Configuración del Firewall en servidores de producción

Todo lo que he instalado está en sus rutas los binarios y los ficheros de configuración en /etc/csf. Los servicios son /etc/init.d/csf y /etc/init.d/lfd (ya están puestos en el runlevel).

Toda la config como ya digo está en /etc/csf, y nos interesan sobre todo el fichero principal “csf.conf” y los ficheros csf.*

Una guía rápida:

csf.allow: fichero donde dejaremos las IPs que no serán chequeadas por el sistema csf.conf: fichero principal de configuración csf.deny: se van metiendo las IPs que se irán bloqueando por el sistema (son bloqueos permanentes!! si alguien nos dice que no accede al server el primer sitio donde mirar es este). csf.ignore: ips que ignoraremos de los chequeos, solo está 127.0.0.1 y salvo causa mayor así debería ser csf.pignore: fichero donde meteremos los ejecutables o usuarios que el sistema ignorará (he metido el proceso de imap y el usuario nrpe). csf.tempban: lista las IPs baneadas temporalmente y la razón (segundo sitio donde mirar si alguien nos dice que no puede acceder al servidor) (es lo mismo que hacer “csf -t”

Comandos básicos: csf -t → lista las ips baneadas temporalmente csf -tr IP → desbanea una IP

csf -a → añade IP a lista blanca y csf.allow csf -d → añade IP a lista negra y csf.deny

/etc/init.d/csf restart (restartea el servicio) /etc/init.d/lfd restart (restartea el servicio)