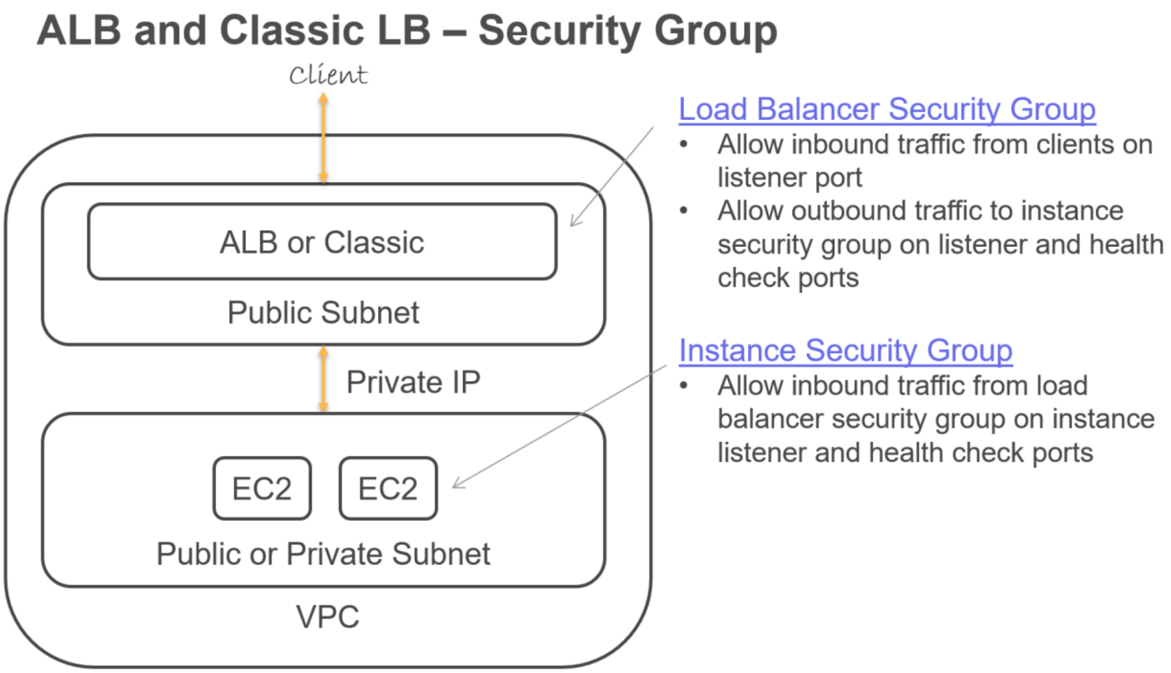
Security Group and Network ACL Configuration Finer Points

Chandra Lingam, Cloud Wave LLC

Application and Classic Load Balancer

The configuration is straight forward for Application and Classic Load Balancers. I will explain the configuration using an application load balancer example. A similar setup applies to a classic load balancer.

Here, the client interacts with the load balancer, and the load balancer interacts with the target using private IP.



ALB and Classic LB – Security Group

Load Balancer Security Group

- Allow inbound traffic from clients on listener port
- Allow outbound traffic to instance security group on listener and health check ports

Instance Security Group

- Allow inbound traffic from load balancer security group on instance listener and health check ports

Application Load Balancer Security Group

The client request must reach the load balancer. So, the load balancer security group must allow inbound traffic from the client on the listener port. The response traffic is automatically allowed as security group is stateful

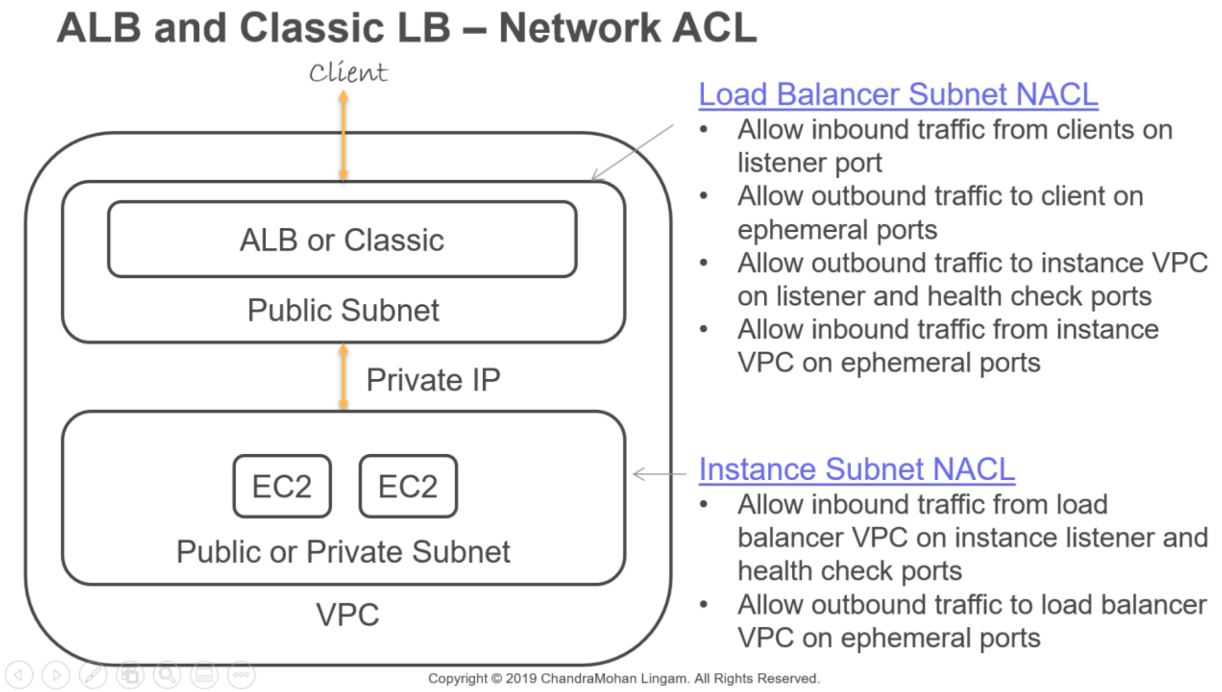
The load balancer needs to forward the request to the registered targets on the target’s listener ports. The load balancer also checks the health of the target by sending requests to target’s health check port

So, the load balancer security group must allow outbound traffic to the instance security group on the instance listener and health check ports

Instance Security Group

The instance must process requests forwarded by the load balancer. Besides, the instance should also allow health check request from the load balancer

So, instance security group must allow inbound traffic from the load balancer security group on instance listener and health check ports



ALB and Classic LB – Network ACL

Load Balancer Subnet NACL

- Allow inbound traffic from clients on listener port
- Allow outbound traffic to client on ephemeral ports
- Allow outbound traffic to instance VPC on listener and health check ports
- Allow inbound traffic from instance VPC on ephemeral ports

Instance Subnet NACL

- Allow inbound traffic from load balancer VPC on instance listener and health check ports
- Allow outbound traffic to load balancer VPC on ephemeral ports

Application LB Subnet - Network ACL Configuration

Load Balancer subnet NACL must allow inbound traffic from the client on listener port. The response traffic to the client is on an ephemeral port.

So, NACL must allow inbound traffic from the client on load balancer listener ports and the corresponding outbound traffic to the client on an ephemeral port

Load Balancer needs to talk to the instance on listener and health check ports, and the corresponding response from the instance is on ephemeral ports.

So, NACL must allow outbound traffic to instance VPC on listener and health check ports. The corresponding response is inbound traffic to load balancer on ephemeral ports.

Instance Subnet – Network ACL Configuration

The instance needs to process client requests forwarded by the load balancer and health check requests from the load balancer.

So, the instance subnet NACL must allow inbound traffic from load balancer VPC, on instance listener ports and health check ports.

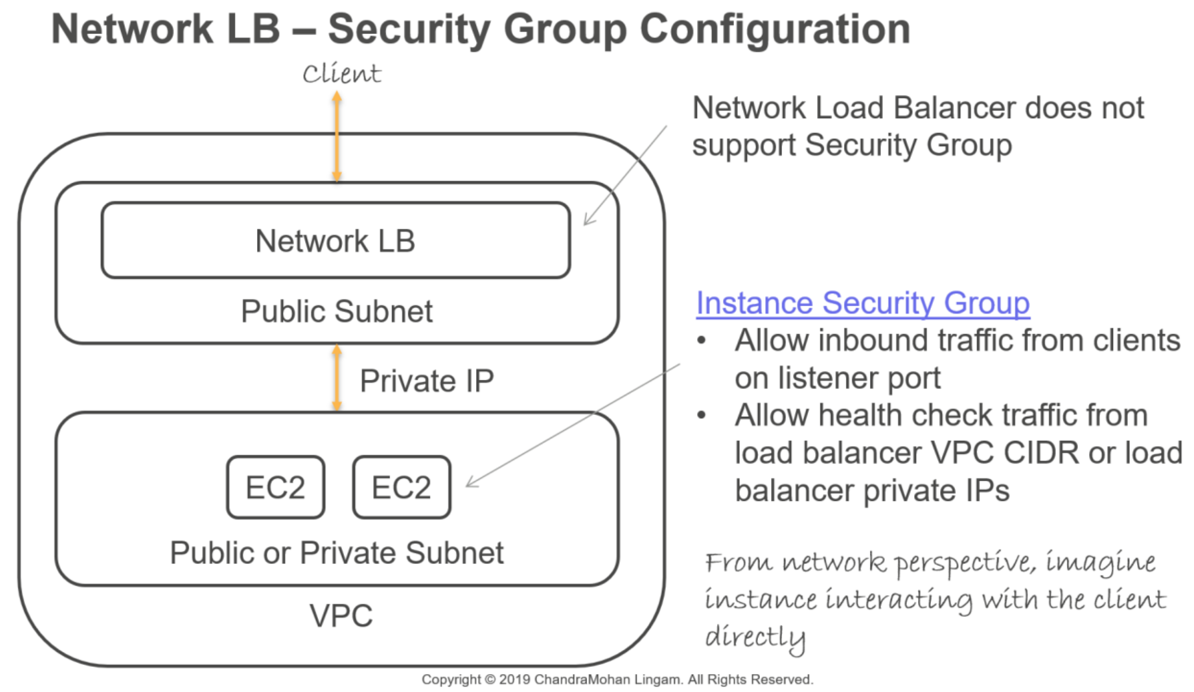
The corresponding response traffic goes back to load balancer on ephemeral ports. So, NACL must allow outbound traffic to load balancer VPC on ephemeral ports.

Network Load Balancer

The Network Load Balancer traffic flow is a little different.

When you register an instance with a network load balancer, from the client traffic flow perspective, it appears as if the instance is directly interacting with the client.

The second aspect is network load balancer does not support security group firewall. Instead, the security group firewall rules are applied as part of the instance security group.



Network LB – Security Group Configuration

Network Load Balancer does not support Security Group

Instance Security Group

- Allow inbound traffic from clients on listener port
- Allow health check traffic from load balancer VPC CIDR or load balancer private IPs

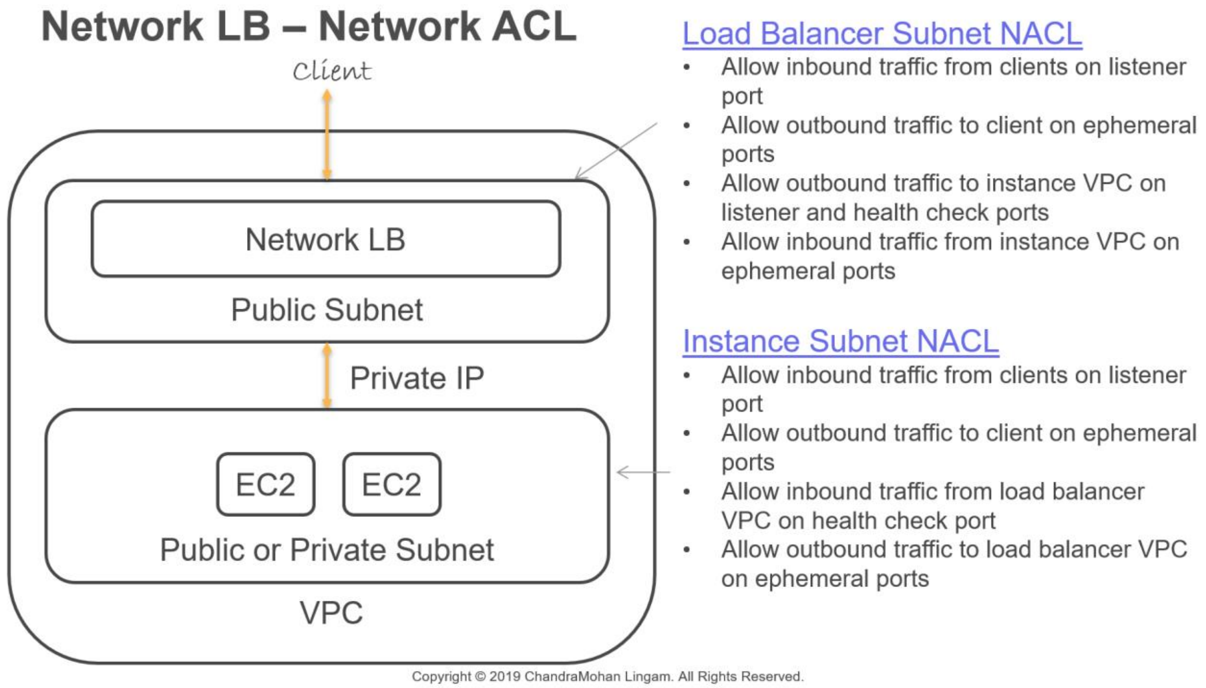
From network perspective, imagine instance interacting with the client directly

Instance Security Group

The instance security group must allow traffic from the client on the listener port. The instance can remain in the private subnet with only a private IP address. However, the request appears as-if coming straight from the client IP address.

The healthy check from load balancers come directly to the instance. Since there is no network load balancer security group, you must specify load balancer VPC CIDR block or Network Load balancer Private IP addresses as the source for health check requests in the inbound rules

Since the security group is stateful, the response traffic to client requests and health check requests are automatically allowed.



Network LB – Network ACL

Load Balancer Subnet NACL

- Allow inbound traffic from clients on listener port
- Allow outbound traffic to client on ephemeral ports
- Allow outbound traffic to instance VPC on listener and health check ports
- Allow inbound traffic from instance VPC on ephemeral ports

Instance Subnet NACL

- Allow inbound traffic from clients on listener port
- Allow outbound traffic to client on ephemeral ports
- Allow inbound traffic from load balancer VPC on health check port
- Allow outbound traffic to load balancer VPC on ephemeral ports

Network LB Subnet - Network ACL Configuration

Load Balancer subnet NACL must allow inbound traffic from the client on listener port. The response traffic to the client is on an ephemeral port.

So, NACL must allow inbound traffic from the client on load balancer listener ports and the corresponding outbound traffic to the client on an ephemeral port

Load Balancer needs to talk to the instance on listener and health check ports, and the corresponding response from the instance is on ephemeral ports.

So, NACL must allow outbound traffic to instance VPC on listener and health check ports. The corresponding response is inbound traffic to load balancer on ephemeral ports.

Instance Subnet – Network ACL Configuration

With the network load balancer, from the client traffic flow perspective, it appears as if the instance is directly interacting with the client.

So, instance subnet (even if it is a private subnet) must allow requests from the client and the corresponding response to client on an ephemeral port. Note that the instance is still private; it is only the firewall rules that we are tweaking.

The instance subnet needs to allow health check requests from the load balancer.

The corresponding response traffic goes back to load balancer on ephemeral ports. So, NACL must allow inbound health check requests and the outbound traffic to load balancer VPC on ephemeral ports.

References

Application Load Balancer

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-update-security-groups.html

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/target-group-register-targets.html

Network Load Balancer

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-register-targets.html

VPC Ephemeral Ports

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#nacl-ephemeral-ports