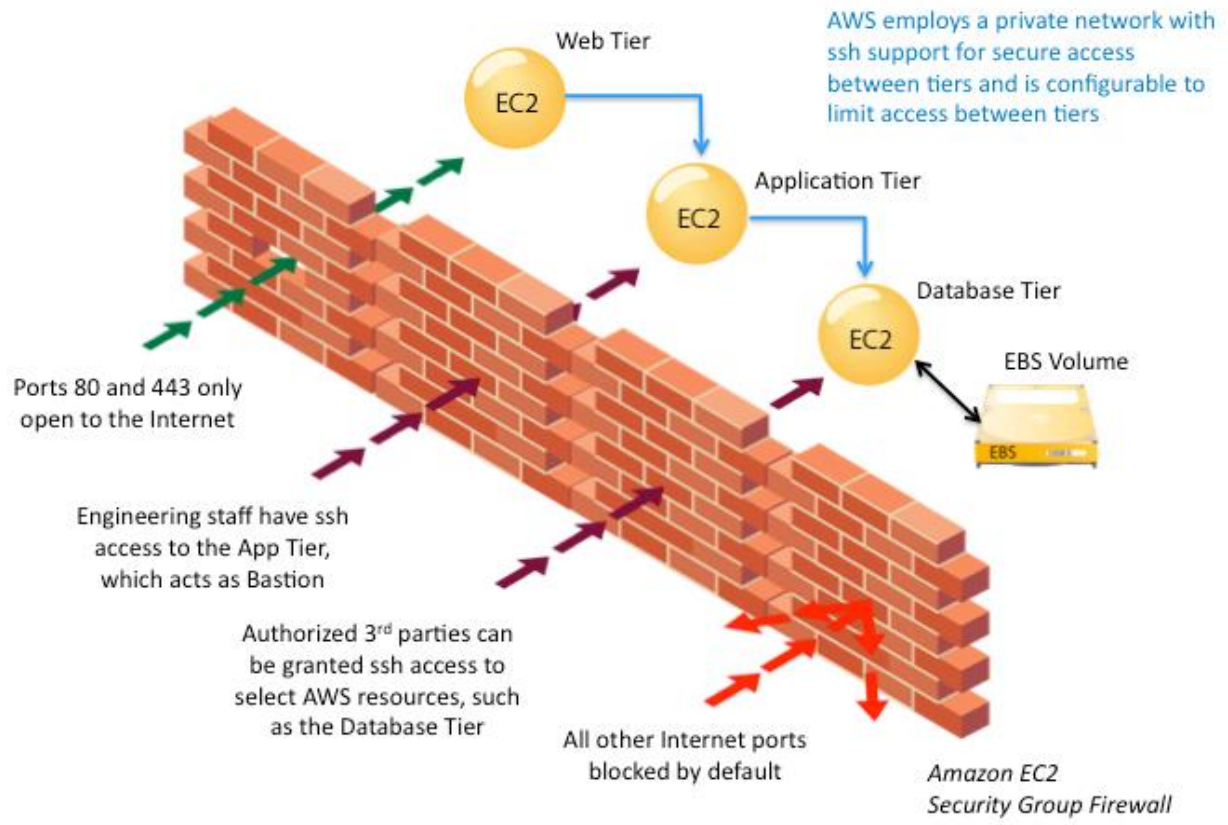
Ec2 Security Groups and Network ACLs



Firewall: Amazon EC2 provides a complete firewall solution; this mandatory inbound firewall is configured in a default

deny-all mode and Amazon EC2 customers must explicitly open the ports needed to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or Classless Inter-Domain
Routing (CIDR) block).

The firewall can be configured in groups permitting different classes of instances to have different rules. Consider, for example, the case of a traditional three-tiered web application. The group for the web servers would have port 80
(HTTP) and/or port 443 (HTTPS) open to the Internet. The group for the application servers would have port 8000 (application specific) accessible only to the web server group. The group for the database servers would have port 3306 (MySQL) open only to the application server group. All three groups would permit administrative access on port 22 (SSH), but only from the customer's corporate network. Highly secure applications can be deployed using this expressive mechanism.

Host Operating System: Administrators with a business need to access the management plane are required to use multifactor authentication to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane of the cloud. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked.

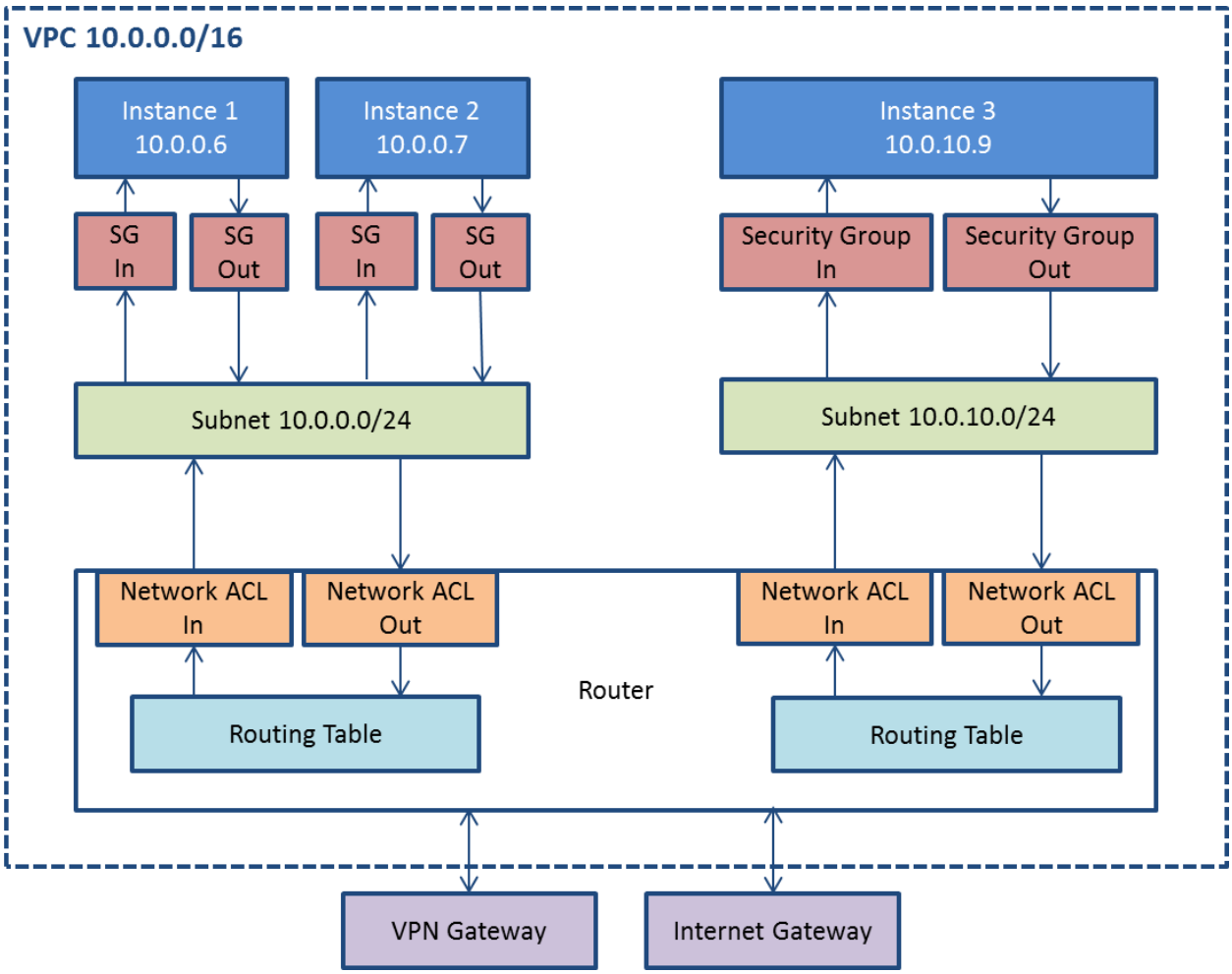
Guest Operating System: Virtual instances are completely controlled by the customer. Customers have full root access or administrative control over accounts, services, and applications. AWS does not have any access rights to customer instances and cannot log into the guest OS. AWS recommends a base set of security best practices to include disabling password-only access to their hosts, and utilizing some form of multi-factor authentication to gain access to their instances (or at a minimum certificate-based SSH Version 2 access). Additionally, customers should employ a privilege escalation mechanism with logging on a per-user basis. For example, if the guest OS is Linux, after hardening their instance, they should utilize certificate-based SSHv2 to access the virtual instance, disable remote root login, use command-line logging, and use 'sudo' for privilege escalation. Customers should generate their own key pairs in order to guarantee that they are unique, and not shared with other customers or with AWS.

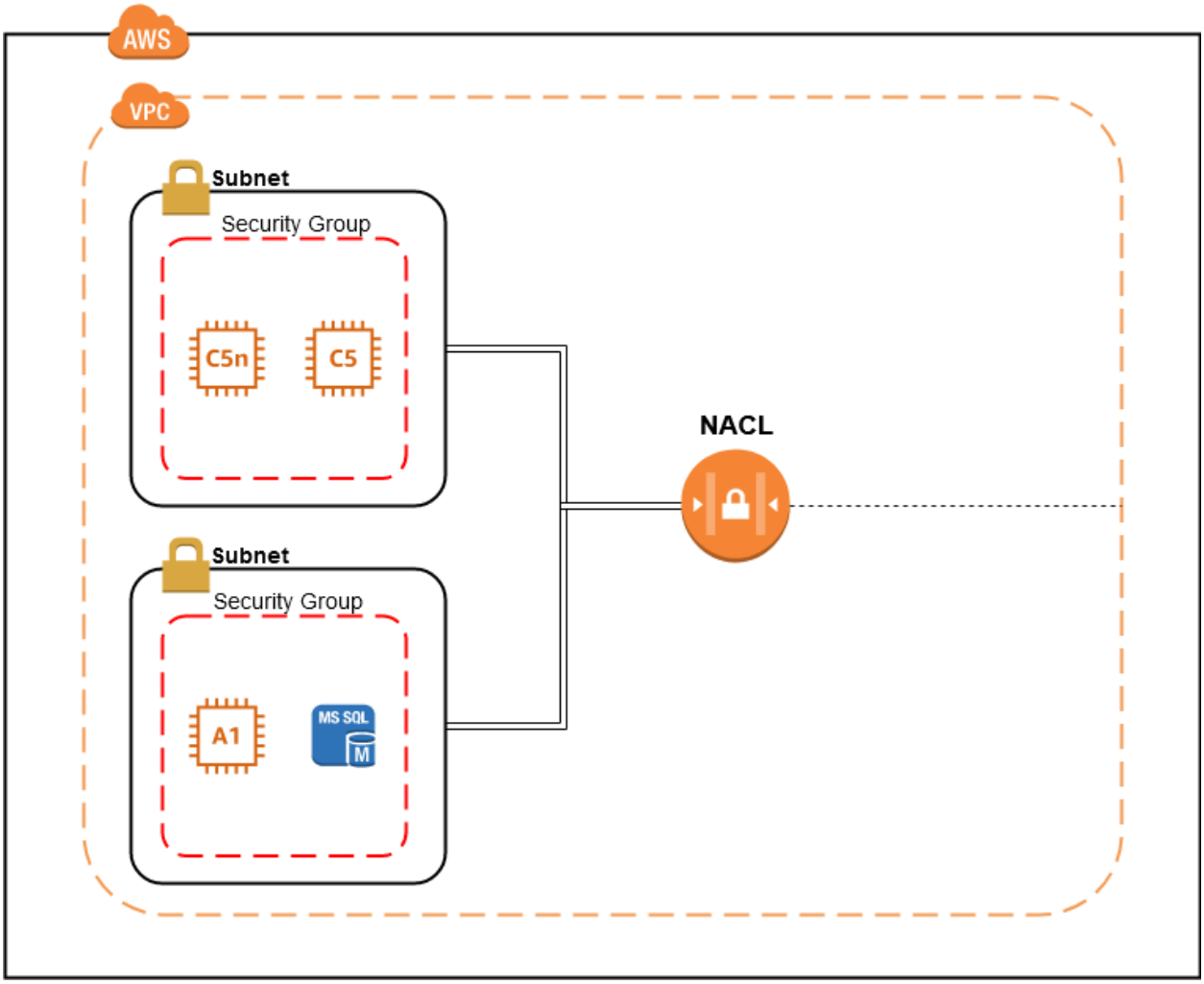
The Hypervisor

Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor, taking advantage of paravirtualization (in the case of Linux guests). Because paravirtualized guests rely on the hypervisor to provide support for operations that normally require privileged access, the guest OS has no elevated access to the CPU. The CPU provides four separate privilege modes: 0-3, called *rings.* Ring 0 is the most privileged and 3 the least. The host OS executes in Ring 0. However, rather than executing in Ring 0 as most operating systems do, the guest OS runs in a lesser-privileged Ring 1 and applications in the least privileged Ring 3. This explicit virtualization of the physical resources leads to a clear separation between guest and hypervisor, resulting in additional security separation between the two.

Network Security Summary

The diagram below depicts how the security controls above inter-relate to enable flexible network topologies while providing complete control over network traffic flows


VPC 10.0.0.0/16
Instance 1
10.0.0.6
Instance 2
10.0.0.7
Instance 3
10.0.10.9
SG
In
SG
Out
SG
In
SG
Out
Security Group
In
Security Group
Out
Subnet 10.0.0.0/24
Subnet 10.0.10.0/24
Network ACL
In
Network ACL
Out
Network ACL
In
Network ACL
Out
Router
Routing Table
Routing Table
VPN Gateway
Internet Gateway



Security Group — Security Group is a stateful firewall to the instances. Here stateful means, security group keeps a track of the State. Operates at the instance level.

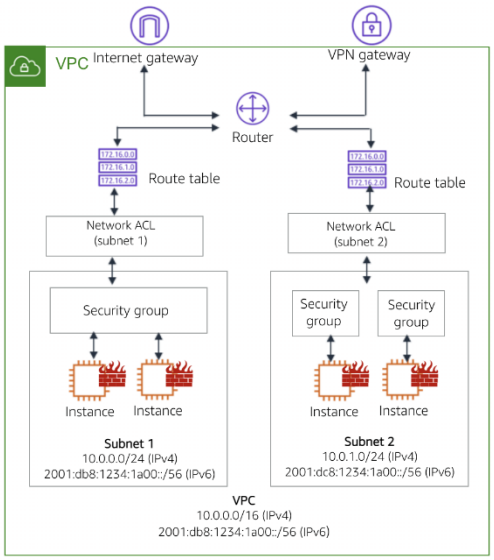
Network Access Control List — NACL is stateless, it won't keep any track of the state. Operates at Subnet level.

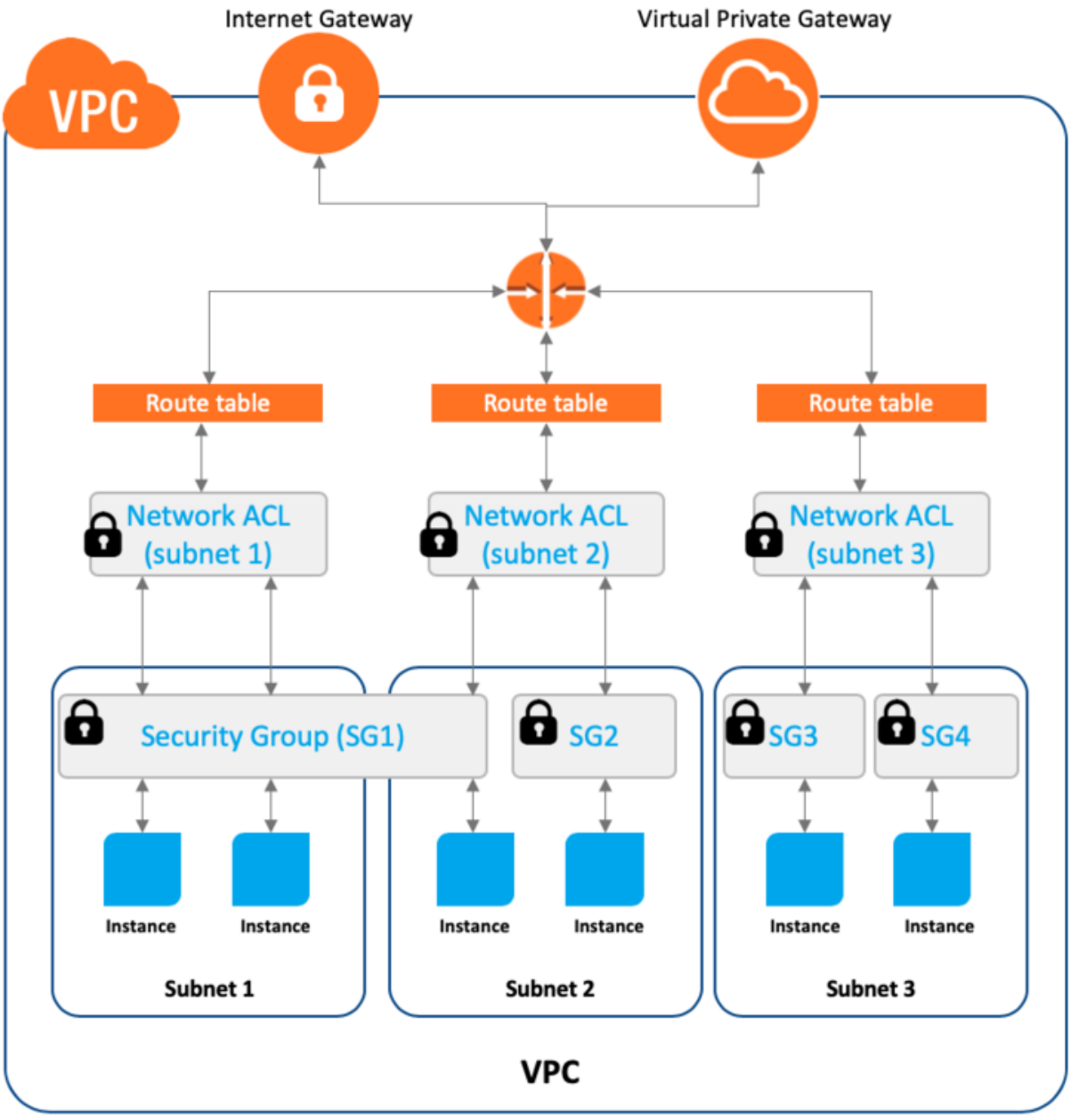
Network Access Control Lists – control traffic at the subnet level

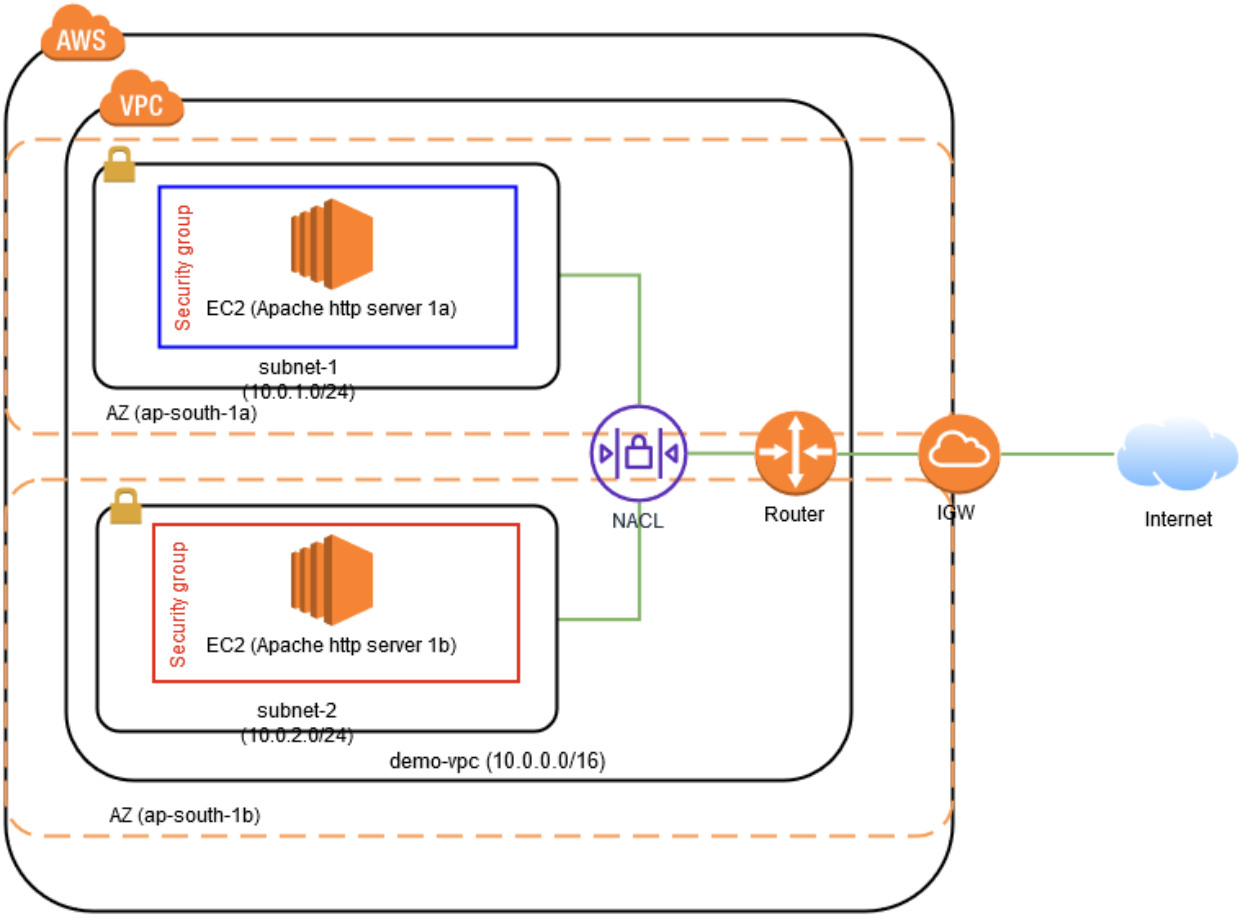
Security groups – control traffic at the instance level

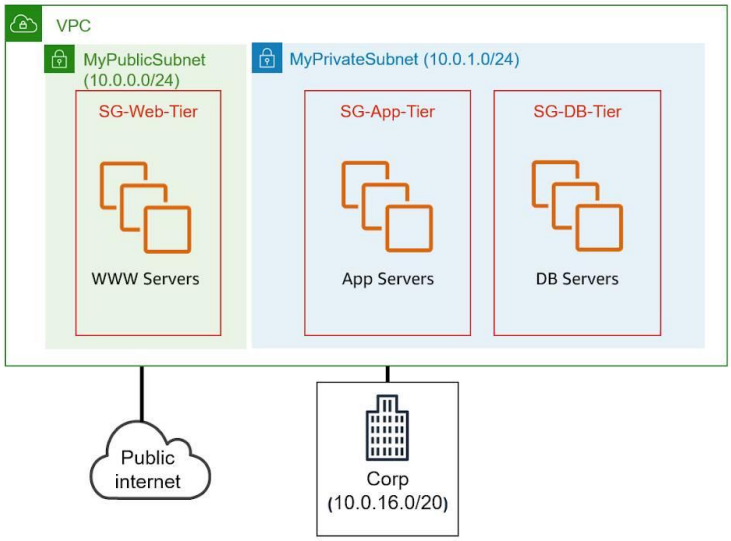
Flow logs– capture network flow information

Host-based firewalls – operating system firewalls




Internet Gateway
Virtual Private Gateway
VPC
Route table
Route table
Route table
Network ACL (subnet 1)
Network ACL (subnet 2)
Network ACL (subnet 3)
Security Group (SG1)
SG2
SG3
SG4
Instance
Instance
Instance
Instance
Instance
Instance
Subnet 1
Subnet 2
Subnet 3
VPC





SG-Web-Tier

Inbound		
Source	Protocol	Port Range
0.0.0.0/0	TCP	80
0.0.0.0/0	TCP	443
10.0.16.0/20	TCP	22

SG-App-Tier

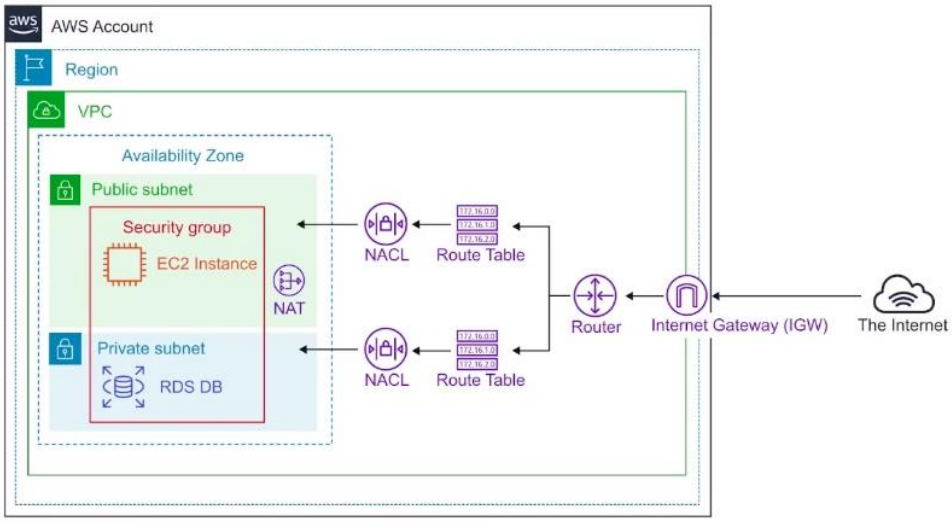
Inbound		
Source	Protocol	Port Range
ID of SG-Web-Tier	TCP	6455
10.0.16.0/20	TCP	22

SG-DB-Tier

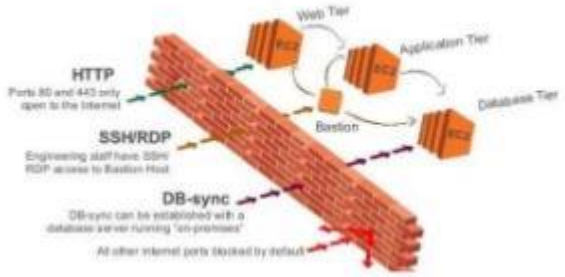
Inbound		
Source	Protocol	Port Range
ID of SG-App-Tier	TCP	3306
10.0.16.0/20	TCP	22

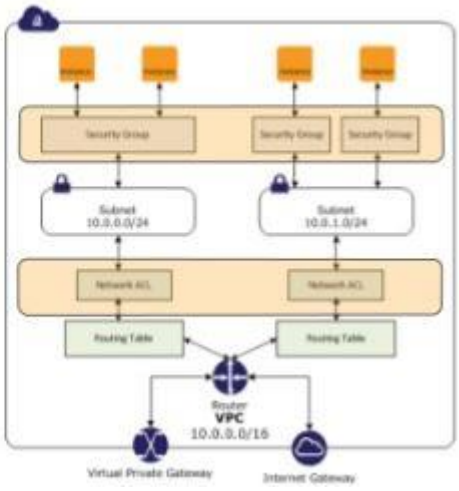
Think of a AWS VPC as your own **personal data centre.**

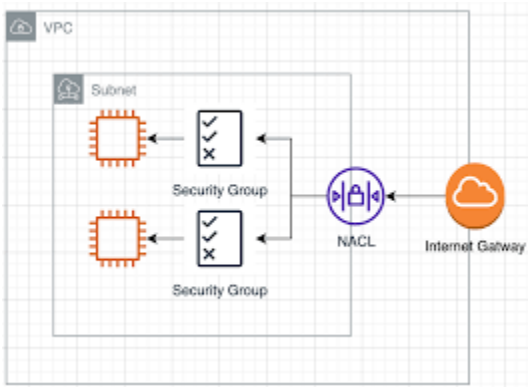
Gives you complete control over your virtual networking environment

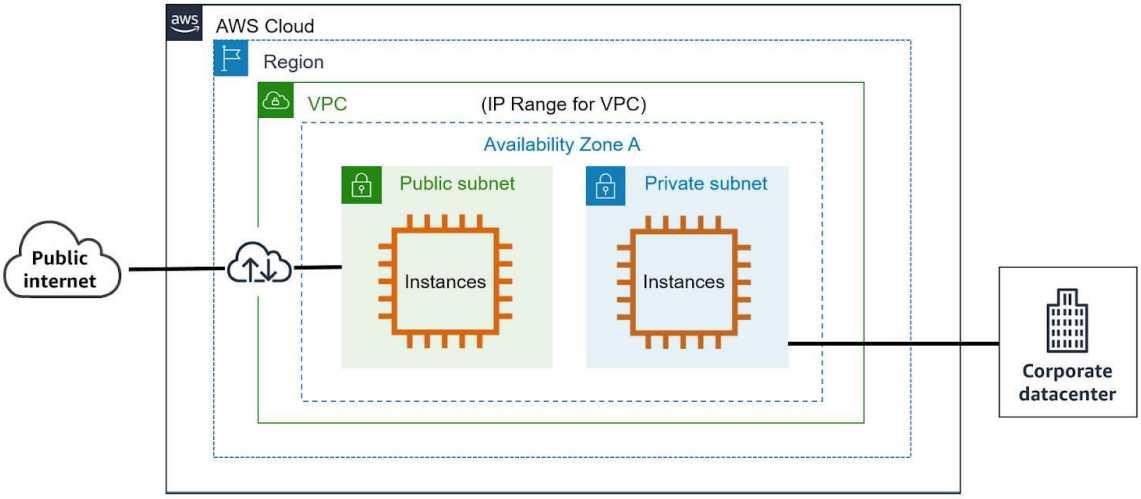


AWS Security Groups and Network ACLs






VPC
Subnet
Security Group
Security Group
NACL
Internet Gatway


AWS Cloud
Region
VPC
(IP Range for VPC)
Availability Zone A
Public subnet
Private subnet
Instances
Instances
Public internet
Corporate datacenter