lograr tener una mayor estabilidad de conexión .

2. Que el balanceo nos permite llevar un control de todo lo que pasa por la red.

Bibliografía.

Fecha de publicación el 28/11/2009
http://blog.khax.net/2009/11/28/multi-gateway-routing-with-iptables- and-iproute2/

http://ecsl.slgt.org/p/internet

http://parkersamp.com/2010/03/howto-using-linux-as-a-simple-load- balancer-nat-router- firewall/

http://lartc.org/howto/lartc.rpdb.multiple-links.html

Manual de configuración del balanceo de carga

El balanceo de carga consta de tener dos accesos a internet y balancear la carga que se tiene al momento de conectarse a internet, configurando como router una PC, que servirá como servidor que alimentara a las PCs clientes que se tendrán conectadas en la red interna. La conexión a internet se hará con módem 3G.

Herramientas a utilizar para el desarrollo del balanceo.

Herramientas de hardware

1. Tres computadoras con sistema operativo linux, pueden ser laptos o de escritorio, (una que funcione como servidor y dos como clientes).
2. Un switch.
3. Tres cables de red cruzados.
4. Dos módem usb 3G.

Herramientas de software

1. Sistema operativo linux (debian).
2. Munin (para graficar el trafico que pasa por la red.
3. Ip route
4. ip table

Configuraciones

Lo primero que se hará es configurar las la red interna, teniendo la ip de red, luego asignar las ips a cada maquina, tenga en cuenta que una de las maquinas se usara como router que alimentara de internet a las maquinas clientes.

Tabla de información.

DISPOSITIVO	INTERFAZ	DIRECCION IP	MASCARA DE SUBRED	PUERTA DE ENLACE
Servidor	Eth0	192.168.0.1	255.255.255.0	10.64.64.64 10.64.64.65
	PPP0	IP Dinámica	No Asignada	No Asignada
	ppp1	IP Dinámica	No Asignada	No Asignada
PC1	eth0	192.168.0.2	255.255.255.0	192.168.0.1
PC2	eth0	192.168.0.3	255.255.255.0	192.168.0.1

Nota: Los clientes tienen como puerta de enlace a la ip de de servidor.

Configuración de dos modem USB 3G

Los módem USB trabajan bajo una ip dinámica por lo tanto cada vez que se conectan la IP de cada módem va cambiando, así que debemos de configurar lo para que cada vez que los módem estén conectados les asigne una IP por defecto y trabajen bajo una IP estática.

Instalamos Ip tables desde la terminal nos vamos a:

>Aplicaciones
>Accesorios
>Terminal

entramos como administrador
su
y tu contraseña

Instalamos iptable
Iptable: (es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red.)

aptitude install iptables

Ejecutas estos comandos

iptables --flush
iptables --table nat --flush
iptables --table nat --append POSTROUTING --out-interface ppp0 -j MASQUERADE
iptables --table nat --append POSTROUTING --out-interface ppp1 -j MASQUERADE
iptables --append FORWARD --in-interface eth0 -j ACCEPT
ip route del default

Balanceador de carga

Ya configurados los módem, pasamos a hacer el balanceo de carga para que cada vez que los clientes lo deseen puedan acceder a Internet.

nano enrutamiento.sh

y lo ajustamos según convenga

```
#!/bin/bash


IF1=ppp0
IF2=ppp1
IP1=10.26.40.65
IP2=10.147.71.178
P1=10.64.64.64
P2=10.64.64.65
P1_NET=10.26.40.65
P2_NET=10.147.71.178



echo "ip route add $P1_NET dev $IF1 src $IP1 table 1"
ip route add $P1_NET dev $IF1 src $IP1 table 1
echo "ip route add default via $P1 table 1"
ip route add default via $P1 table 1

echo "ip route add $P2_NET dev $IF2 src $IP2 table 2"
ip route add $P2_NET dev $IF2 src $IP2 table 2

echo "ip route add default via $P2 table 2"
ip route add default via $P2 table 2


echo "ip route add $P1_NET dev $IF1 src $IP1"
ip route add $P1_NET dev $IF1 src $IP1


echo "ip route add $P2_NET dev $IF2 src $IP2"
ip route add $P2_NET dev $IF2 src $IP2



echo "ip rule add from $IP1 table T1"
ip rule add from $IP1 table 1
```

echo "ip rule add from $IP2 table T2   "
ip rule add from $IP2 table 2

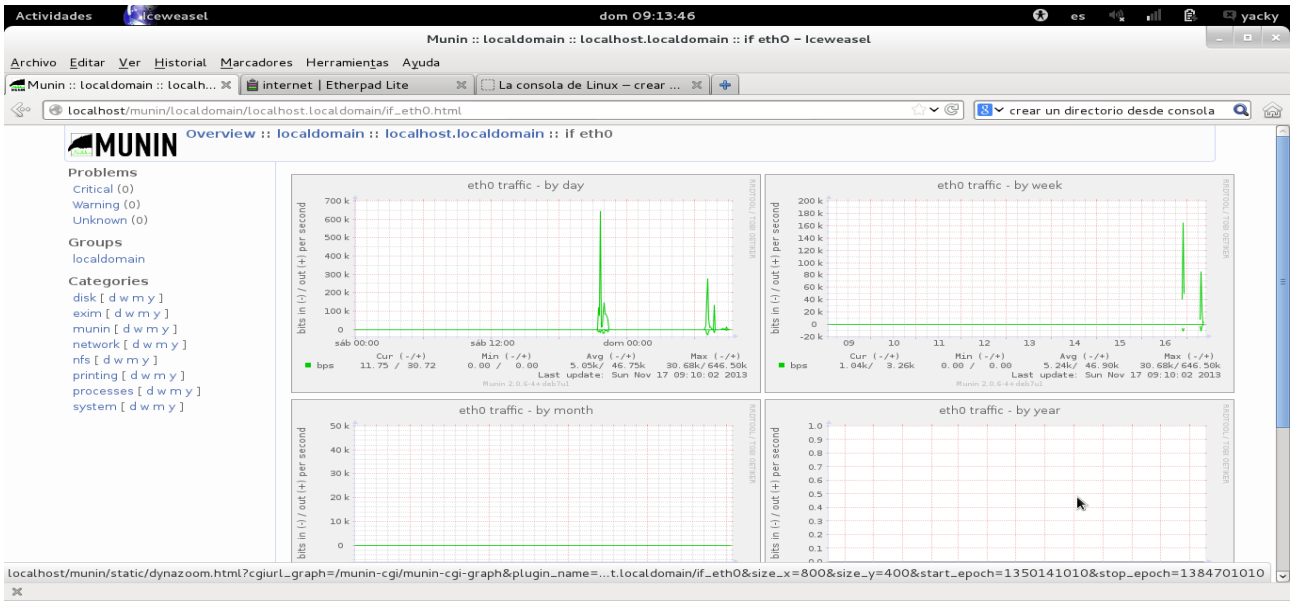
echo "ip route add default scope global nexthop via $P1 dev $IF1 weight 1 nexthop via $P2 dev $IF2 weight 1"
ip route add default scope global nexthop via $P1 dev $IF1 weight 1 nexthop via $P2 dev $IF2 weight 1

Munin

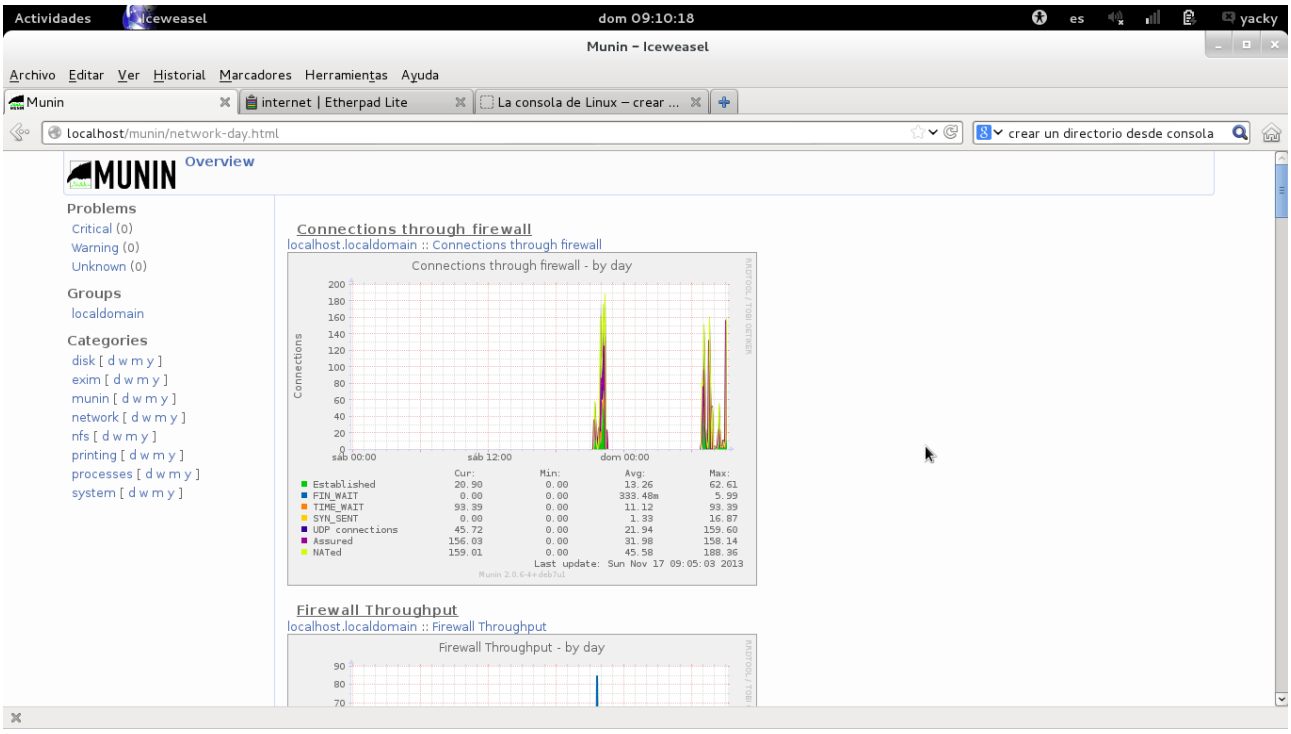
Munin: es un capturador de paquete de monitoreo del trafico que circula por la red, el cual muestra de forma gráfica el trafico.

Instalación de Munin
apt-get install munin

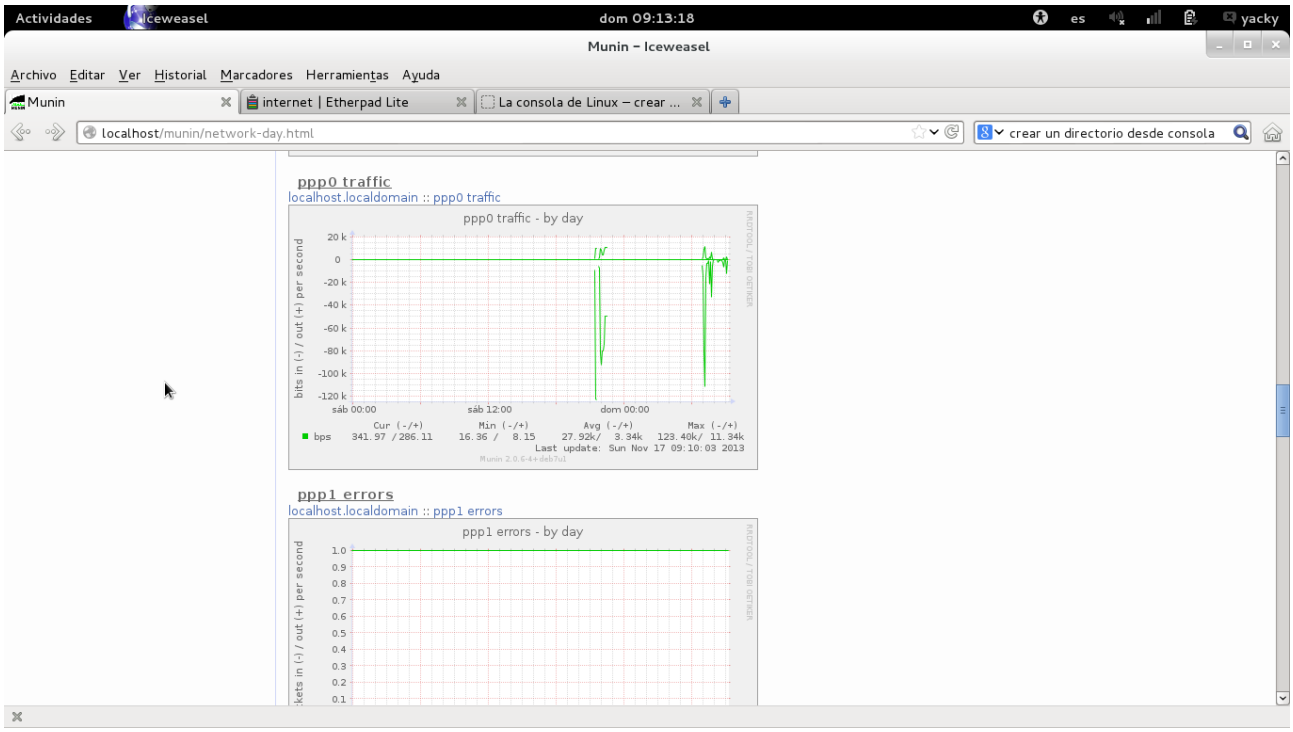
Gráfica del trafico que circula por la red
Trafico de Eth0



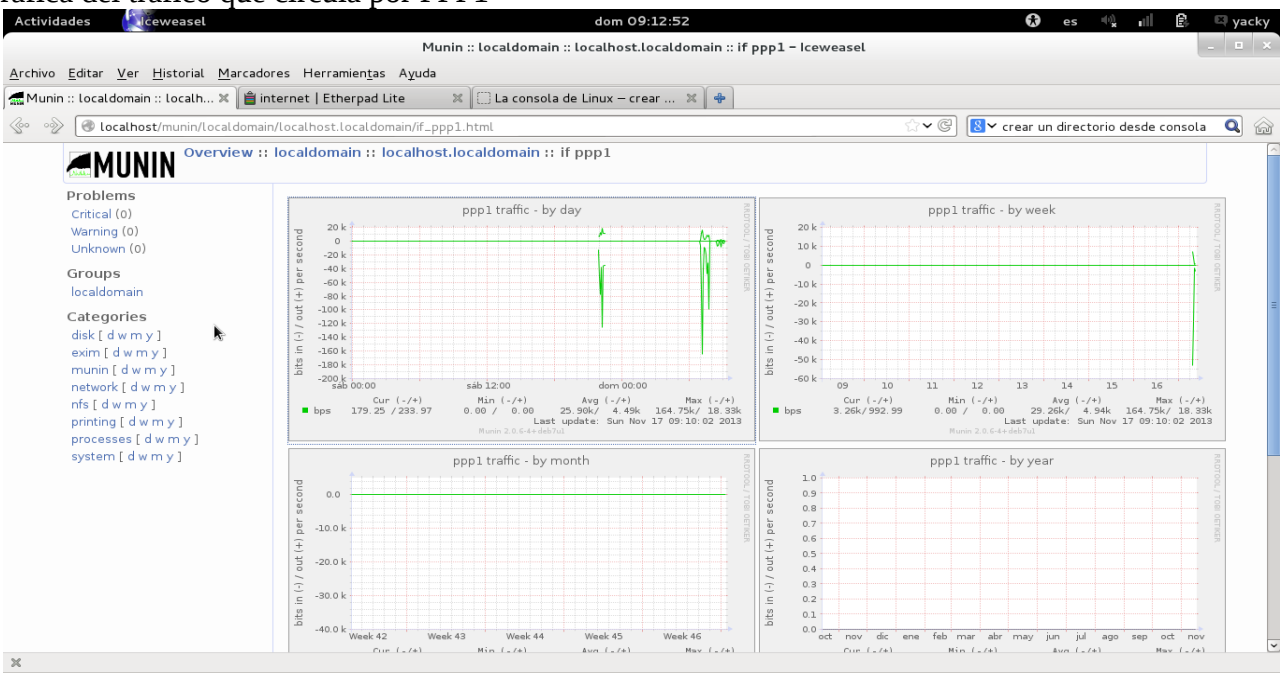
Gráfica del firewall en la red



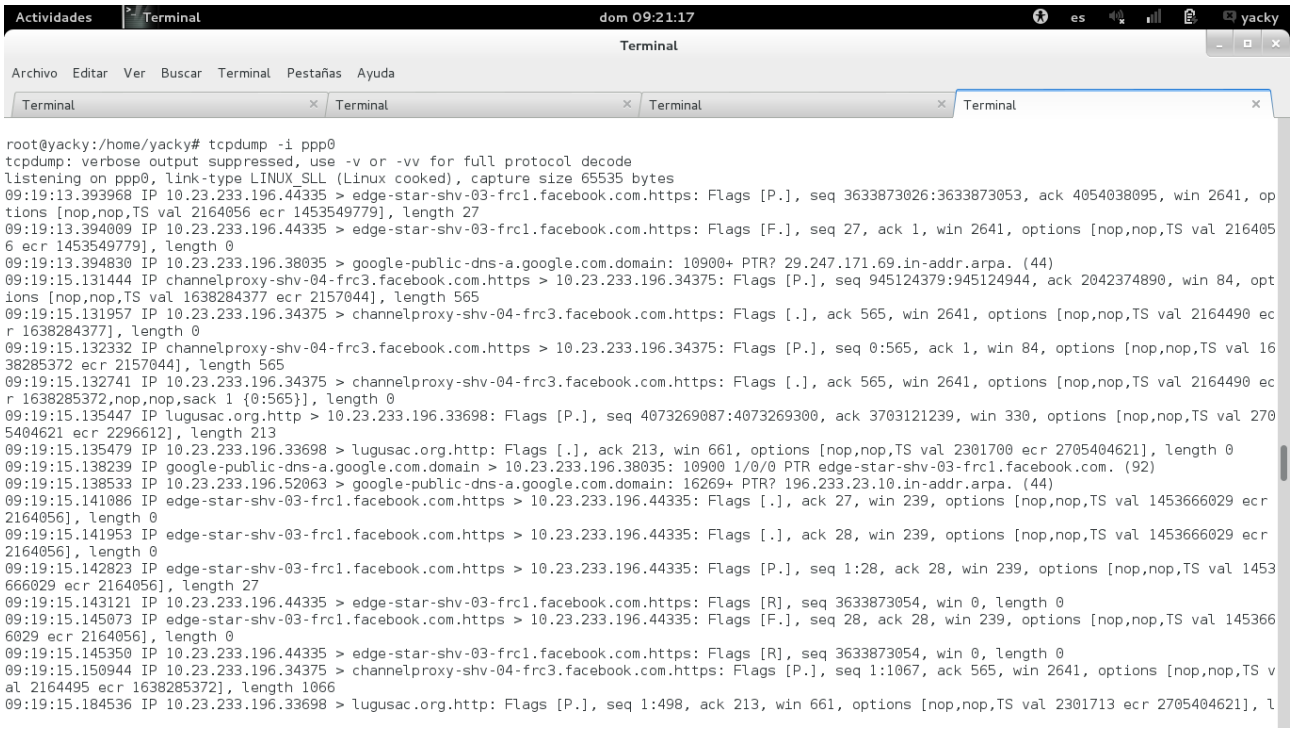
Gráfica del trafico que circula por PPP0



Gráfica del trafico que circula por PPP1



Trafico que pasa por ppp0 visto mediante la consola con tcpdum



Trafico que pasa por la ppp1 mediante de la consola con tcpdum