Security groups and ACLs in the cloud

Security architecture · https://nuabee.com/documents/security-groups-and-acls-in-the-cloud/

Customer requirements

In a Nuabee DRP context, the customer has a dedicated backup space in the OTC Cloud, entirely inaccessible from the outside (trust bubble), called tenant.

This article explains the relationship between tenant (or project) concepts and the complementary security solutions offered by security groups and ACLs.

Tenant and VPC architecture principles

Each customer's backup space is hosted in a dedicated tenant. A tenant is a concept used to group resources (VMs, subnets, users, etc.) within an OpenStack cloud environment, enabling better organization, resource isolation and access control within the cloud infrastructure.

Multiple VPCs are possible within a single tenant. The Virtual Private Cloud (VPC) service provides logically isolated, configurable and manageable virtual networks for servers (ECS), enhancing the security of resources in the Cloud system and simplifying network deployment.

Security Groups: what are they used for?

A security group contains one or more security rules:

- Rules can be applied either inbound or outbound
- Allow TCP/UDP/ICMP packets from or to a CIDR or other security group
- By default, a machine can receive packets from other machines in the same security group and send packets to anywhere.

Inter VPC peering

VPC peering is a function for linking two VPCs in Flexible Engine.

- Works between local VPCs (within the same tenant) and remote VPCs (between different tenants).
- In both cases, the peering set-up must be formally accepted by both parties

A VPC pairing is accompanied by routing rules that indicate which CIDRs can traverse the pairing.

They must be entered on both sides if a bidirectional connection is desired.

- A multi-peering architecture can centralize multiple flows.

[peering-VPC.png]

The principles of an ACL in a VPC

Network ACLs (access control lists) are an optional security layer in a VPC that :

- Acts as a firewall to control incoming and outgoing traffic on one or more subnets.

Network ACLs use rules similar to security groups to add an extra layer of security to a VPC.

- Provides a second layer of security on top of security groups to restrict global flows.

[ACL.png]

ACLs complement security groups.

- For example, they can be used to block entire CIDRs globally, without having to configure each individual machine.
- To authorize only a company's IPs to access cloud services, particularly in the case of an IS Cloud environment.

They enable global security rules to be applied across an entire network.

In the case of communication between machines in the Cloud, via peering for example, ACLs enable more detailed management of authorized traffic in the context of inter-VPC peering.

Network ACL versus Security Group

Security group	Network ACL
Works at instance level (first layer of defense)	Operates at subnet level (second layer of defense)

Applies to an instance only if someone specifies the security group when the instance is launched, or subsequently associates the security group with the instance	Applies automatically to all instances on subnets with which it is associated (backup defense layer, so you don't have to rely on someone specifying the security group)
Allows only source **OR** destination IPs to be specified (inbound or outbound rule)	Allows source **AND** destination IPs to be specified
Is stateful: return traffic is automatically allowed, unless explicitly prohibited.	
We evaluate all rules before deciding whether to allow traffic	We process rules in numerical order to decide whether to allow traffic