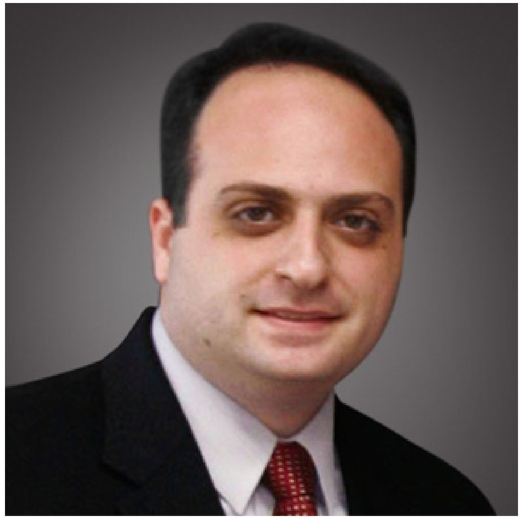
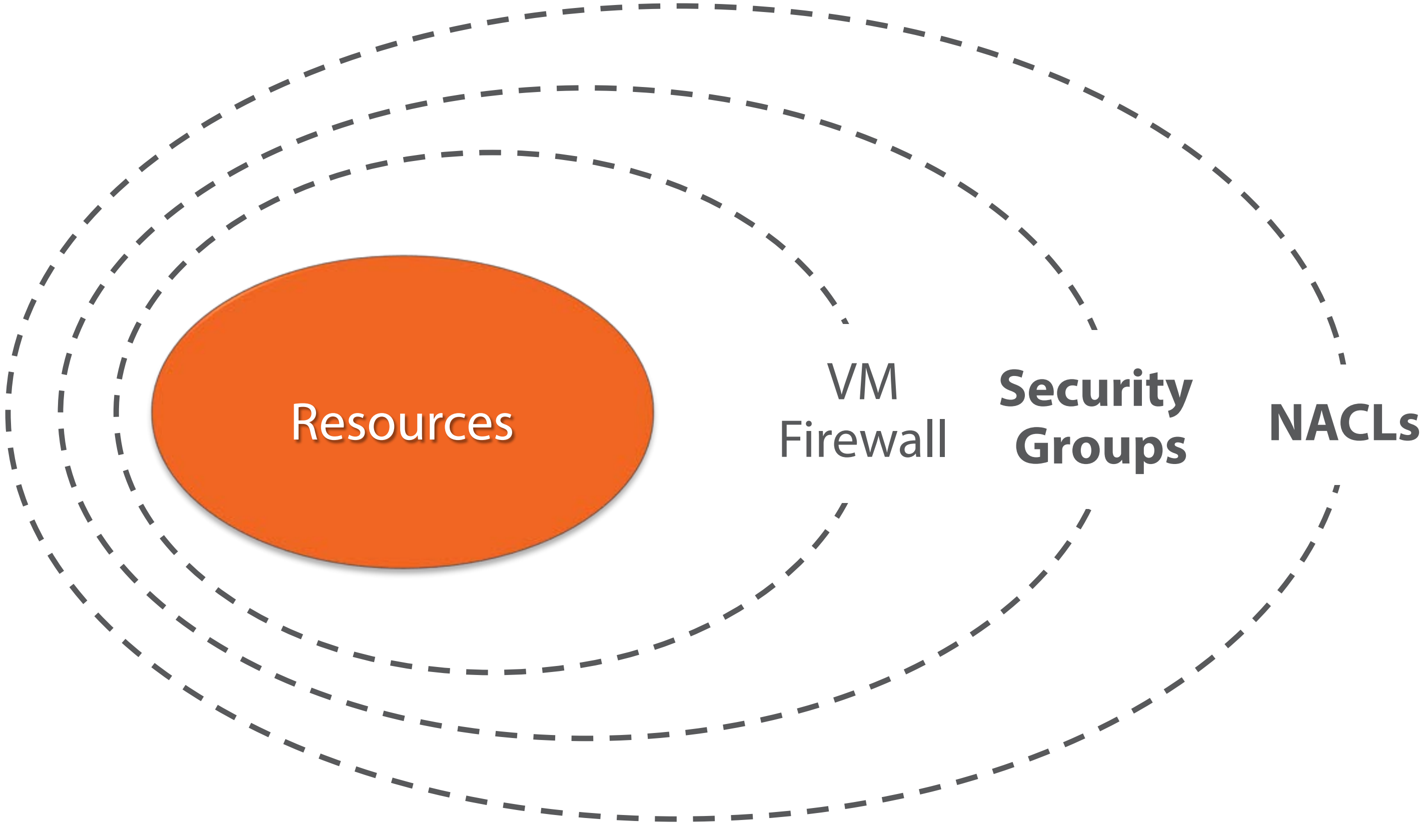
Working with Security Groups and NACLs



Elias Khnaser

@ekhnaser | www.eliaskhnaser.com

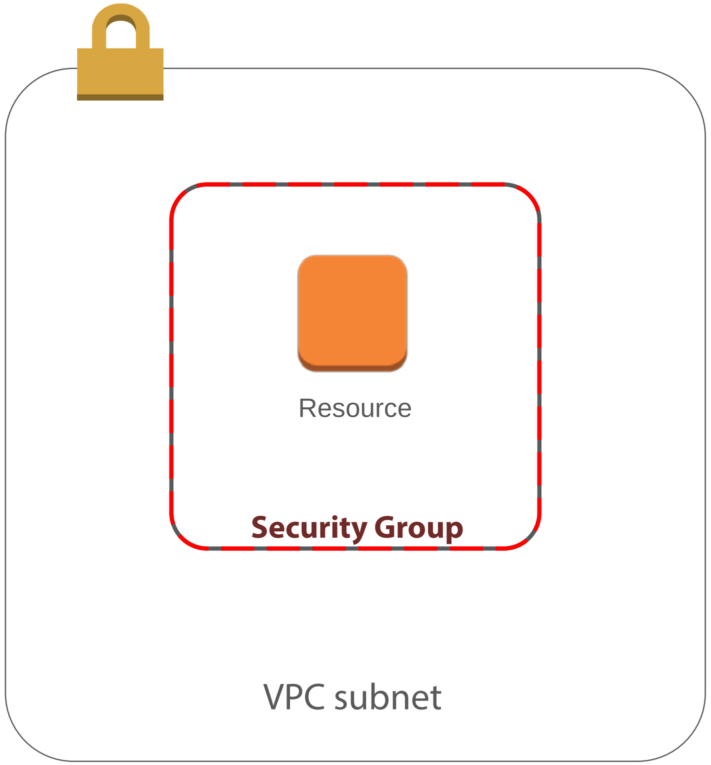
Layered Security



Security Groups and NACLs

Security Groups

- Resource level traffic firewall
  - Instance, ELB, etc…
- Ingress and Egress
- Stateful
  - Return traffic allowed



Network Access Control Lists

- Subnet level traffic firewall
  - Separate inbound and outbound rule set
- Source and Protocol filtering
- Stateless
  - Traffic strictly filtered

Understanding Security Groups

Resource
Security Group

Resource level traffic firewall

SG maximums:

- Up to 100 security groups per VPC
- Up to 50 lines in each SG
- Up to 5 SG per instance

Understanding Security Groups

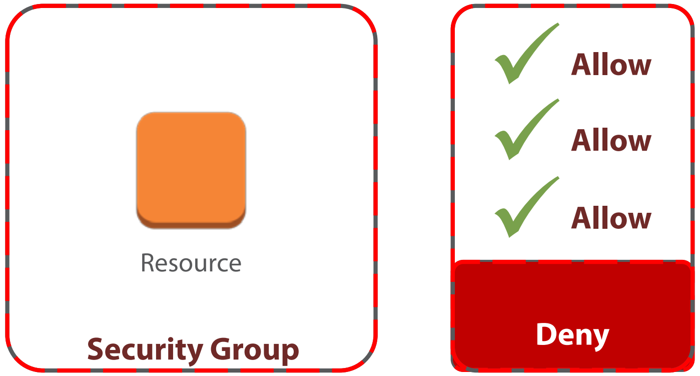
Resource
Security Group

Instances can't communicate unless allowed

Default SG allows communications from other instances in the same SG

Destination port filtering only (no source port filtering)

Security Groups and NACLs



Resource

Security Group

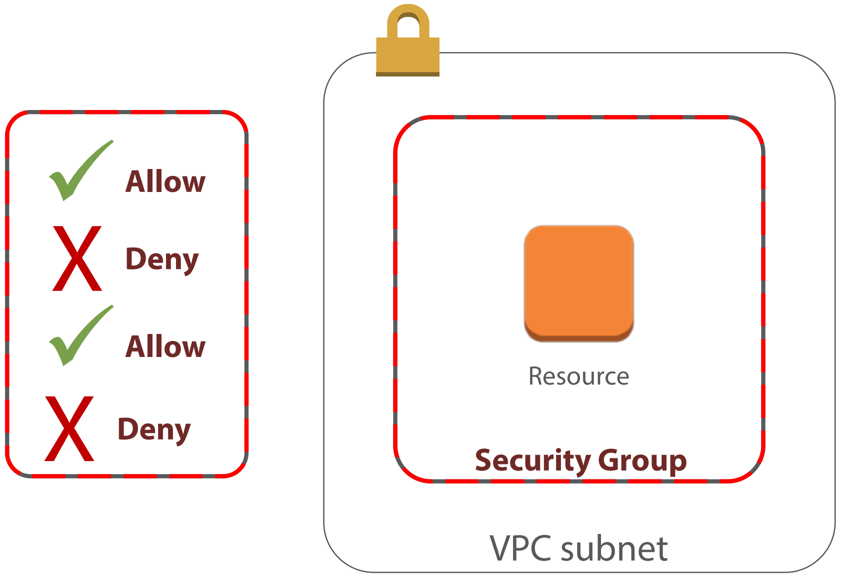
✓ Allow

✓ Allow

✓ Allow

Deny

- Deny all inbound until allow
- Allow rules only
- Allow all outbound until allow
- SGs are Stateful - return traffic allowed



✓ Allow

✗ Deny

✓ Allow

✗ Deny

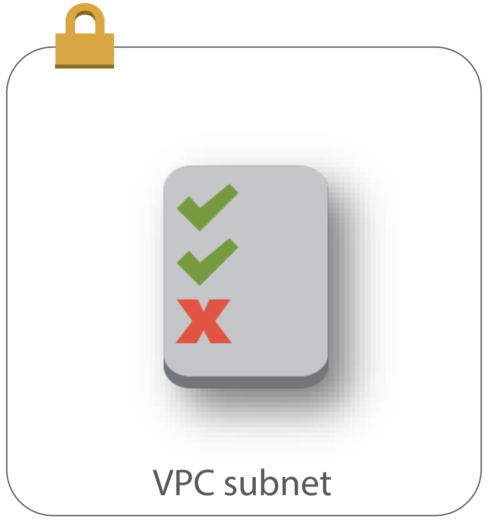
Resource

Security Group

VPC subnet

- Default rule: deny all
- Can have permit and deny rules
- One NACL per subnet
- NACLs are stateless - Traffic strictly filtered

Understanding Network Access Control Lists (NACLs)



Subnet level traffic firewall

Are a list of rules

- Lower numbers are processed first
- Stop on first match

Separate inbound / outbound rules

Summary

Understanding Security Groups

Understanding NACLs