5) a)

	red interna	server	internet
red interna	X	HTTP, HTTPS DNS	DROP
server	DROP	X	DROP
internet	DROP	DNS, HTTP HTTPS	X

- DNS debe responder consultas de internet
- Internet debe poder conectarse al web server (aunque todo de manera segura como no segura)
- La red interna debe poder conectarse al server (ambas seguras y no seguras)
- DNS debe responder consultas de la red interna.

Suponiendo que el server DNS tiene IP 8.8.8.8 y el server web tiene IP 100.100.100.100, las reglas quedarían de la siguiente forma:

red interna → < 192.168.0.0, *, 100.100.100.100, 80, TCP > HTTP red local → web server

< 192.168.0.0, *, 100.100.100.100, 443, TCP > HTTPS red local → web server

< 192.168.0.0, *, 8.8.8.8, 53, UDP > DNS red local → dns server

< internet, *, 100.100.100.100, 80, TCP > HTTP internet → web server

< internet, *, 100.100.100.100, 443, TCP > HTTPS internet → web server

< internet, *, 8.8.8.8, 53, UDP > DNS internet → dns server

b) La autoridad certificante firma el certificado para el servidor con la clave privada de CA. Los clientes se conectan al server de forma segura realizando el handshake TLS/SSL. En este handshake el server le manda el certificado al cliente y el cliente con la clave pública de CA desencripta el certificado. Luego de esto obtiene un hash que fue aplicado sobre la clave pública del server y su identidad, el cliente, que recibió estos 2 parámetros desde el server aplica la función de hash y compara con la del certificado desencriptado. Si la comparación es correcta, el cliente puede confiar que el servidor es quien dice ser.

NOTA