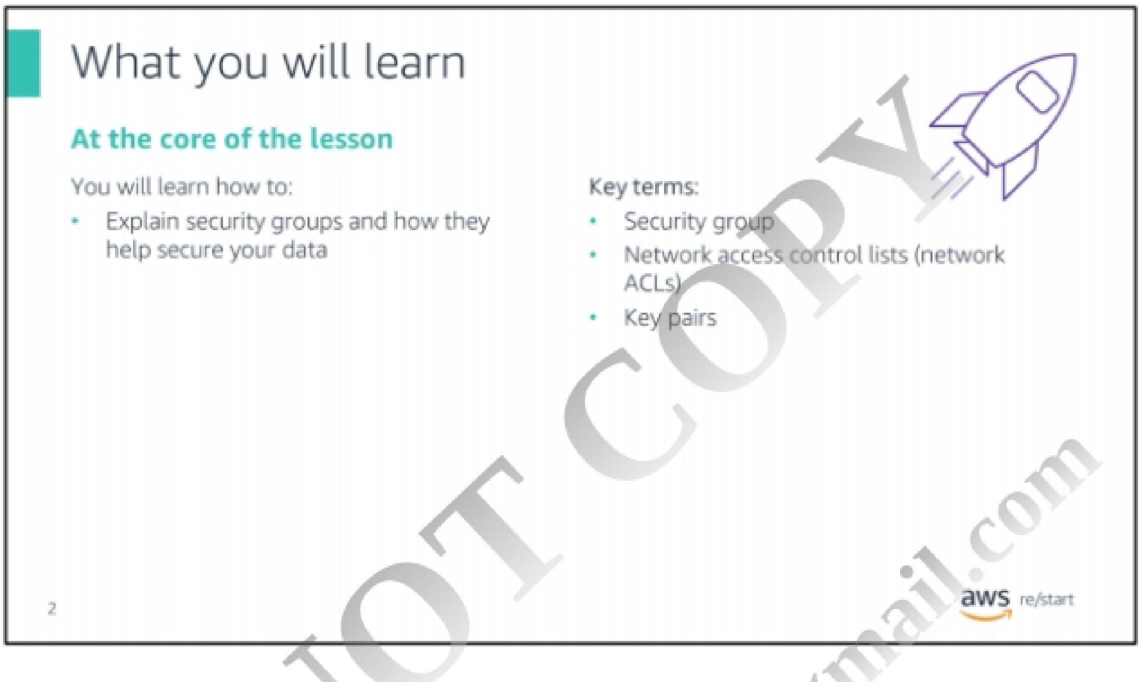
aws re/start

AWS Security Groups

Security of the AWS Cloud is the top priority for AWS. This lesson reviews how you can use AWS security groups to improve the security of your virtual private cloud (VPC).



What you will learn

At the core of the lesson

You will learn how to:

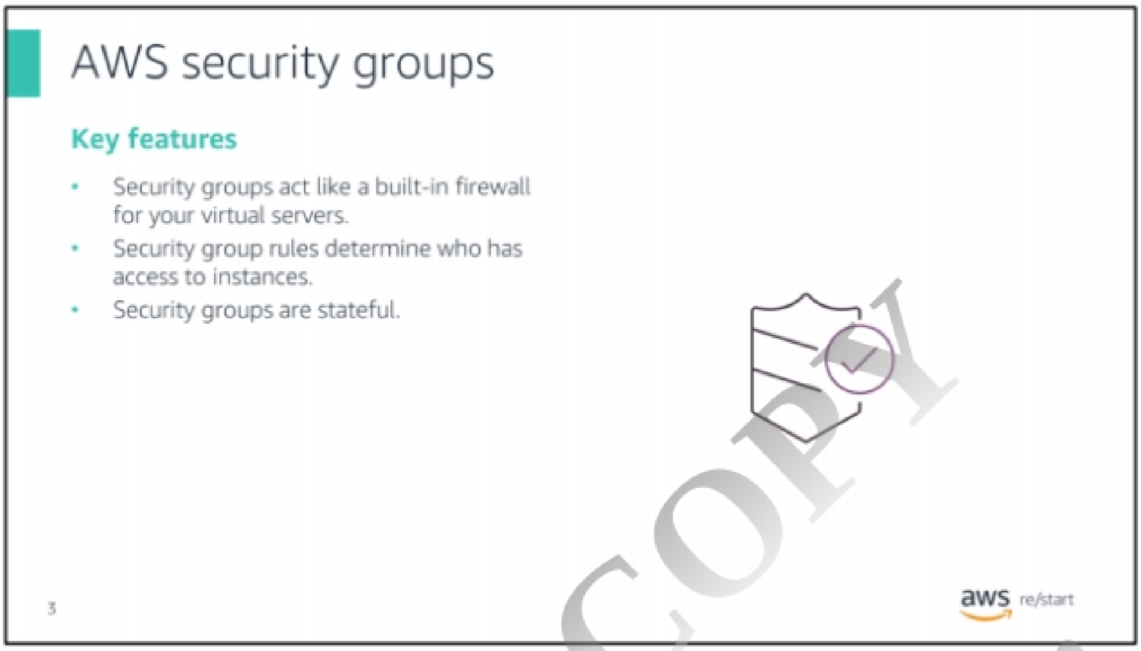
- Explain security groups and how they help secure your data

Key terms:

- Security group
- Network access control lists (network ACLs)
- Key pairs

2

In this lesson, you will learn about the features and benefits of AWS security groups.



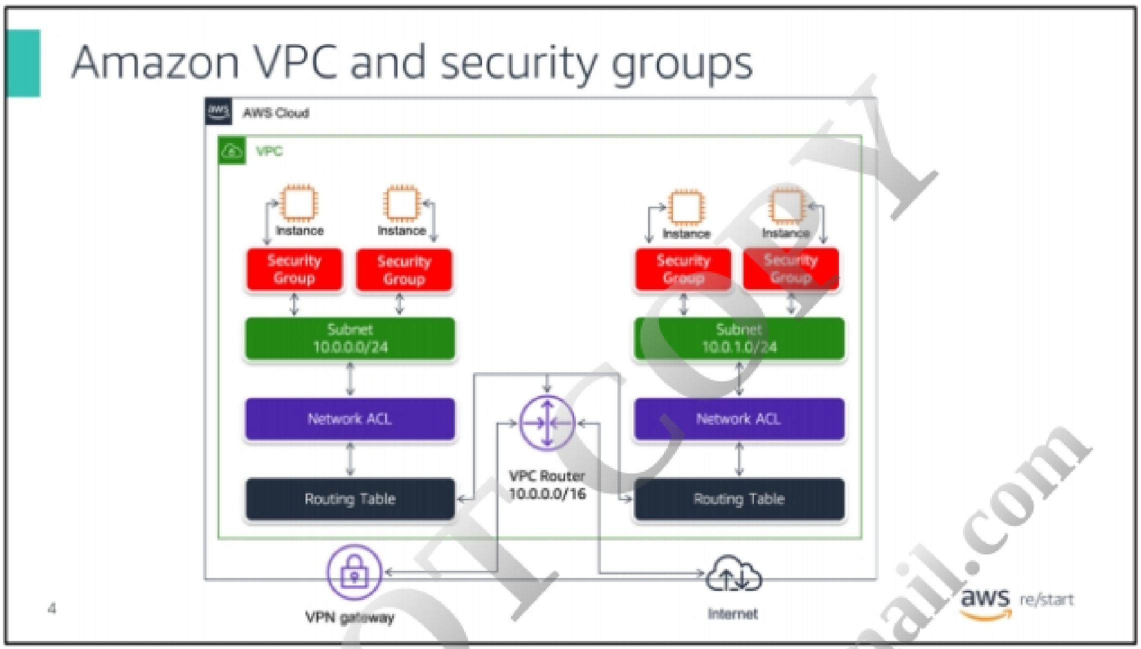
AWS security groups

Key features

- Security groups act like a built-in firewall for your virtual servers.
- Security group rules determine who has access to instances.
- Security groups are stateful.

At AWS, security groups act like a built-in firewall for your virtual servers. With these security groups, you have full control on how accessible your instances are.

At the most basic level, a security group is only another method to filter traffic to your instances. It provides you control over which traffic to allow or deny. To determine who has access to your instances, configure a security group rule. Rules can vary, from keeping the instance entirely private to entirely public.



Amazon VPC and security groups

Amazon Virtual Private Cloud (Amazon VPC) provides various features for increasing and monitoring the security for your VPC:

- Security groups act as a firewall for associated Amazon Elastic Compute Cloud (Amazon EC2) instances. Security groups control both inbound and outbound traffic at the instance level.
- Network access controls lists (network ACLs) act as a firewall for associated subnets. They control both inbound and outbound traffic at the subnet level.
- Amazon EC2 uses public key cryptography to encrypt and decrypt login information. Public key cryptography uses a public key to encrypt a piece of data. The recipient uses the private key to decrypt the data. The private and public keys are known as a *key pair*. To log in to your instance, you must do the following actions:
  - Create a key pair.
  - Specify the name of the key pair when you launch the instance.

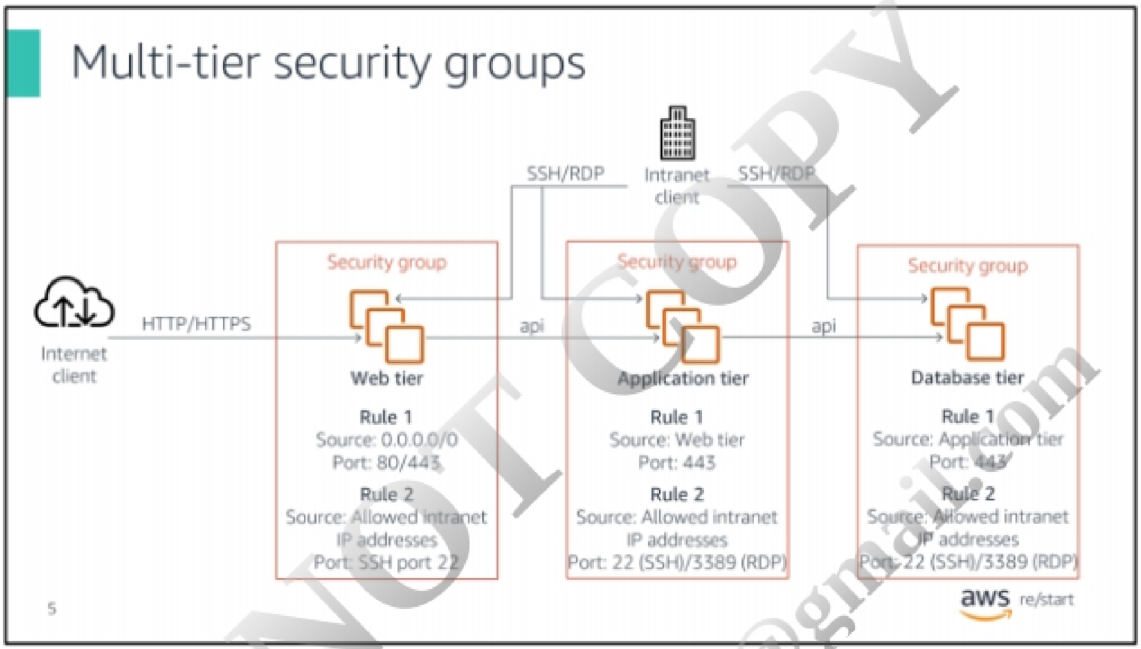
    - Provide the private key when you connect to the instance.

  Linux instances have no password, so you use a key pair to log in by using Secure Shell (SSH).

  Microsoft Windows instances require a key pair to obtain the administrator password so that you can log in through Remote Desktop Protocol (RDP).

Security groups are stateful, but network ACLs are stateless.

- *Stateful* means that the computer tracks the state of interaction, usually by setting values in a storage setting that is designated for that purpose.
- *Stateless* means that no information is retained by the sender or receiver. Each interaction request must be handled based entirely on information that comes with it.



Multi-tier security groups

Intranet client

SSH/RDP

SSH/RDP

Internet client

HTTP/HTTPS

api

api

Security group

Web tier

Rule 1
Source: 0.0.0.0/0
Port: 80/443

Rule 2
Source: Allowed intranet IP addresses
Port: SSH port 22

Security group

Application tier

Rule 1
Source: Web tier
Port: 443

Rule 2
Source: Allowed intranet IP addresses
Port: 22 (SSH)/3389 (RDP)

Security group

Database tier

Rule 1
Source: Application tier
Port: 443

Rule 2
Source: Allowed intranet IP addresses
Port: 22 (SSH)/3389 (RDP)

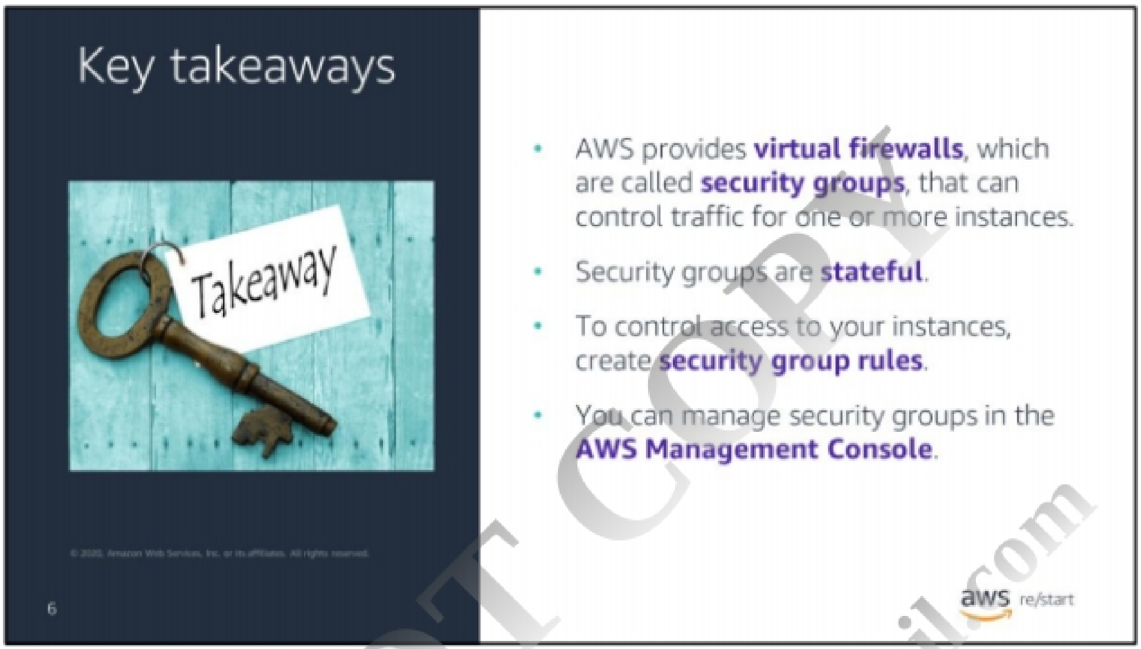
This diagram is an example of an AWS security group design applied to a classic three-tier web application architecture. Different security group rules were created to accommodate this multi-tiered web architecture.

Starting at the web tier, a defined rule accepts traffic from anywhere on the internet on *port 80/443* by selecting the source *0.0.0.0/0*.

At the application tier, a security group accepts traffic only from the web tier on the secure HTTPS port (443). Similarly, the database tier can accept traffic only from the application tier on port 443.

Finally, a rule was created in all tiers to allow remote administration from allowed IP addresses in the corporate network (intranet) over SSH port 22 or RDP port 3389.

To learn more, refer to Security groups for your VPC in the *Amazon VPC User Guide*.



Key takeaways

Takeaway

- AWS provides **virtual firewalls**, which are called **security groups**, that can control traffic for one or more instances.
- Security groups are **stateful**.
- To control access to your instances, create **security group rules**.
- You can manage security groups in the **AWS Management Console**.

aws re/start

Key takeaways from this lesson include:

- AWS provides virtual firewalls, called security groups, that can control traffic for one or more instances.
- Security groups are stateful.
- To control access to your instances, create security group rules.
- You can manage security groups on the AWS Management Console.