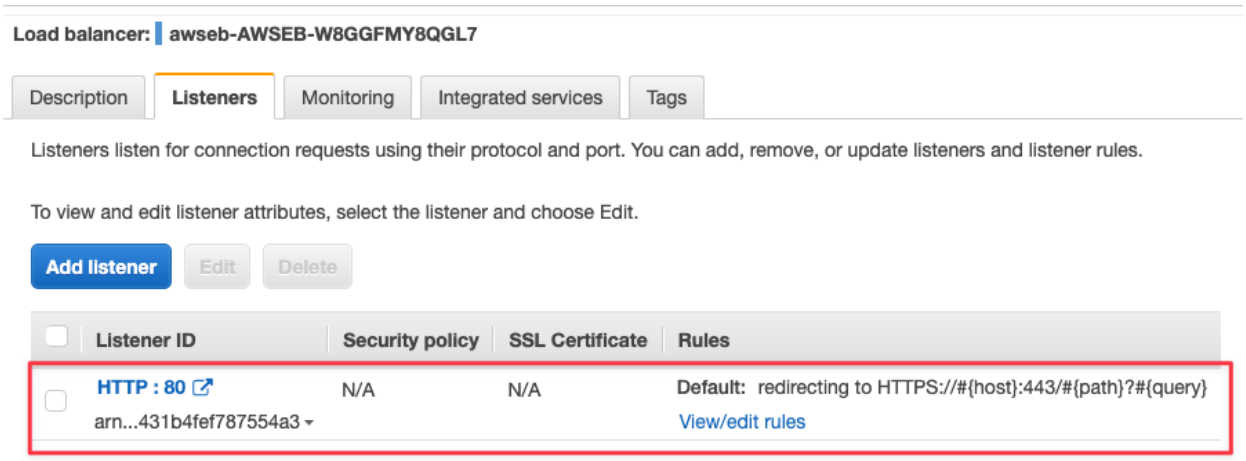
Listener Rules and Redirecting

As mentioned in the previous sections, Application Load Balancers (ALBs) have the ability to perform complex routing decisions, directing incoming traffic to appropriate backend services. Well, ALBs are able to make said decisions through the use of **Listeners** and **Listener Rules**.

Listeners are the processes that check for connection requests using the port and protocol we specify. Said listeners have a set of **rules**, called listener rules defined within them that determine how the load balancer should route requests to its registered **targets**. Both Listener Rules and their targets have to be defined by the cloud administrators when an Application Load Balancer (ALB) is being being created.

Listen Rules and ALBs allow us to perform a great many functions in conjunction beyond just simple traffic routing. One such function is the ability of ALBs to redirect HTTP requests to HTTPS, ensuring that all traffic is transmitted with the extra layer of security provided by HTTPS. Another such function is request manipulation, that is, the ability of Listener Rules to be able to modify the contents of a request before they reach backend services by, for example, adding headers to them. Request manipulation can prove especially handy when dealing with, say, CORS restrictions (a major source of headache for many people around the world).

An example of a Listener that checks for connections requests using HTTP on port 80, and redirects said request to HTTPS is shown below:



A listener rule for redirecting from HTTP to HTTPs (Source: Vanta)

TLDR;

Listener Rules are the conditions set on an ALB that determines how requests should be handled. Used to redirect HTTP to HTTPS; Can also add headers to requests.