Seguridad Perimetral

Seguridad Perimetral

- IANUX Soluciones | Comunidad de Software Libre

http://ianux.com.ar | http://saltalug.org.ar

LPIC Oscar Gonzalez,
Consultor IT,
Security Researcher,
Instructor LPI Linux

MSN+Gtalk:
oscar.gonzalez@ianux.com.ar
oscar.gonzalez@saltalug.org.ar
Skype: gonzalez_oscar

Ing. Miguel Tolaba
Administrador de Red
Profesor de Sistemas Operativos

MSN + Gtalk
miguel@saltalug.org.ar

IANUX SOLUCIONES

Seguridad Perimetral

Agenda:

- Introducción
- Breves Definiciones
- Soluciones Existentes
- Shorewall
  - Ventajas y Funcionalidades
  - Instalación y Configuración
  - Ejemplos de implementación

IANUX SOLUCIONES

Introducción

- Que es la seguridad?
- Que hay que proteger?
- De quien hay que protegerlo?
- Como Protegerlo?

Definiciones

- Que es la Seguridad Perimetral?
- Que son los Firewalls?
- Que son los IDS/IPS?
- Que son los HoneyPots/HoneyNets?
- Que es la Alta Disponibilidad?
- Que es el Balanceo de Carga?
- Que es el Traffic Shaping?
- Que es una VPN?
- Que es la DMZ?
- Que es un Proxy?
- Que es NAT?
- Que son VLANs?

Aclaraciones

- Se debe elegir una política de seguridad antes de iniciar la distribución de los firewalls.
- Además del firewall, pueden coexistir otros mecanismos de seguridad, como un servidor de autenticación (LDAP/Kerberos/Radius), un IDS u otros.
- No hay reglas a seguir para colocar los firewall salvo las básicas de seguridad y el sentido común.

Honeypots

- Se conoce como Honeypots (tarros de miel) a una trampa que se coloca a los atacantes para que dejen sus huellas, expulsarlos o incluso contraatacar. Suele tratarse de un entorno controlado en el que el atacante puede moverse libremente sin que peligre nuestra red.

Ejemplos

- **Sticky**: Se usan para ralentizar un ataque.
- **Sugarcane**: Simulando un proxy abierto.
- **Spamtrap**: Una dirección de correo que utilizamos solo para spam.

Honeynets

- Una Honeynet es una red de Honeypots. También son entornos altamente controlados. Ofrecen mas información que los Honeypots ya que dan mas libertad al atacante.

Honeypots
de baja iteraccion

Características

- Simulan un sistema operativo o servicios.
- Las posibilidades del atacante son mínimas
- En Linux: honeyd.

Desventajas

- Muy simples y por lo tanto es posible detectarlos.
- No ofrecen casi información sobre el ataque.
- Diseñados para detectar ciertos comportamientos.

Honeypots
de alta iteraccion

Características

- Son sistemas operativos completos.
- Están preparados para no comprometer la red.
- Difícil de implementar.
- Casi exclusivos en entornos de investigación
- Ofrecen toda la información que queramos.

Desventajas

- Dan mucha libertad al atacante.
- Si esta mal diseñado puede comprometer a la red.
- Depende de la habilidad del administrador.

Soluciones de Firewalls

Kernel Support

BSD

Linux

Ejemplo de Soluciones existentes:

IPCOP

Endian

ClearOS

Juniper

PFSense

Shorewall

Astaro

IANUX SOLUCIONES

Funcionalidades

- Acceso remoto (VNC,SSH,Terminal Service,..)
- VPN
- Control de Trafico (P2P,Voip..) I7Filter, QOS
- Panel de Administración Web
- Proxy Cache
- Control Parental (DansGuardian)
- Integración con usuarios LDAPs
- Correo Electrónico
- Ruteo, DNAT, SNAT....

IANUX SOLUCIONES

Que nos conviene?

- Utilizamos las soluciones existentes?
- Instalamos un Server desde 0?

Re:Cuales son las necesidades a cubrir?

- La información a custodiar es de vital importancia y necesitamos invertir en seguridad, Que debo tener en cuenta?
- Buscamos lograr una integración 100% con soluciones existentes en nuestra empresa, y queremos que dicha integración sea segura, que tenemos en cuenta?
- Me interesa la seguridad informática y tenemos tiempo para investigar, por donde empiezo?
- Que nivel de seguridad es el conveniente?

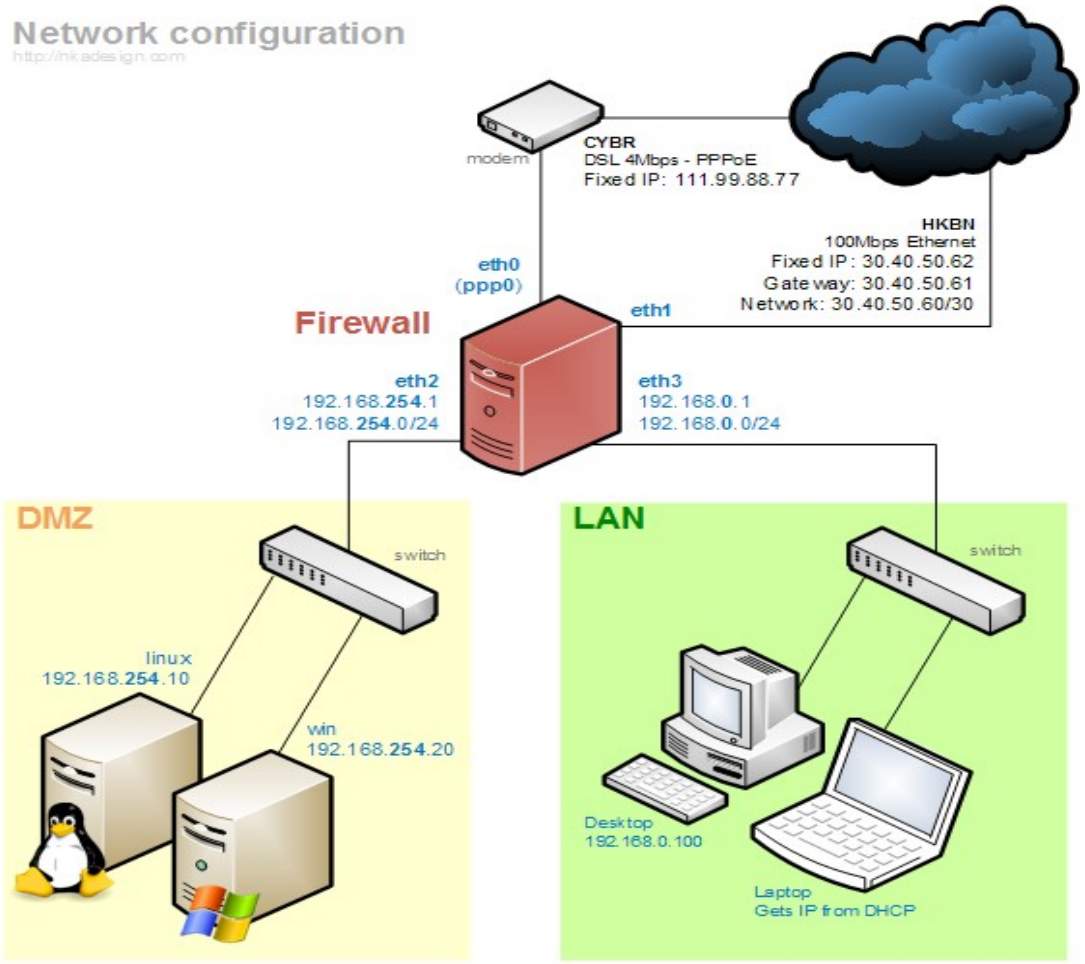
IANUX SOLUCIONES

Hardware Critico

- Placas de red
- Memoria RAM
- Disco Rigido
- Procesador

Esquema de Red 1

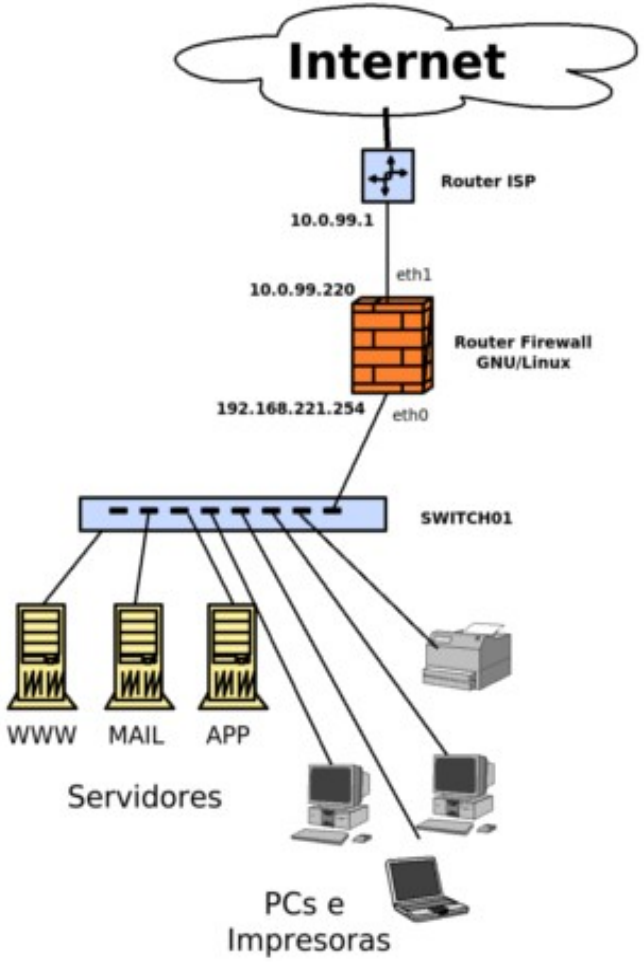
2 WAN+DMZ+LAN



ANUX SOLUCIONES

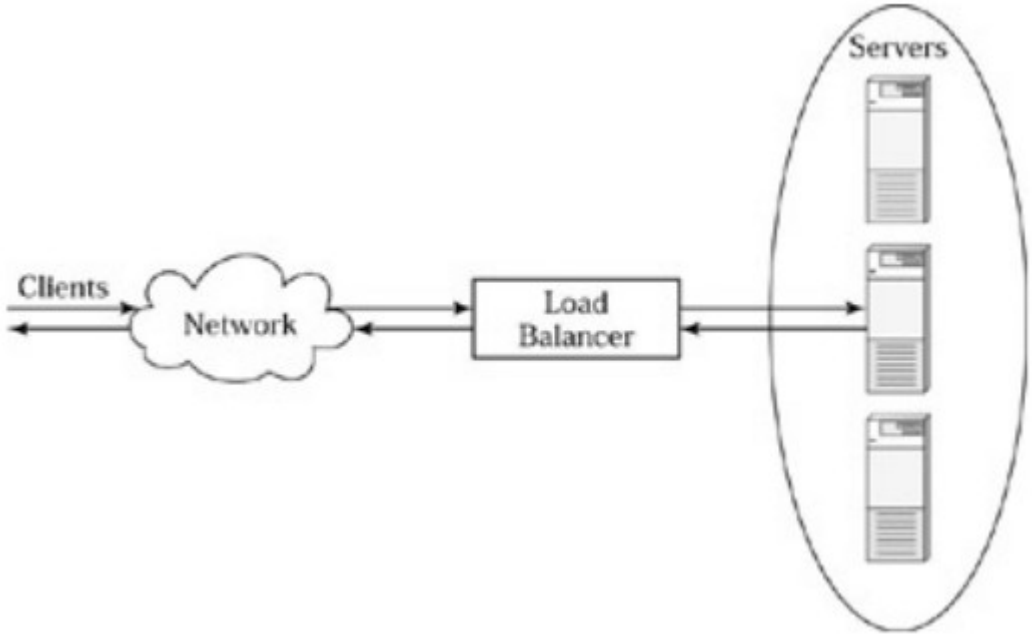
Esquema de Red 2

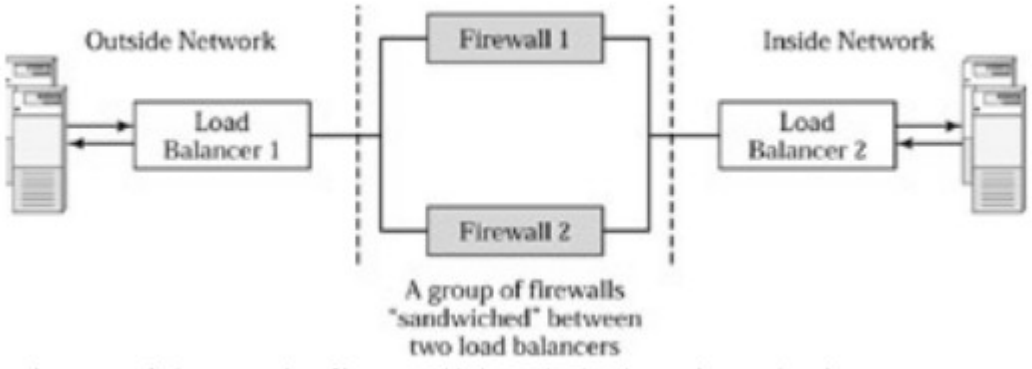
1 WAN+LAN



IANUX SOLUCIONES

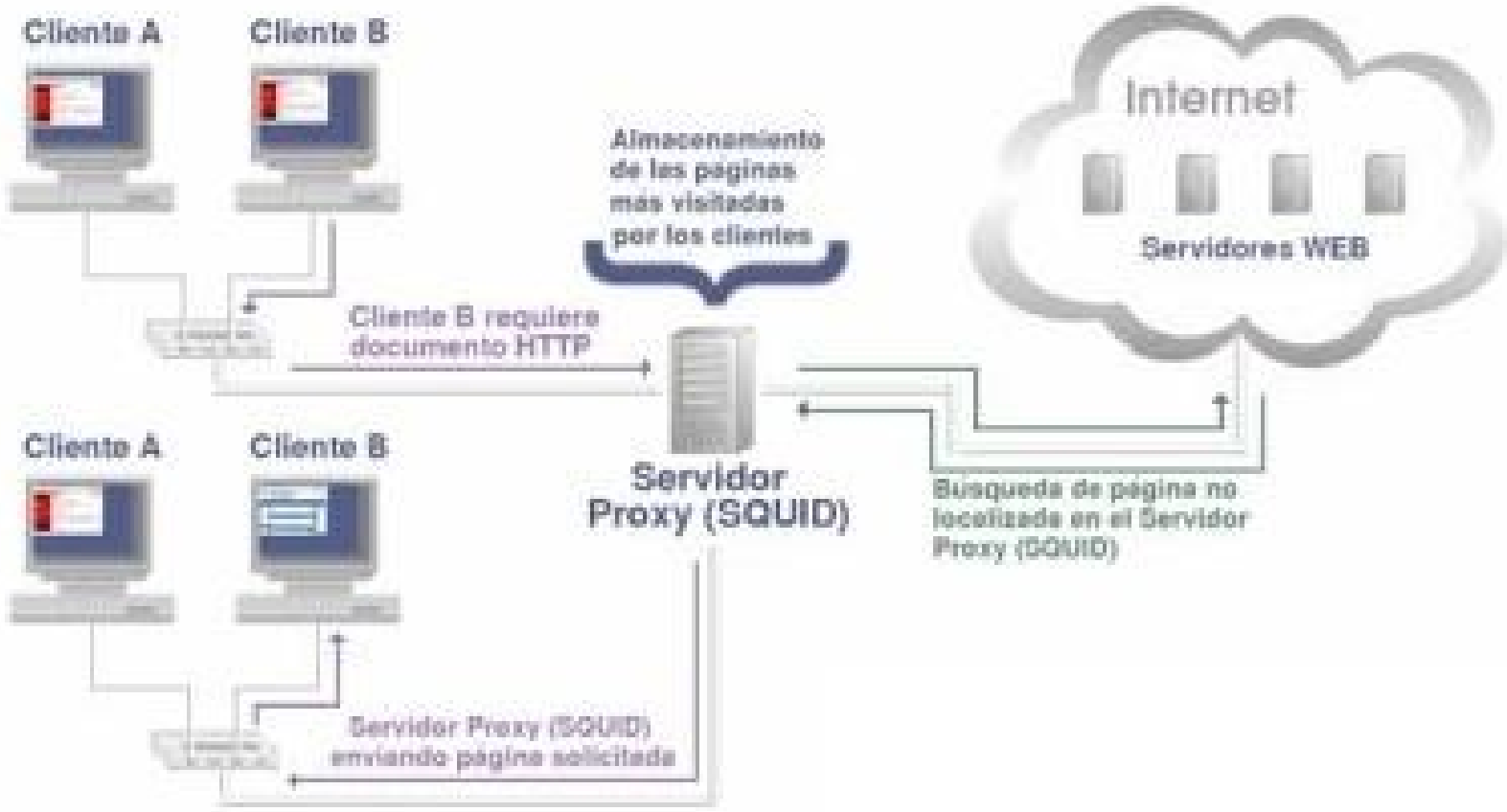
Load Balancer





IANUX SOLUCIONES

Proxy Cache



IANUX SOLUCIONES

Mini Taller

Agenda:

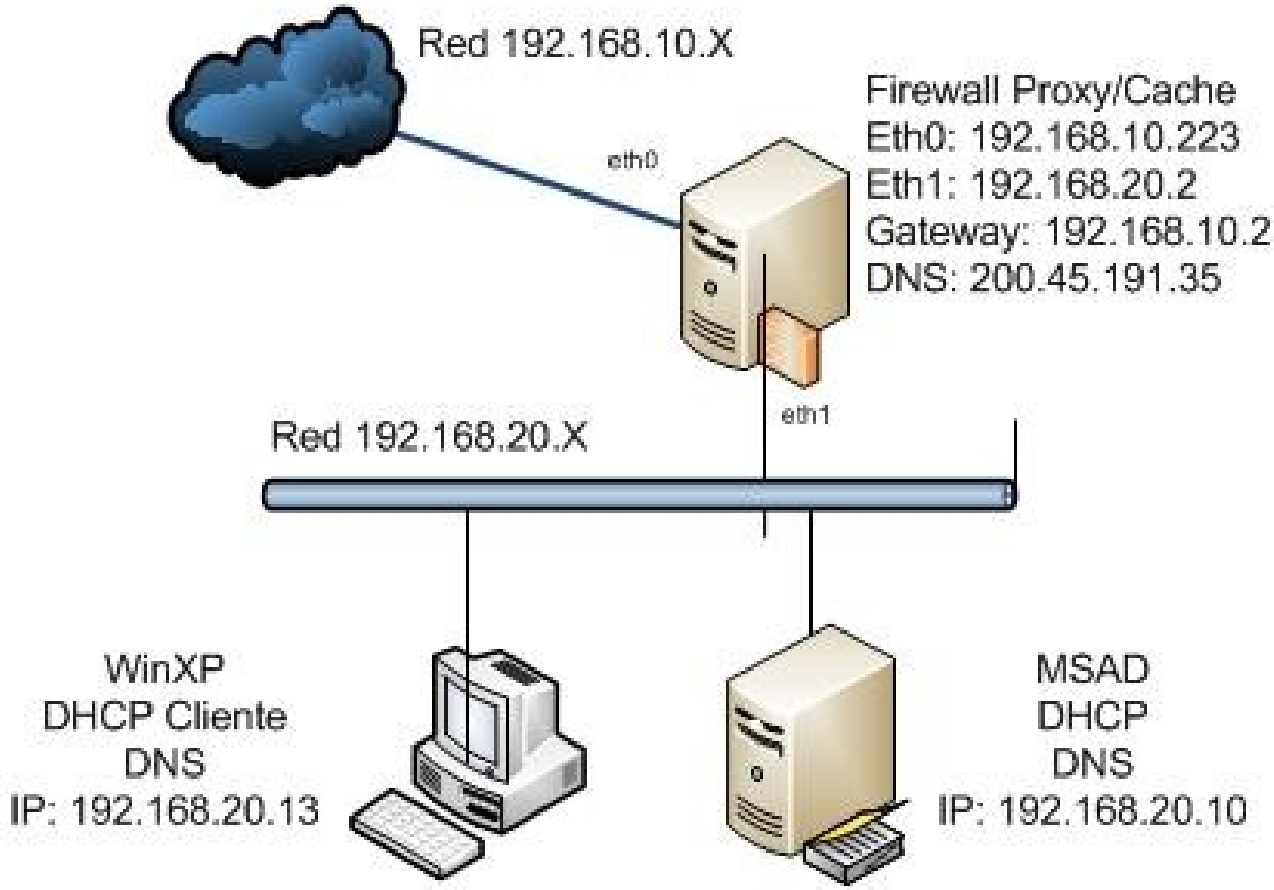
- Consejos y Recomendaciones para la instalación desde 0.
- Configuración de Placas de Red, DHCP SQUID Transparent, Shorewall
- Troubleshooting “Problemas Comunes”

Instalación desde 0

- Linux Debian
- Particionado Seguro
- Actualización Automática
- Backups Automáticos Local y Remoto
- Disaster Recovery (Mondo Rescue)
- Logs y notificaciones
- Control de integridad
- Hardening
- Configuración de los servicios de red
- Pentesting de cada Servicio

IANUX SOLUCIONES

Esquema Básico



IANUX SOLUCIONES

Particionado

[code][File: **/etc/fstab**]

```
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
/dev/sda1      /               ext3    nosuid,errors=remount-ro 0       1
/dev/sda7      /home           ext3    nodev,nosuid,noexec,usrquota,grpquota 0       2
/dev/sda2      /tmp            ext3    nodev,nosuid    0       2
/dev/sda6      /usr            ext3    nodev           0       2
/dev/sda5      /var            ext3    noatime,nodev,nosuid,noexec         0       2
/dev/sda7      /var/tmp        ext3    nodev,nosuid,noexec         0       2
/dev/sda8      /var/log                nodev,nosuid,noexec
none           /dev/shm        tmpfs   defaults,noexec,nosuid 0 0
/dev/sda9      /cache          reiserfs notail,noatime,nodev,nosuid,noexec 0       2
/dev/sda3      none            swap    sw              0       0
```

[/code]

IANUX SOLUCIONES

/etc/hosts

[code][File: **/etc/hosts**]

```
127.0.0.1       localhost.localdomain       localhost
127.0.1.1       gateway.local.com           gateway

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

[/code]

/etc/hostname

[code][File: **/etc/hostname**]

gateway.local.com

[/code]

/etc/network/interfaces

[code][File: **/etc/network/interfaces**]

```
auto lo
iface lo inet loopback
#WAN
auto eth0
iface eth0 inet dhcp
#LAN
auto eth1
iface eth1 inet static
post-down /usr/sbin/ethtool -s eth0 wol g speed 100 duplex full
address         192.168.27.1
netmask         255.255.255.0
broadcast 192.168.27.255
dns-nameservers 200.45.191.35 200.45.48.233 192.168.27.1
```

[/code]

Instalando Paquetes

[code][Ejecutar en Consola]

aptitude update; aptitude safe-upgrade; apt-get install sudo zsh vim-nox bzip2 ssh ntp ntpdate mutt ssmtp mc ethtool fail2ban iptables iproute perl squid3 dhcp3-server

[/code]

[code][Ejecutar en Consola]

chown proxy:proxy -R /cache/

[/code]

/etc/defaults/

[code][File: **/etc/defaults/dhcp3-server**]

INTERFACES="eth1"

[/code]

/etc/defaults/dhcp3-server

[code][File: **/etc/defaults/dhcp3-server**]

```
ddns-update-style none;
default-lease-time 86400;
max-lease-time 604800;
subnet 192.168.27.0 netmask 255.255.255.0 {
range 192.168.27.10 192.168.27.50;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.27.255;
option routers  192.168.27.1;
        option domain-name-servers              200.45.191.35, 200.45.48.233;
         option domain-name "local.com";
default-lease-time 600;
max-lease-time 7200;
}
```

[/code]

/etc/squid3/squid.conf

[code][File: **/etc/squid3/squid.conf**][Parte1]

```
emulate_httpd_log on
logfile_rotate 7
cache_store_log none
logformat squid %tl %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
pid_filename /var/run/squid.pid
access_log /var/log/squid3/access.log squid
cache_log /var/log/squid3/cache.log
cache_access_log syslog:local6.info
cache_store_log none
strip_query_terms off
log_mime_hdrs off
buffered_logs off
half_closed_clients off
server_persistent_connections off
forwarded_for off
```

[/code]

/etc/squid3/squid.conf

[code][File: **/etc/squid3/squid.conf**][Parte2]

#Debugging

debug_options ALL,1

#debug_options ALL,1 33,2

Configurar el puerto:

http_port 192.168.27.1:3128 transparent

visible_hostname gateway.local.com

Configurar el tamaño de los archivos a guardar en la caché

maximum_object_size_in_memory 512 KB

maximum_object_size 4 MB

memory_replacement_policy lru

cache_replacement_policy lru

quick_abort_min -1 KB

[/code]

/etc/squid3/squid.conf

[code][File: **/etc/squid3/squid.conf**][Parte3]

Configurar el tamañe la caché y el tipo de almacenamiento. Usamos .aufs. porque hemos visto que Squid funciona mejor, creando varios threads para manejo de los archivos:

cache_dir aufs /cache 19456 16 256

cache_effective_user proxy

cache_effective_group proxy

#El parátro cache_mem establece la cantidad de memoria para los objetos en transito, objetos frecuentemente utilizados y objetos negativamente utilizados en la cache este parametro esta limitado por la memoria RAM del sistema.

cache_mem 150 MB

Especificar los DNSs a usar. Esto es cuando se desea usar otros DNSs distintos a los que están indicados en /etc/resolv.conf:

dns_nameservers 200.45.191.35 200.45.48.223 192.168.27.1

[/code]

/etc/squid3/squid.conf

[code][File: **/etc/squid3/squid.conf**][Parte 4]

```
# Configurar los patrones de refresco (refresh_pattern). Esto debe ser configurado con cuidado.
# Debian
refresh_pattern -i \.deb$   129600 100% 129600
refresh_pattern -i \.udeb$   129600 100% 129600
refresh_pattern -i \.gz$   129600 100% 129600
refresh_pattern -i \.bz2$   129600 100% 129600
refresh_pattern changelogs.ubuntu.com/*  0  1% 1
# Imagenes
refresh_pattern -i \.gif$ 14400 80% 43200
refresh_pattern -i \.tiff?$ 14400 80% 43200
refresh_pattern -i \.bmp$ 14400 80% 43200
refresh_pattern -i \.jpe?g$ 14400 80% 43200
refresh_pattern -i \.xbm$ 14400 80% 43200
.....  pueden agregar mas...
```

[/code]

/etc/squid3/squid.conf

[code][File: **/etc/squid3/squid.conf**][Parte 5]

```
# Configurar una ACL que permita a los usuarios de la intranet hacer uso del proxy:
acl localhost src 127.0.0.1
acl intranet src 192.168.27.0/255.255.255.0
# Purgar Cache
acl PURGE method PURGE
http_access allow PURGE localhost
http_access deny PURGE
# Denegar Youtube
cache deny youtube
acl blacklist_webs url_regex "/etc/squid3/listas/blacklist_webs"
acl manager proto cache_object
http_access deny blacklist_webs
http_access allow intranet
http_access deny manager
http_access deny all
```

[/code]

Shorewall

[code][**Ejecutar en Consola**]

mkdir -p ~/paquetes/shorewall; cd ~/paquetes/shorewall/;

wget
http://www.shorewall.net/pub/shorewall/CURRENT_STABLE_VERSION_IS_4.4/shorewall-4.4.1

tar jxvf shorewall-4.*.tar.bz2; cd shorewall-4.*;

./install.sh

[/code]

[**Recomendación SQUID**]

32 MB RAM ----- 1GB CACHE en Disco # 256 descriptores ↔ 4 MB RAM

descriptor=(MemoriaTotal * 256) /4 =(256*256) /4=16384

Editar /etc/sysctl.conf y agregar (fs.file-max = 16384)

#Calculando la maxima cantidad de procesos por usuario

#max-limite-perproc=(fs.file-max /2)=16384/2=8192

Editar /etc/security/limits.conf y agregar lo siguiente:

* soft nofile 8192

* hard nofile 8192

[/Recomendación]

IANUX SOLUCIONES

Shorewall

[code][File: **/etc/shorewall/params**]

```
# Log level
LOG=ULOG
# Interfaz WAN
NET_IF=eth0
# Interfaz LAN
LAN_IF=eth1
# Subred LAN
LOC_SUBNET=192.168.27.0/24
# Sin Internet
LAN_NO=192.168.27.10,192.168.27.11,192.168.27.12,192.168.27.13.....
# Con Internet
LAN_SI=192.168.27.30,192.168.27.31,192.168.27.32,192.168.27.33.....
```

[/code]

Shorewall

[code][File: **/etc/shorewall/interfaces**]

```
#ZONE           INTERFACE          BROADCAST        OPTIONS
net     $NET_IF          detect
dhcp,blacklist,tcpflags,routefilter=1,nosmurfs,logmartians=1,nets=(!$LOC_SUBNET)
lan1    $LAN_IF          detect        dhcp,blacklist,tcpflags,nosmurfs,nets=($LOC_SUBNET)
```

[/code]

[code][File: **/etc/shorewall/zones**]

```
#ZONE    TYPE    OPTIONS       IN                    OUT
#                                OPTIONS               OPTIONS
fw       firewall
net      ipv4         #Zona Internet
lan1     ipv4    #Zona Local
```

[/code]

[code][File: **/etc/shorewall/masq**]

```
$NET_IF              $LOC_SUBNET
```

[/code]

IANUX SOLUCIONES

Shorewall

[code][File: **/etc/shorewall/policy**]

```
#SOURCE      DEST        POLICY      LOG LEVEL      LIMIT:BURST
# Policies for traffic originating from the local LAN (loc)
lan1         net         ACCEPT      $LOG
lan1         $FW         ACCEPT      $LOG
lan1         all         REJECT      $LOG
# Policies for traffic originating from the firewall ($FW)
$FW          net         ACCEPT      $LOG
$FW          lan1        ACCEPT      $LOG
$FW          all         REJECT      $LOG
# Policies for traffic originating from the Internet zone (net)
#net         lan2        DROP        info
net          $FW         DROP        $LOG
net          lan1        DROP        $LOG
net          all         DROP        $LOG        8/sec:30
# THE FOLLOWING POLICY MUST BE LAST
all          all         REJECT      $LOG
```

[/code]

IANUX SOLUCIONES

Shorewall

[code][File: **/etc/shorewall/rules**] [parte1]

```
#       Trafico originado en el Firewall (fw) con destino el Internet (net): fw2net
#
ACCEPT          $FW                     net                     tcp         80,443,5060,5061
ACCEPT          $FW                     net                     udp         53,123,5060,5061
ACCEPT          $FW                     net                     icmp        8
#       Trafico originado en el Internet (net) con destino el Firewall (fw): net2fw
ACCEPT:$LOG     net                     $FW             tcp     22,5060,5061
ACCEPT          net                     $FW             udp     53,464,5060,5061
ACCEPT          net                     $FW             icmp    8
#       Trafico originado en la LAN (loc) con destino el Firewall (fw)
ACCEPT:info     lan1                    $FW             tcp     22,3389,88,5060,5061
# Proxy Transparente
REDIRECT        lan1        3128        tcp         80      -       !192.168.27.99
ACCEPT          lan1        $FW         udp         53,123,3389,88,135,139,445,5060,5061
ACCEPT                      lan1        $FW         icmp        8
```

IANUX SOLUCIONES

Shorewall

[code][File: **/etc/shorewall/rules**][parte 2]

```
#       Trafico originado en la LAN (loc) con destino el Internet (net): loc2net
REJECT          lan1:$LAN_NO        net         tcp     80,110,143,443,587,993,1863,5323
ACCEPT          lan1:$LAN_SI        net         tcp     80              # HTTP
ACCEPT          lan1:$LAN_SI        net         tcp     22              # SSH
ACCEPT          lan1:$LAN_SI        net         tcp     21              # FTP
ACCEPT          lan1:$LAN_SI        net         tcp     25              # CORREO
ACCEPT          lan1:$LAN_SI        net         tcp     53              # DNS
ACCEPT          lan1:$LAN_SI        net         tcp     110              # POP3
ACCEPT          lan1:$LAN_SI        net         tcp     143              # IMAP
ACCEPT          lan1:$LAN_SI        net         tcp     443              # HTTPS
ACCEPT          lan1:$LAN_SI        net         tcp     587              # SMTP SUbmission
ACCEPT          lan1:$LAN_SI        net         tcp     993              # IMAP sobre SSL
ACCEPT          lan1:$LAN_SI        net         tcp     995              # POP3 sobre SSL
ACCEPT          lan1:$LAN_SI        net         tcp     1863             # MSN Messenger
ACCEPT          lan1:$LAN_SI        net         tcp     6667             # IRC
ACCEPT          lan1:$LAN_SI        net         tcp     5223             # Jabber SSL/TLS
```

[/code]

IANUX SOLUCIONES

Shorewall

[code][File: **/etc/shorewall/rules**][parte 3]

```
ACCEPT      $FW         lan1        tcp    22,53,88,135,139,445,5060,5061
ACCEPT      $FW         lan1        udp    88,5060,5061

SSH/ACCEPT  lan1        $FW
SSH/ACCEPT  $FW         lan1
Ping/DROP   net         $FW
Ping/ACCEPT lan1:$LAN_SI $FW
Ping/ACCEPT lan1:$LAN_SI net
Ping/DROP   lan1:$LAN_NO net
ACCEPT      $FW         net         icmp
ACCEPT      $FW         lan1        icmp
```

[/code]

Shorewall

[code][File: **/etc/shorewall/blacklist**]

```
$LAN_NO             udp          53
$LAN_NO             tcp          80,3128

   -                udp          1024:1862,1864:3127,3129:5221,5223:6666,6668:49151,49152:65535
   -                tcp          1024:1862,1864:3127,3129:5221,5223:6666,6668:49151,49152:65535
```

[/code]

[code][File: **/etc/shorewall/shorewall.conf**]

```
STARTUP_ENABLED=Yes
```

[/code]

[code][File: **/etc/default/shorewall**]

```
startup=1
```

[/code]

Quiero Mas!!!

- **PortKnocking**

  Alguien alguna vez toco una puerta para poder entrar en una casa?

  Que es? Como se toca la puerta?

- **SSL + PortKnocking**

  Cuando sus vecinos vieron como toca la puerta y donde deja la llave, Que medidas puede tomar?

- **Balanceo de Internet (Multi WANs)**

  /etc/shorewall/providers

  Alguien tiene N conexiones WAN y no sabe como utilizarlas en conjunto?

Dudas? | Preguntas?
Sugerencias ? | Reclamos?

Muchas Gracias

A todos, en especial a los organizadores por hacernos sentir muy cómodos

CCBOL 2010,

Trinidad Beni, Bolivia


60
70
80
x100
20
40
60
80
100
120
140
160
180
200
km/h
9500
H


PACEÑA


XVIII
Bol
2010

LPIC Oscar Gonzalez,
Consultor IT,
Security Researcher,
Instructor LPI Linux

MSN+Gtalk:
oscar.gonzalez@ianux.com.ar
oscar.gonzalez@saltalug.org.ar
Skype: gonzalez_oscar

Ing. Miguel Tolaba
Administrador de Red
Profesor de Sistemas Operativos

MSN + Gtalk
miguel@saltalug.org.ar