Security Groups & NACLs

What's the difference and when do you use each?

So, what are they?

NACL

- NACL = Network Access Control List
- Applies to a Subnet
- Acts as a Packet Filter against an ORDERED rule set
- Stateless – NACL's require both INBOUND and OUTBOUND rules
- Good for controlling OUTBOUND traffic from a locked down subnet i.e. controlling what a server can access
- Defaults to all ALLOW

Security Groups

- SG for short
- Applies to objects. Eg you can associate an SG for an EC2 or a Load Balancer
- Can be applied to IP's or CIDR's
- Stateful – replies/responses are automatically allowed
- Requires explicit ALLOW as everything is automatically all DENIED

Stateful/Stateless?

NACL - Stateless

- If you wanted to allow HTTP/80 traffic to your subnet, and for your instances to also communicate over HTTP/80, you'd require both an INBOUND and OUTBOUND rule for HTTP/80

SG – Stateful

- If you allow HTTP/80 traffic to an instance, responses are auto-allowed

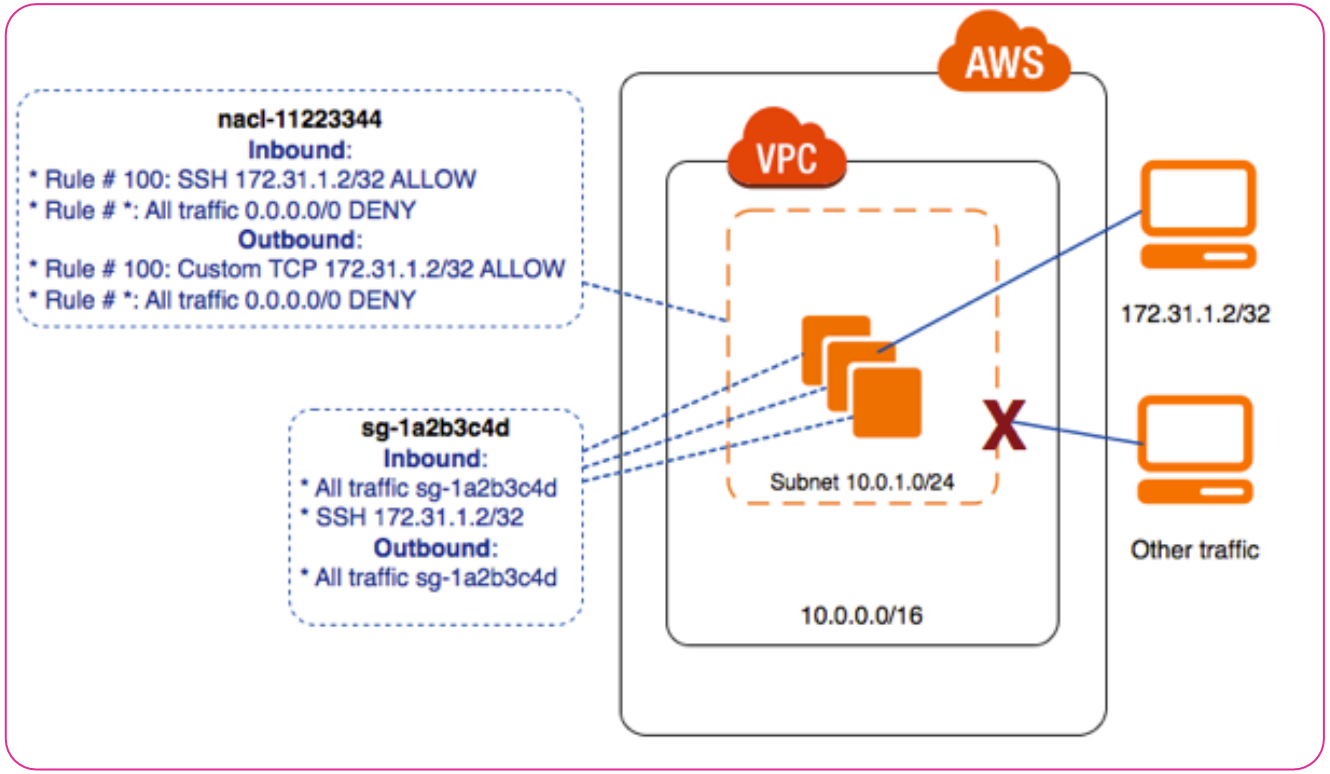
Considerations for NACLs

MISCONFIGURED RULES CAN MEAN INEFFECTIVE RULES

WILDCARD DENY RULE - TO COVER ANY RULES THAT AREN'T COVERED

DEFAULT VPCS ALLOW ALL TRAFFIC – THIS IS TO MAKE IT BEGINNER FRIENDLY

NACL example



What are we using today?

- SG only, keeping the default NACL
- SG will be created for the following:
  - Webservers
    - Port 80
    - ICMP
  - Application Load Balancer
    - HTTP
    - HTTPS
    - ICMP