DISICO

Configuración de Bridge+Firewall con FreeBSD y OpenBSD

Manual

Configuración de Bridge+Firewall con FreeBSD y OpenBSD

¿Qué es un Bridge?

Un cable inteligente que conecta dos tarjetas de red. Un bridge es un dispositivo de software o de hardware usado para conectar dos segmentos de la red. No es semejante a un router, crea el aspecto de un segmento de la red sola grande. Con el bridge bajamos la tormenta de colisión en la red si usamos solo hubs.

¿Qué es un Firewall?

Un firewall es una barrera que controla el flujo del tráfico entre los hosts, los sistemas de redes, y los dominios. Existen diferentes clases, las más débiles y las más seguras, que deberían bloquear el paso de cualquier tipo de datos.

¿Para que un Bridge + Firewall?

Puedes utilizar un bridge para la creación de un firewall lógicamente transparente, ya que el bridge es configurado sin ip, no tiene acceso remoto. ¿Por que usar un bridge para hacer un firewall? tenemos una simple red conectada a Internet con un gateway para que un firewall funcione, todos los paquetes que entran y salen a la red tiene que pasar a través de él, si tu red esta creada con switch para forzar a todas las maquinas que pasen por el firewall tendrías que en un switch separar físicamente el firewall y el gateway que solo sean visible entre ellos, y el firewall también conectado a la red es como una vlan. Si no tienes el suficiente conocimiento para hacerlo tendrás que buscar ayuda de otra persona ;) (¿Un poco complicado?).

Con el bridge no tendrás la necesidad de dividir tu switch en dos, ya que simple mentes, cortaras o pondrás tu bridge en una salida del gateway y la otra salida al switch donde estaba dicho gateway anteriormente. Parece un poco ilógico a primera vista pero el bridge no usara ip y ni la red ni el gateway se darán cuenta que tienes el bridge de por medio (no sale más fácil así ?). Ya con tu bridge en el medio configures el firewall en el manejando las interfaces de las tarjetas de red. Esto de no usar ip tiene muchas ventajas ya que remotamente no tendrás acceso a el, si alguien quiere hacer un ataque al firewall no sabrá lógicamente donde este se encuentra y si nadie sabe que lo pusiste nadie notara la diferencia ;) . Desventaja no podrás controlarlo remotamente, pero si pones una tercera tarjeta de red con un ip o un alias en una de las ya puesta puedes entrar a el.

Cómo uso un Bridge+Firewall ?

Es fácil de usar solo se cortara la ruta físicamente que conecta el gateway o router con la red local y se pondrá. Me explico mejor con un pequeño grafico.

```
************
* Internet *
************
   |
***********
* Gateway *
***********
   |
***********
* Bridge  *
***********
   |
*************
* Red Local *
*************
```

Manos a la Obra... =)

Requisitos:

2 tarjetas de red de 100Mb/seg. Para tener una buena velocidad. Lo demás es cosa de una pc.

FreeBSD

Tienes que recompilar tu kernel de la siguiente forma:

```
# cd /usr/src/sys/i386/conf
# cp GENERIC BRIDGE
# vi BRIDGE
Agregar las siguientes opciones:
options BRIDGE
options IPFIREWALL
options IPFIREWALL_VERBOSE
options IPFIREWALL_FORWARD
```

Luego pasamos a compilar.

```
# /usr/sbin/config BRIDGE
# cd ../../BRIDGE
# make depend
# make
# make install
```

Tienes que tener paciencia en esto =)

Verifica que tus tarjetas de redes hayan sido detectadas por el sistema:

dmesg | more

Busca los devices de tus tarjetas... tales como xl0, xl1, ed0, ed1, etc.

A continuación la parte más difícil, es hacer el puente entre las dos tarjetas de red.

Editamos el archivo /etc/sysctl.conf agregando las siguientes líneas:

net.link.ether.bridge=1
net.link.ether.bridge_ipfw=1

OpenBSD

El OpenBSD por defecto no tiene que ser recompilado el kernel.

Manos a la obra ;-)

Es igual de difícil como lo fue con FreeBSD, solo tiene que editar los archivos correspondientes a tu tarjeta de red, en este caso usaremos a ep0 y ep1 como ejemplo.

editamos /etc/hostname.ep0

inet media 100BaseT up

editamos /etc/hostname.ep1

inet media 100BaseT up

editamos /etc/bridgename.bridge0

add ep0
add ep1
up

Para ver el trafico entre las tarjetas de red prueba con tcpdump. Acuérdate de hacer reboot ;)

Firewall

La configuración del firewall es común solo cambia un poco entre ipfw, pf y ipf

Para activar ipfw en FreeBSD:

Edita el archivo /etc/rc.conf y agregas estas líneas.

firewall_enable="YES"
firewall_type="/etc/rc.firewall"

donde /etc/rc.firewall tendrá tus reglas de firewall

Para activar el ipf o pf en OpenBSD:

Editamos el archivo /etc/rc.conf cambiando el "NO" a las líneas:

pf=NO

o

ipf=NO

Por "YES"

Las reglas estarán en /etc/ipf.rules o /etc/pf.config

Reglas comunes para el firewall:

*Con ipf

(ep0 y ep1 son mis tarjetas de red)

```
#  tu loopback está libre ;)

pass in quick on lo0 all

# bloqueo de paquetes fragmentados

block in quick all with frag

# bloqueo para mira las versiones del OS con nmap

block  in quick proto tcp all flags FUP

# bloqueo de paquetes no enrutados

block in quick on ep0 from 192.168.0.0/16 to any
block in quick on ep0 from 172.16.0.0/12 to any
block in quick on ep0 from 127.0.0.0/8 to any
block in quick on ep0 from 10.0.0.0/8 to any

# permiso para el paso de tcp/udp/icmp

pass  in quick on ep1 proto tcp from any to any flags S keep state
pass  in quick on ep1 proto udp from any to any keep state
pass  in quick on ep1 proto icmp from any to any keep state

# bloqueo el resto

block in quick all
```

Son unas simples reglas y puedes usarlas para ipfw con unos pequeños cambios.

Links :

http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/kernelconfig.html
http://www.daemonnews.org/200103/ipf_bridge.html
http://www.freebsd-howto.com/HOWTO/Ipfw-HOWTO
http://www.openbsd.org/faq/faq6.html#6.2
http://www.obfuscation.org/ipf/ipf-howto.txt