Internetwork traffic privacy in Amazon VPC

PDF

Kindle

RSS

Amazon Virtual Private Cloud provides features that you can use to increase and monitor the security for your virtual private cloud (VPC):

- **Security groups**: Security groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level. When you launch an instance, you can associate it with one or more security groups that you've created. Each instance in your VPC could belong to a different set of security groups. If you don't specify a security group when you launch an instance, the instance is automatically associated with the default security group for the VPC. For more information, see Security groups for your VPC.
- **Network access control lists (ACLs)**: Network ACLs act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level. For more information, see Network ACLs.
- **Flow logs**: Flow logs capture information about the IP traffic going to and from network interfaces in your VPC. You can create a flow log for a VPC, subnet, or individual network interface. Flow log data is published to CloudWatch Logs or Amazon S3, and it can help you diagnose overly restrictive or overly permissive security group and network ACL rules. For more information, see VPC Flow Logs.

- **Traffic mirroring**: You can copy network traffic from an elastic network interface of an Amazon EC2 instance. You can then send the traffic to out-of-band security and monitoring appliances. For more information, see the Traffic Mirroring Guide.

You can use AWS Identity and Access Management (IAM) to control who in your organization has permission to create and manage security groups, network ACLs, and flow logs. For example, you can give your network administrators that permission, but not give permission to personnel who only need to launch instances. For more information, see Identity and access management for Amazon VPC.

Amazon security groups and network ACLs don't filter traffic to or from link-local addresses (`169.254.0.0/16`) or AWS reserved IPv4 addresses (these are the first four IPv4 addresses of the subnet, including the Amazon DNS server address for the VPC). Similarly, flow logs do not capture IP traffic to or from these addresses. These addresses support the following:

- Domain Name Services (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Amazon EC2 instance metadata
- Key Management Server (KMS) — license management for Windows instances
- Routing in the subnet

You can implement additional firewall solutions in your instances to block network communication with link-local addresses.

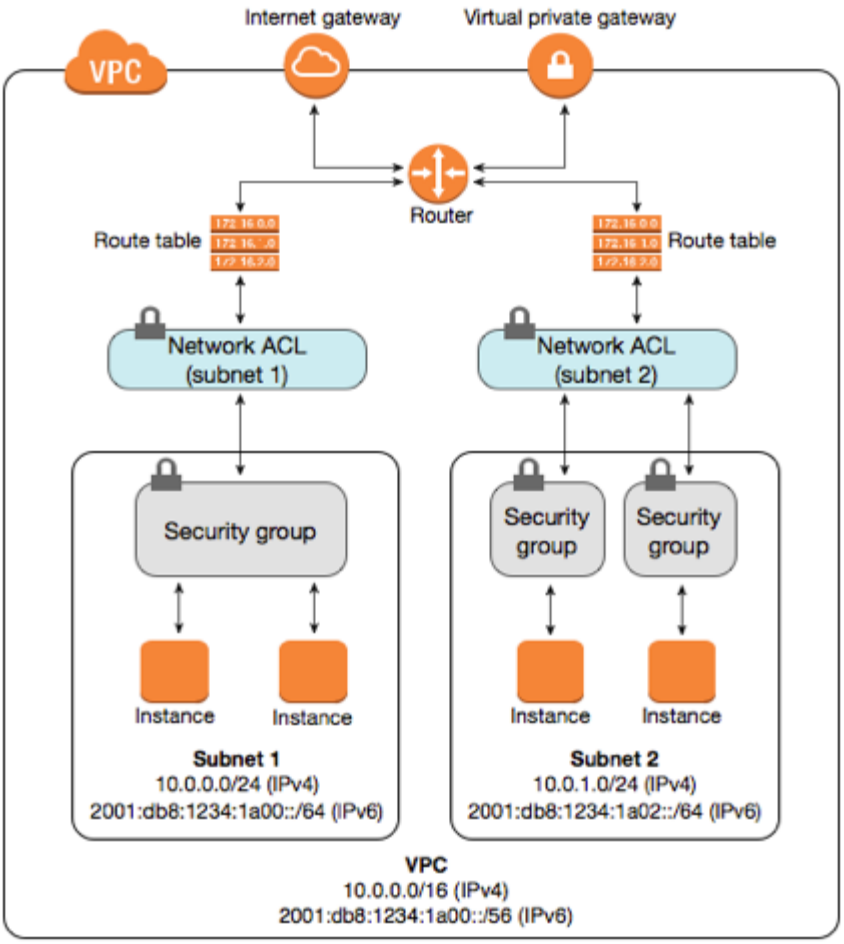
Comparison of security groups and network ACLs

The following table summarizes the basic differences between security groups and network ACLs.

Security group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules

We evaluate all rules before deciding whether to allow traffic	We process rules in order, starting with the lowest numbered rule, when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets that it's associated with (therefore, it provides an additional layer of defense if the security group rules are too permissive)

The following diagram illustrates the layers of security provided by security groups and network ACLs. For example, traffic from an internet gateway is routed to the appropriate subnet using the routes in the routing table. The rules of the network ACL that is associated with the subnet control which traffic is allowed to the subnet. The rules of the security group that is associated with an instance control which traffic is allowed to the instance.



You can secure your instances using only security groups. However, you can add network ACLs as an additional layer of defense. For an example, see Example: Controlling access

to instances in a subnet.

Did this page help you?

Provide feedback

Edit this page on GitHub

Previous topic: Data protection

Next topic: Identity and access management

Need help?

- Try the forums
- Connect with an AWS IQ expert