VPC Security

## Service Overview

*Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.*

*Security is a shared responsibility between AWS and you. The*[*shared responsibility model*](http://aws.amazon.com/compliance/shared-responsibility-model/)*describes this as security*of*the cloud and security*in*the cloud:*

* *Security of the cloud – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the*[*AWS Compliance Programs*](http://aws.amazon.com/compliance/programs/)*. To learn about the compliance programs that apply to Amazon Virtual Private Cloud, see*[*AWS Services in Scope by Compliance Program*](http://aws.amazon.com/compliance/services-in-scope/)*.*
* *Security in the cloud – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company’s requirements, and applicable laws and regulations.*

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

* *A*[***security group***](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)*acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups. For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic..****Security Groups are Stateful****if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.;*
* *A*[**network access control list**](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html) (ACL)*is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.  Network Access Control Lists are Stateless, which means that responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa).*
  + *You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.*
  + *Network ACLs contain a numbered list of rules that is evaluated in order, starting with the lowest numbered rule.*
  + *Network ACLs have separate inbound and outbound rules, and each rule can either allow or deny traffic.*
  + *Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa.)*

|  |  |
| --- | --- |
| *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.*

## Traffic is controlled using security groups and network ACLs

## Use cases / Considerations

* *Secure you data*

## Governance

## Cautions

* **Network ACLs per VPC** - 2000. You can associate one network ACL to one or more subnets in a VPC. This quota is not the same as the number of rules per network ACL.
* **Rules per network ACL** - 20. This is the one-way quota for a single network ACL. This quota is enforced separately for IPv4 rules and IPv6 rules; for example, you can have 20 ingress rules for IPv4 traffic and 20 ingress rules for IPv6 traffic. This quota includes the default deny rules (rule number 32767 for IPv4 and 32768 for IPv6, or an asterisk \* in the Amazon VPC console).
* This quota can be increased up to a maximum of 40; however, network performance might be impacted due to the increased workload to process the additional rules
* **VPC security groups per Region** – 2500. This quota applies to individual AWS account VPCs and shared VPCs. If you increase this quota to more than 5000 security groups in a Region, we recommend that you paginate calls to describe your security groups for better performance.
* **Inbound or outbound rules per security group** – 60. You can have 60 inbound and 60 outbound rules per security group (making a total of 120 rules). This quota is enforced separately for IPv4 rules and IPv6 rules; for example, a security group can have 60 inbound rules for IPv4 traffic and 60 inbound rules for IPv6 traffic. A rule that references a security group or AWS-managed prefix list ID counts as one rule for IPv4 and one rule for IPv6.
* A quota change applies to both inbound and outbound rules. This quota multiplied by the quota for security groups per network interface cannot exceed 1000. For example, if you increase this quota to 100, we decrease the quota for your number of security groups per network interface to 10.
* If you reference a customer-managed prefix list in a security group rule, the maximum number of entries for the prefix lists equals the same number of security group rules.
* **Security groups per network interface** – 5. The maximum is 16. This quota is enforced separately for IPv4 rules and IPv6 rules. The quota for security groups per network interface multiplied by the quota for rules per security group cannot exceed 1000. For example, if you increase this quota to 10, we decrease the quota for your number of rules per security group to 100.

## Pricing considerations

*https://aws.amazon.com/vpc/pricing/*

## More details

https://docs.aws.amazon.com/vpc/latest/userguide/security.html