Hete aquí las susodichas:

```
#!/bin/bash

# Limpiar todas las reglas actualmente establecidas en el servidor:
iptables -F
iptables -X

# Establecer la política de filtros, para Denegar todo por defecto:
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Aceptar todas las peticiones entrantes por HTTP al servidor web por el puerto 80 desde cualquier sitio
iptables -A INPUT -p tcp -s 0/0 –sport 1024:65535 -d 192.168.0.10 –dport 80 -m state –state NEW,ESTABLISHED -j
ACCEPT

# Aceptar todas las respuestas salientes por HTTP desde el servidor web por el puerto 80 a cualquier sitio
iptables -A OUTPUT -p tcp -s 192.168.0.10 –sport 80 -d 0/0 –dport 1024:65535 -m state –state ESTABLISHED -j ACCEPT

# Aceptar todas las peticiones entrantes por HTTPS al servidor web por el puerto 443 desde cualquier sitio
iptables -A INPUT -p TCP -s 0/0 –sport 1024:65535 -d 192.168.0.10 –dport 443 -m state –state NEW,ESTABLISHED -j
ACCEPT

# Aceptar todas las respuestas salientes por HTTPS desde el servidor web por el puerto 443 a cualquier sitio
iptables -A OUTPUT -p tcp -s 192.168.0.10 –sport 443 -d 0/0 –dport 1024:65535 -m state –state ESTABLISHED -j ACCEPT

# Aceptar conexiones entrantes SSH SOLAMENTE desde la dirección IP de administración (192.168.1.10) al servidor web
en el puerto 22 TCP
iptables -A INPUT -p tcp -s 192.168.1.10 –sport 1024:65535 -d 192.168.0.10 –dport 22 -m state –state
NEW,ESTABLISHED -j ACCEPT

# Aceptar todo el trafico SSH saliente SOLAMENTE desde el servidor web en el puerto 22/TCP la dirección IP de
administración
iptables -A OUTPUT -p tcp -s 192.168.0.10 –sport 22 -d 192.168.1.10 –dport 1024:65535 -m state –state ESTABLISHED -
j ACCEPT

# Finalmente, de forma explicita definir que todo el trafico entrante y/o saliente que no coincida con los
criterios anteriormente declarados, deben ser borrados
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
```