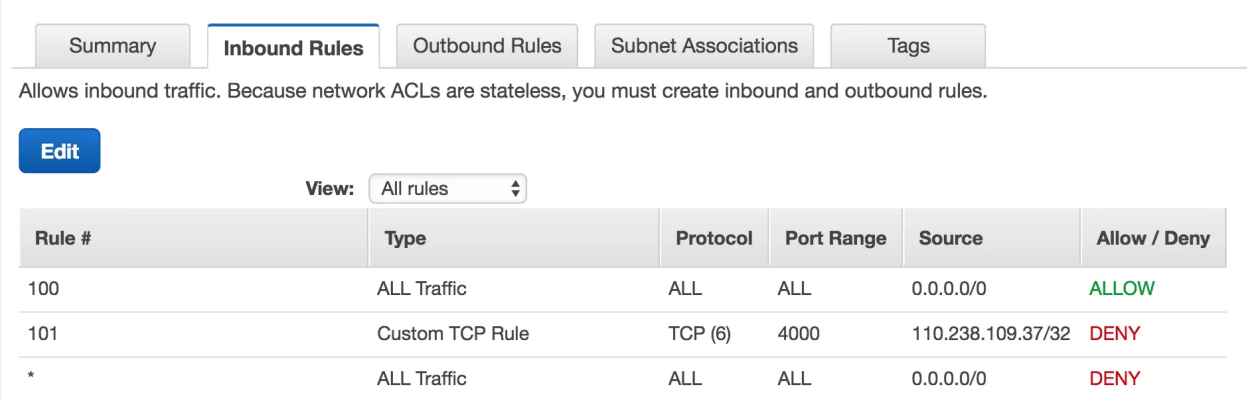
NACL/SG Rule priority

Both NACLs and Security Groups have been discussed in the last section and how they rely on a sequence of rules. In order to better understand how these rules are organized and evaluated, an example set of NACL inbound rules are given below:



Summary | **Inbound Rules** | Outbound Rules | Subnet Associations | Tags

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

View: All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	Custom TCP Rule	TCP (6)	4000	110.238.109.37/32	DENY
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Source: TutorialsDojo

Lower the rule number, the higher priority it is treated with. The “*” rule in particular being the lowest priority and highest number rule. For example, the “*” rule as shown in the image is the default and lowest rule of the NACL. Additionally, higher priority rules will overpower lower priority ones. In the list of rules present in the above example, rule “100“ will be called first, then “101“, then “*“. So, because all traffic goes through rule 100 first, any and all inbound requests will be passed through regardless of protocol or port range.

A similar format is followed for the organization and evaluation of NACL Outbound rules and Security Groups as well, and therefore I shall refrain from regurgitating the same set of information for the aforementioned categories.