Firewall Rules for Connectionless Protocol / Two Way Firewall Rule (Reverse Rule)

Generally, when we configure access via firewall policy, we configure a permit access rule from source to destination. This allows the traffic to be initiated from source to destination and also allows response from destination to source for the service we allowed.

Single access rule works successfully for services using connection oriented protocols like TCP, but not for connection-less protocols like UDP, ESP, etc. In case of connectionless protocols, we have to create two way firewall rule, to allow traffic from either way, which means we need to add another reverse access rule from destination to source, as there is no way for firewall to associate traffic in both direction with a particular session.

Connection-oriented protocols create a session/connection before actual data interchange starts. Firewalls can sniff TCP/IP handshake or in case of NAT they initiate a new connection to destination on behalf of source. Either way, whenever a connection is initiated from source to destination through a firewall, critical information unique to that connection is saved in a state table by Firewall. It consists of source IP, source port, destination IP and destination port. In case of NAT, more information is stored. So when a response is received by firewall from destination, it checks it state table for an existing connection initiated by source. Firewall will forward this response only if:

1. The response is from destination IP and destination port in state table.
2. Response is directed to source IP and source port in state table.

But in case of connection-less protocol, there is no handshake, no sessions are created, each packet is an individual packet. So from source to destination it allows traffic if a matching rule is found, and for response from destination to source a matching rule is required, otherwise the response will be blocked.

So in case of connectionless protocols we need to create reverse firewall access rule to allow two way communication.

However, many firewalls can take care of some well known connectionless services like DNS and can track DNS responses for given requests without requiring any reverse rule. And if there is any such support in firewall it is recommended to use it. Then it is better not to create reverse rules. How they do it, is specific to firewall vendor. For example you can check this link how Juniper handles this.