1. Convertir el Sistema del Servidor en un Conmutador o Enrutador:

sudo echo "1" > /proc/sys/net/ipv4/ip_forward ---> Habilitar Temporalmente los Enrutamientos de Datos.

sudo cp -rpfv /etc/sysctl.conf /etc/sysctl.conf.default ---> Respaldar el Archivo Original del Control del Sistema.

sudo nano /etc/sysctl.conf ---> Abrir y editar el Control del Sistema.

net.ipv4.ip_forward=1 ---> Descomentar el Parámetro para Habilitar Permanentemente los Enrutamientos de Datos.

sudo reboot o shutdown -r now ---> Reiniciar el Sistema del Servidor para Aplicar los Cambios.

2. Descargar e Instalar Shorewall para el Firewall del Servidor:

Sitio Oficial del Shorewall: https://shorewall.org

Sitio de Descarga para Debian y Derivados: https://packages.debian.org/stable/net/

Shorewall: http://ftp.us.debian.org/debian/pool/main/s/shorewall/shorewall_5.2.3.2-1_all.deb

Shorewall-Core: http://ftp.us.debian.org/debian/pool/main/s/shorewall-core/shorewall-core_5.2.3.2-1_all.deb

Shorewall-Init: http://ftp.us.debian.org/debian/pool/main/s/shorewall-init/shorewall-init_5.2.3.2-1_all.deb

cd /tmp ---> Ir al Directorio Temporal para Descargar e Instalar Shorewall.

sudo wget http://ftp.us.debian.org/debian/pool/main/s/shorewall/shorewall_5.2.3.2-1_all.deb

sudo wget http://ftp.us.debian.org/debian/pool/main/s/shorewall-core/shorewall-core_5.2.3.2-1_all.deb

sudo wget http://ftp.us.debian.org/debian/pool/main/s/shorewall-init/shorewall-init_5.2.3.2-1_all.deb

sudo dpkg -i shorewall_5.2.3.2-1_all.deb ---> Instalar Shorewall.

sudo dpkg -i shorewall-core_5.2.3.2-1_all.deb ---> Instalar Shorewall-Core.

sudo dpkg -i shorewall-init_5.2.3.2-1_all.deb ---> Instalar Shorewall-Init.

3. Configurar Shorewall Firewall:

a. Copiar los Archivos de Configuración hacia al Directorio /etc/shorewall/:

cd /usr/share/shorewall/configfiles ---> Directorio de los Archivos de Configuración del Shorewall.

sudo cp -rpfv {accounting,actions,arprules,blrules,conntrack,ecn,hosts,interfaces,maclist,mangle,nat,netmap,params,policy,providers,proxyarp,routes,rtrules,rules,secmarks,shorewall.conf,snat,stoppedrules,tcclasses,tcdevices,tcfilters,tcinterfaces,tcpri,tunnels,zones} /etc/shorewall/

b. Respaldar los Archivos de Configuración (NO TODOS) para la Gestión del Firewall:

cd /etc/shorewall/ ---> Ir al Directorio del Shorewall.

sudo cp -rpfv shorewall.conf shorewall.conf.default ---> Respaldar el Archivo de Configuración General del Shorewall.

sudo cp -rpfv zones zones.default ---> Respaldar el Archivo para las Zonas de Red TCP/IP.

sudo cp -rpfv interfaces interfaces.default ---> Respaldar el Archivo para las Interfaces de Red TCP/IP.

sudo cp -rpfv snat snat.default ---> Respaldar el Archivo para el Enmascaramiento de Red TCP/IP.

sudo cp -rpfv policy policy.default ---> Respaldar el Archivo para las Políticas de la Red TCP/IP.

sudo cp -rpfv rules rules.default ---> Respaldar el Archivo para las Reglas (Filtros) de la Red TCP/IP.

c. Configurar los Archivos necesarios del Shorewall:

sudo nano shorewall.conf ---> Abrir para editar la Configuración General del Shorewall.

STARTUP_ENABLED=Yes ---> Parámetro para Habilitar el Levantamiento del Shorewall.

LOGFILE=/var/log/messages ---> Archivo para los Registros de los Filtros de Datos.

IPTABLES=/usr/sbin/iptables ---> Ruta para la Ejecución del Iptables mediante Shorewall.

DETECT_DNAT_IPADDRS=Yes ---> Parámetro para Habilitar el DNAT o el Port Forwarding.

DISABLE_IPV6=Yes ---> Parámetro para Deshabilitar el Protocolo de Internet versión 6.

FASTACCEPT=Yes ---> Parámetro para Acelerar los Filtros de Aceptación en las Reglas del Shorewall.

IP_FORWARDING=On ---> Parámetro para Permitir los Enrutamientos de Datos con Shorewall.

IMPLICIT_CONTINUE=Yes ---> Parámetro para Permitir la Continuidad Implícita de los Filtros de Datos.

ROUTE_FILTER=Yes ---> Parámetro para Permitir los Filtros de los Enrutamientos de Datos.

d. Editar el Archivo para las Zonas de Red TCP/IP:

sudo nano zones ---> Abrir el Archivo para las Zonas del Firewall.

ZONA TIPO

---

fw firewall

net ipv4

loc ipv4

e. Editar el Archivo para las Interfaces de Red TCP/IP:

sudo nano interfaces ---> Abrir el Archivo para las Interfaces del Firewall.

ZONAS INTERFACES OPCIONES

---

net ens32 dhcp,nosmurfs,tcpflags,routefilter,routeback

loc ens33 nosmurfs,tcpflags,routefilter,routeback

f. Editar el Archivo para el Enmascaramiento de Red TCP/IP:

sudo nano snat ---> Abrir el Archivo para el Enmascaramiento del Firewall.

ACTION ORIGEN DESTINO

SNAT(192.168.0.122) 192.168.10.0/24 ens32

g. Editar el Archivo para las Políticas de la Red TCP/IP:

sudo nano policy ---> Abrir el Archivo para las Políticas del Firewall.

ORIGEN DESTINO ACCION NIVEL DEL REGISTRO

---

fw all ACCEPT

net fw DROP info

loc fw DROP info

loc net DROP info

all all REJECT info

h. Editar el Archivo para las Reglas (Filtros) de la Red TCP/IP:

sudo nano rules ---> Abrir el Archivo de las Reglas del Firewall.

ACCION ORIGEN DESTINO PROTOCOLOPUERTO DESTINO

Reglas del WAN

?COMMENT Permitir desde cualquier Origen Enviar Señales ECHO hacia al Servidor FW

Ping(ACCEPT) all fw:192.168.0.122

?COMMENT Permitir solamente a MI PC conectarse al Servidor FW mediante SSH

ACCEPT net:192.168.0.2 fw:192.168.0.122 tcp 222

?COMMENT Permitir a la Red WAN Interna conectarse al Servidor FW mediante WEBMIN

ACCEPT net:192.168.0.0/25 fw:192.168.0.122 tcp 10111

#----------#

Reglas del LAN

?COMMENT Permitir a la Red Local enviar Señales ECHO hacia cualquier Destino

Ping(ACCEPT) loc:192.168.10.0/24 all

?COMMENT Permitir Comunicación en la Red Local mediante UDP con los Protocolos BOOTPS,BOOTPC,NETBIOS-NS,NETBIOS-DGM,NETBIOS-SN y MS-DS

ACCEPT loc:192.168.10.0/24 loc:192.168.10.0/24 udp 67,68,137,138,139,445

?COMMENT Permitir Comunicación en la Red Local mediante TCP con los Protocolos NETBIOS-NS,NETBIOS-DGM,NETBIOS-SN y MS-DS

ACCEPT loc:192.168.10.0/24 loc:192.168.10.0/24 tcp 137,138,139,445

?COMMENT Permitir al Servidor AD conectarse y administrar al Servidor FW mediante SSH y WEBMIN

ACCEPT loc:192.168.10.1 fw:192.168.10.254 tcp 222,10111

?COMMENT Obligar al Servidor AD sincronizar el Tiempo mediante NTP solamente con el Servidor FW

NTP(ACCEPT) loc:192.168.10.1 fw:192.168.10.254

?COMMENT Obligar a la Red Local sincronizar el Tiempo mediante NTP solamente con el Servidor AD

NTP(ACCEPT) loc:192.168.10.0/24 loc:192.168.10.1

?COMMENT Permitir el DNS Forwarder del Servidor AD peticionar DNS hacia cualquier Servidor DNS Externo

DNS(ACCEPT) loc:192.168.10.1 net

?COMMENT Obligar a la Red Local peticionar DNS solamente con el Controlador de Dominio del Servidor AD

DNS(ACCEPT) loc:192.168.10.0/24 loc:192.168.10.1

?COMMENT Permitir a la Red Local conectarse al Internet mediante UDP con los Puertos Aleatorios

ACCEPT loc:192.168.10.0/24 net udp 1024-65535

?COMMENT Permitir a la Red Local conectarse y navegar en la Internet con los Protocolos HTTP, HTTPS y Puertos Aleatorios

ACCEPT loc:192.168.10.0/24 net tcp 80,443,1024-65535

4. Habilitar y Levantar el Shorewall Firewall:

sudo nano /etc/default/shorewall ---> Editar la Configuración por Defecto del Shorewall

startup=1 ---> Parámetro para levantar el Shorewall durante el Booteo del Sistema.

sudo systemctl is-enabled shorewall ---> Revisar si el Shorewall está habilitado o Deshabilitado.

sudo systemctl enable shorewall ---> Habilitar el Shorewall.

sudo systemctl start shorewall ---> Levantar el Shorewall

5. Revisar el Shorewall en el Webmin.

Networking ----> Shorewall Firewall.