

# Security Group Structure

A **security group** acts as a virtual firewall that controls the traffic for one or more instances. Instances are associated with one or more security groups. Rules can be added to each security group to allow traffic to or from its associated instances. Rules for a security group can be modified at any time; the new rules are automatically applied to all instances that are associated with the security group. When deciding whether to allow traffic to reach an instance, all of the rules from all the security groups that are associated with the instance are evaluated.

Security group structure should be given in-depth consideration in the design and planning of AWS infrastructure. It is the primary security control and differs from traditional firewalls. Security groups do act as stateful firewalls but they are bound to the instance rather than a choke point like a traditional firewall appliance. They are permit only and can reference the presence of a security group on another object.

AWS Security group documentation can be found at the following link: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html>

Notre Dame's implementation can be found in the Security resources box folder in the document [AWS Security Groups Guidance for Practitioners](#).