Configuración segura de FreeBSD como gateway/firewall.

Jesús Leal Elizondo.

jleal@freebsdmexico.org

Congreso de Software Libre
México D.F.

http://www.freebsd.org.mx

FreeBSD México

Requerimientos de FreeBSD como Gateway(puerta de enlace) .

Tener Instalado FreeBSD 4.9 (release de Producción) .

Minimo 2 tarjetas de red .

Compilar Kernel

Habilitar NAT (Network Address Translation)

Configurar Archivo de Reglas .

FreeBSD como Gateway .

-Debido a la estabilidad y confiabilidad de FreeBSD , son mas las empresas y personas que lo utilizan como su puerta de enlace al internet .

-Una puerta de enlace o "Gateway" es un sistema que se encarga de enviar paquetes de una interfaz a otra como por ejemplo : trafico de internet .

-Permite el manejo de Diferentes segmentos e Interfaces de red .

Por que Utilizar FreBSD como Gateway.

-Fácil configuración y administración .

-Permite el monitoreo del trafico de red.

-Restricción de trafico mediante politicas y manejo eficiente de los recursos .

Alta confiabilidad .

Gateway.

En el archivo /etc/firewall.rules se definen las politicas y reglas a seguir por nuestro gateway .

Si queremos un ambiente sin restricciones la configuración
será:

-f flush
add divert natd all from any to any via xl0
add pass all from any to any

Seguridad.

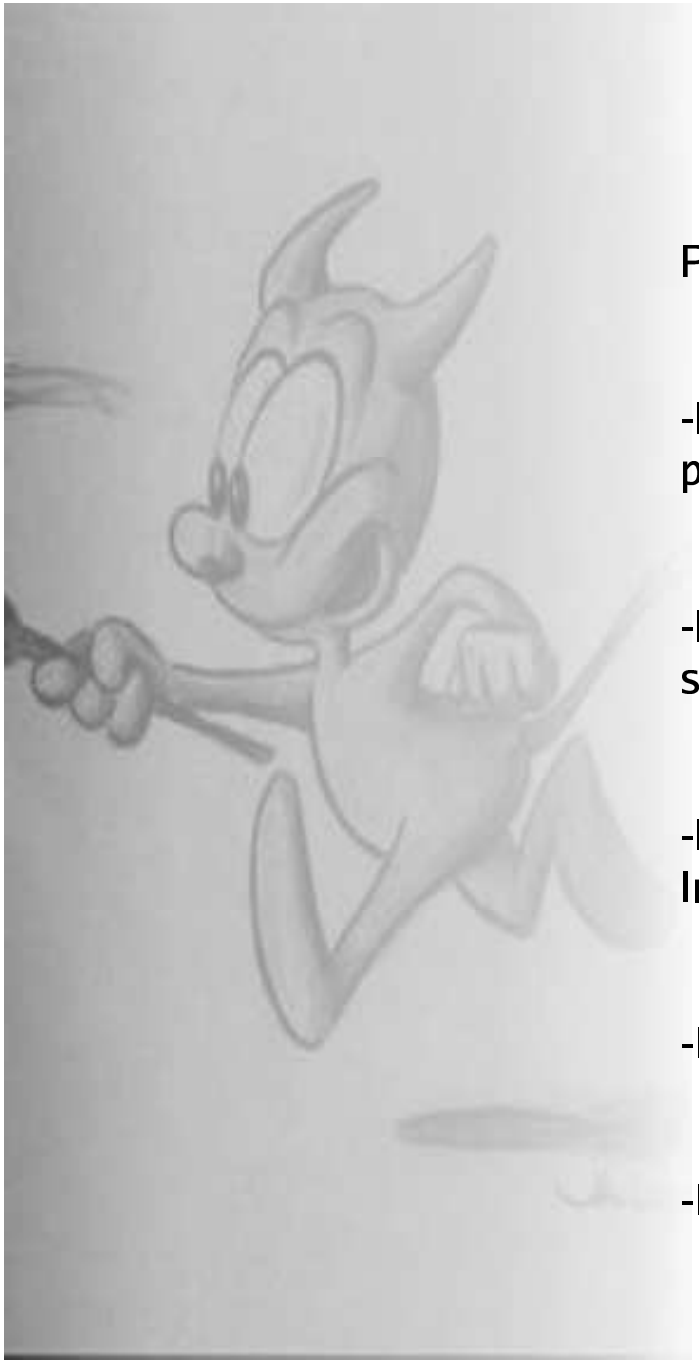
FreeBSD viene con seguridad Integrada por default .

Es posible Incrementar la seguridad .

FreeBSD maneja Niveles de seguridad predefinidos por el sistema .

Opciones de Cifrado y encriptado incluidas .

SSH (Secure Shell) Integrado .



Introducción.

Para tener un entorno seguro primero se debe :

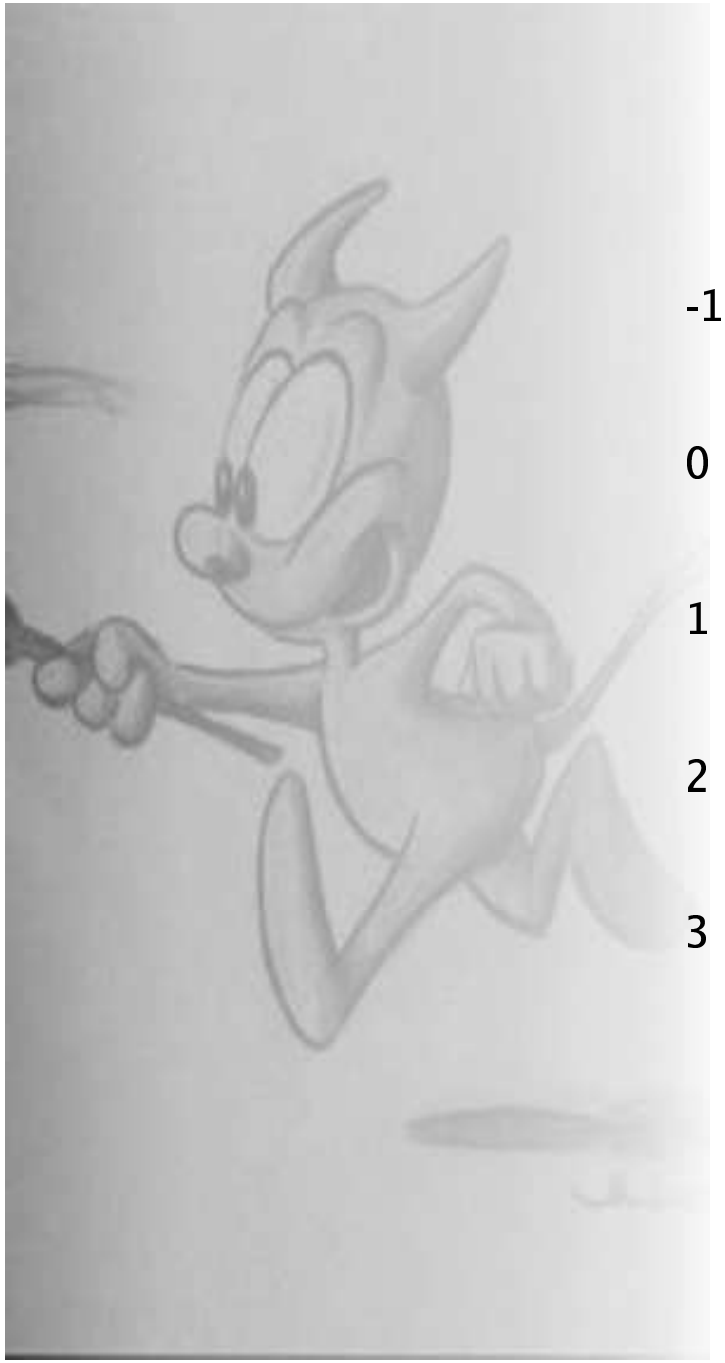
-Deshabilitar el software que es potencialmente peligroso .

-Parchar y actualizar el sistema contra errores de seguridad .

-Mantener respaldos actualizados acerca de la Información del Sistema.

-Instalar software de monitoreo del sistema .

-Evitar el uso de root en lo posible .



Niveles de Seguridad .

-1 Modo inseguro permanente (default) .

0 Modo inseguro.

1 Modo seguro.

2 Modo altamente seguro.

3 Modo seguro en red.

Consideraciones .

-Ataques de negación de servicios (DoS).

-Cuentas de usuario comprometidas.

-Puertas traseras (BackDoors).

-Posibilidad de acceder a root desde servidores remotos.

-Comprometer la cuenta de root mediante los usuarios .

Código fuente del sistema .

Utilerias para la seguridad.

-Snort.

-Acid.

-nessus.

-nmap.

-ethereal.

-tcpdump.

-sudo.

Seguridad en Passwords.

-El tipo de encriptado que viene por default en FreeBSD es el MD5 , que es ya algo antiguo , se debe sustituir este tipo de encriptado por uno mas actual llamado Blowfish (blf).

-Modificando :

/etc/auth.conf

/etc/login.conf

Monitoreo de Procesos.

Siempre es bueno saber exactamente que esta pasando en nuestro servidor así como que comandos fueron ejecutados por los usuarios.

Habilitamos en : /etc/rc.conf

accounting_enable="YES"

Podemos usar los comandos : lastcomm(1), y sa(8) para obtener las estadísticas de la base de datos de procesos .

SSH vs Telnet.

-SSH maneja todo el trafico y datos encriptados .

- Telnet no encripta , es decir utiliza texto plano para hacer transferencias .

KERNEL.

Añadimos al kernel :

options IPFIREWALL

options IPFIREWALL_VERBOSE

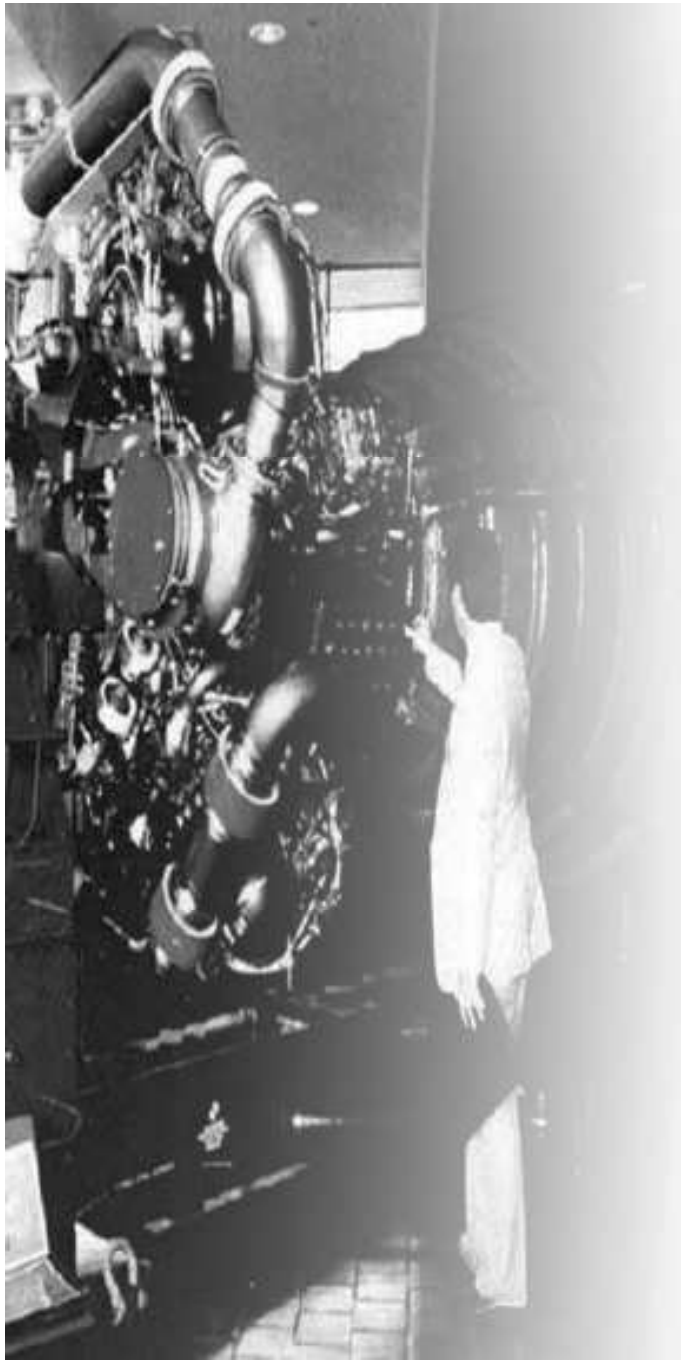
options IPSTEALTH

options RANDOM_IP_ID

Permisos.

-Es muy importante saber , que es lo que los usuarios pueden ver , por ejemplo no queremos que los usuarios tengan acceso al contenido de la carpeta de /root . Ejecutando un: "chmod 0750 /root" , impedirá que vean el contenido , a menos que se encuentren en el grupo Wheel .

-Si no queremos que los usuarios de Wheel tengan acceso al directorio ejecutamos un: "chmod 0700 /root" y con esto solo el usuario de root tendrá acceso a su directorio .



Ocultando Procesos.

-Se pueden limitar los procesos que los usuarios pueden ver cuando ejecutan el comando ps .

-Por default FreeBSD permite a los usuarios ver todos los procesos , incluidos los que NO les pertenecen .

-Ejecutamos el comando sysctl con la siguiente opción kern.ps_showallprocs=0 .

Firewall.

Utilidad :

-Bloqueo de paquetes .

-Bloqueo de Puertos .

-Restricción de Trafico .

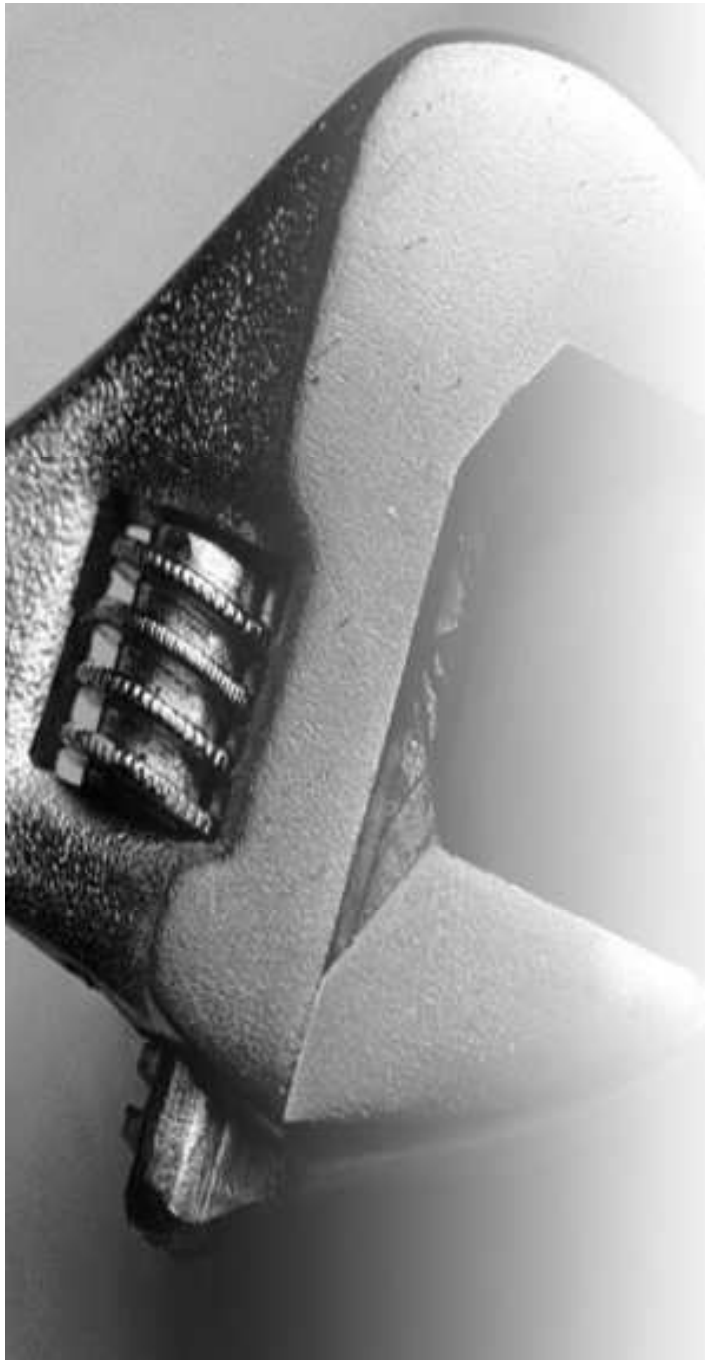
Configuración :

Se debe recompilar el kernel de FreeBSD con la opción :

IPFIREWALL .

Archivo de Configuración :

/etc/rc.firewall
/etc/firewall_rules
/etc/rc.conf



Ejemplos.

ipfw add pass all from $segmento_seguro to any

ipfw add pass all from any to $segmento_seguro

ipfw add deny all from $hackers to $segmento_seguro

ipfw add deny all from $alumnos to 200.56.43.0/24

M s información.

http://www.freebsd.org

http://www.freebsd.org.mx

http://www.eldemonio.org

http://www.google.com/bsd

http://www.defcon1.org

http://bsdvault.net