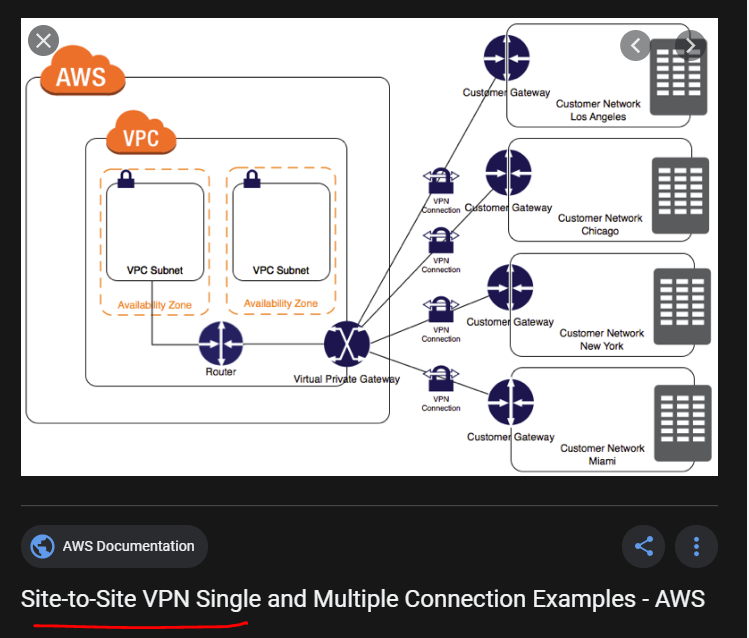


<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-network-to-amazon.html>



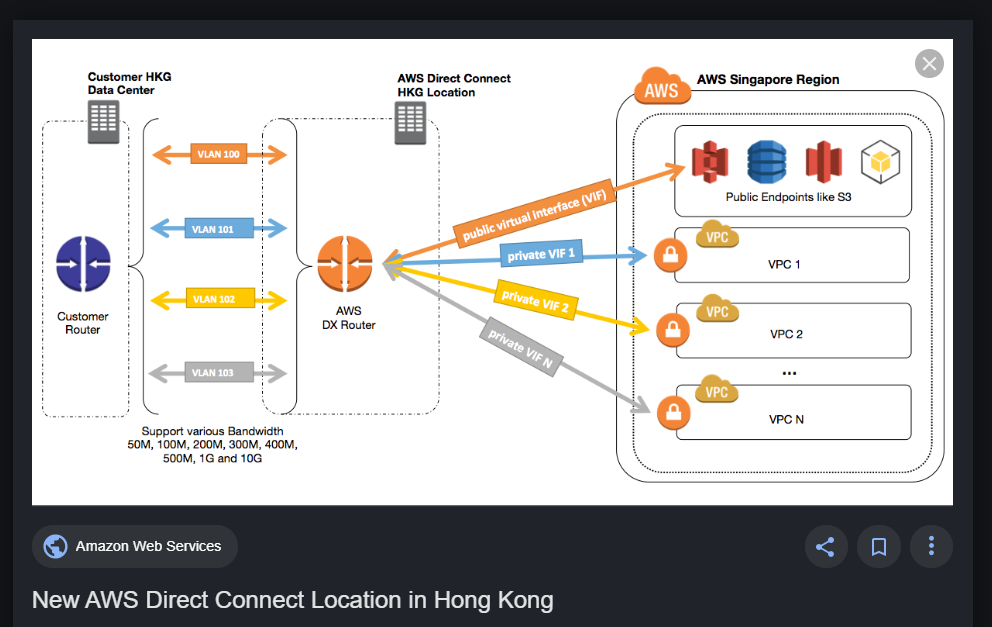
<https://docs.aws.amazon.com/vpn/latest/s2svpn/Examples.html>

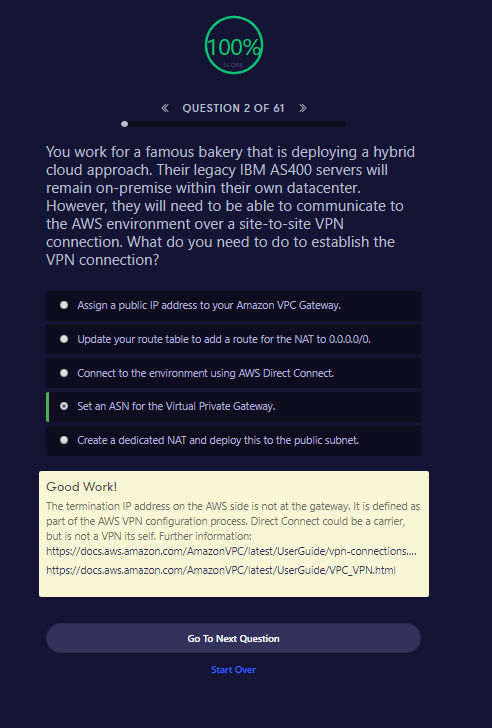
**What is AWS Direct Connect?**

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection, you can create *virtual interfaces* directly to public AWS services (for example, to Amazon S3) or to Amazon VPC, bypassing internet service providers in your network path. An AWS Direct Connect location provides access to AWS in the Region with which it is associated. You can use a single connection in a public Region or AWS GovCloud (US) to access public AWS services in all other public Regions.

The following diagram shows how AWS Direct Connect interfaces with your network.


    AWS Direct Connect
  





# Site-to-Site VPN Single and Multiple Connection Examples

The following diagrams illustrate single and multiple Site-to-Site VPN connections.

## Single Site-to-Site VPN Connection

The VPC has an attached virtual private gateway, and your remote network includes a customer gateway, which you must configure to enable the Site-to-Site VPN connection. You set up the routing so that any traffic from the VPC bound for your network is routed to the virtual private gateway.


        VPN layout
      

## Single Site-to-Site VPN Connection with a Transit Gateway

The VPC has an attached transit gateway, and your remote network includes a customer gateway, which you must configure to enable the Site-to-Site VPN connection. You set up the routing so that any traffic from the VPC bound for your network is routed to the transit gateway.


        Single Site-to-Site VPN Connection with a Transit Gateway
      

## Multiple Site-to-Site VPN Connections

The VPC has an attached virtual private gateway, and your remote network includes a customer gateway, which you must configure to enable the Site-to-Site VPN connection. You set up the routing so that any traffic from the VPC bound for your network is routed to the virtual private gateway.

When you create multiple Site-to-Site VPN connections to a single VPC, you can configure a second customer gateway to create a redundant connection to the same external location. You can also use it to create Site-to-Site VPN connections to multiple geographic locations.

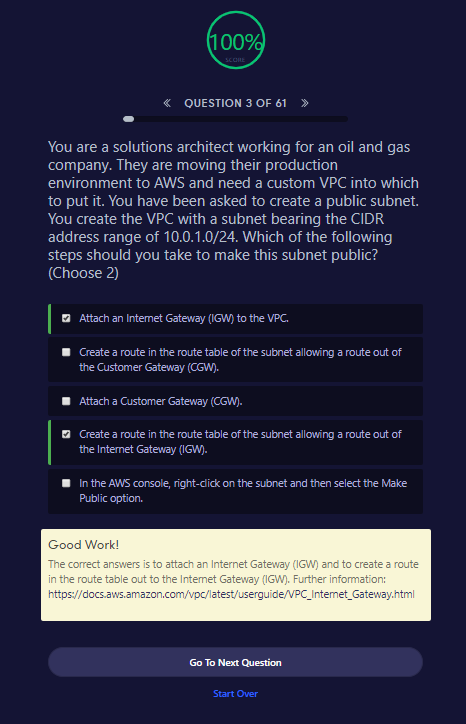

        Multiple Site-to-Site VPN layout
      

## Multiple Site-to-Site VPN Connections with a Transit Gateway

The VPC has an attached transit gateway, and your remote network includes a customer gateway, which you must configure to enable the Site-to-Site VPN connection. You set up the routing so that any traffic from the VPC bound for your network is routed to the transit gateway.

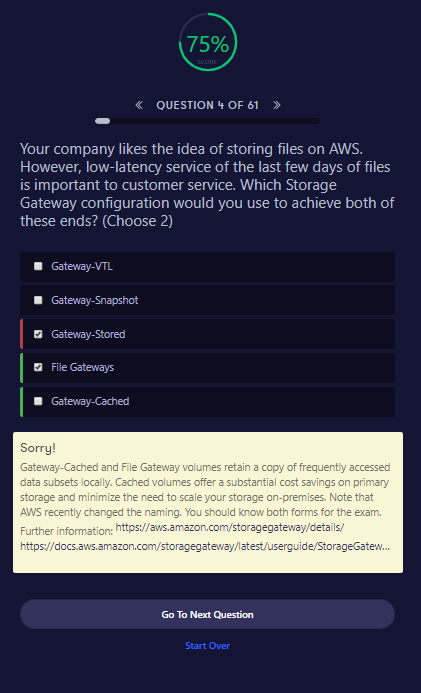
When you create multiple Site-to-Site VPN connections to a single VPC, you can configure a second customer gateway to create a redundant connection to the same external location. You can also use it to create Site-to-Site VPN connections to multiple geographic locations.


        Multiple Site-to-Site VPN connections with a Transit Gateway
      



##### **Good Work!**

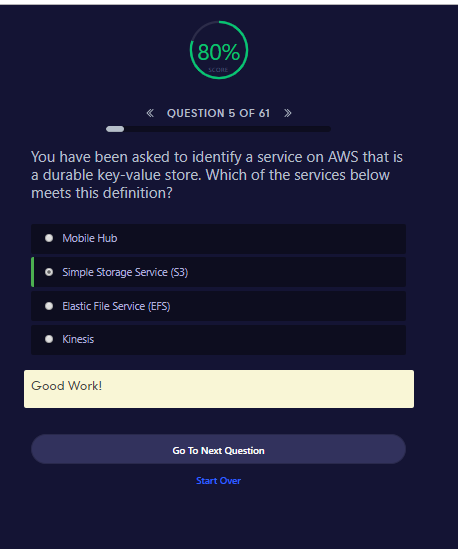
The correct answers is to attach an Internet Gateway (IGW) and to create a route in the route table out to the Internet Gateway (IGW). Further information: <https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html>

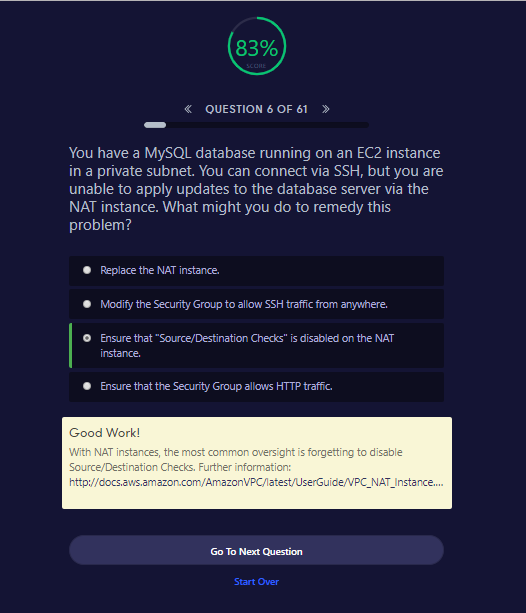


##### **Sorry!**

Gateway-Cached and File Gateway volumes retain a copy of frequently accessed data subsets locally. Cached volumes offer a substantial cost savings on primary storage and minimize the need to scale your storage on-premises. Note that AWS recently changed the naming. You should know both forms for the exam. Further information: <https://aws.amazon.com/storagegateway/details/><https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html>

Go To Next QuestionStart Over





The AWS documentation says “Each EC2 instance performs source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives.”

In simple words, each EC2 instance either sends or receives internet traffic. That is, it itself is the source and / or destination of the traffic. But, the NAT instance is neither the source nor the destination of the traffic. NAT Instances merely act as a gateway for the traffic. Thus, the Source/Destination checks need to be disabled on NAT instance so that the NAT instance can serve as a gateway and allow instances in a private subnets to securely connect to the internet.

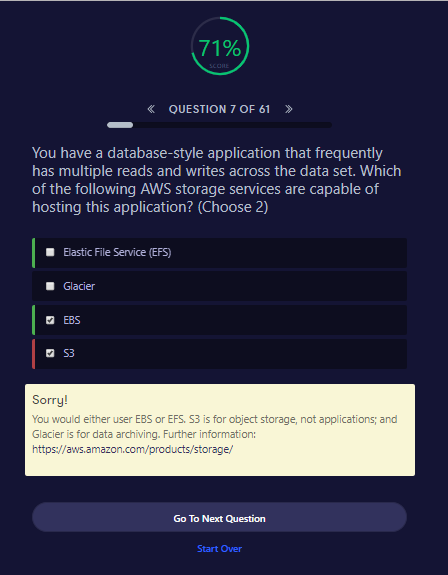
Note: At the time of writing this, NAT gateways are becoming more popular and it looks like NAT instances are on their way out. More about NAT gateways [here](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html).

Source: [AWS NAT instances](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html#EIP_Disable_SrcDestCheck)

##### **Good Work!**

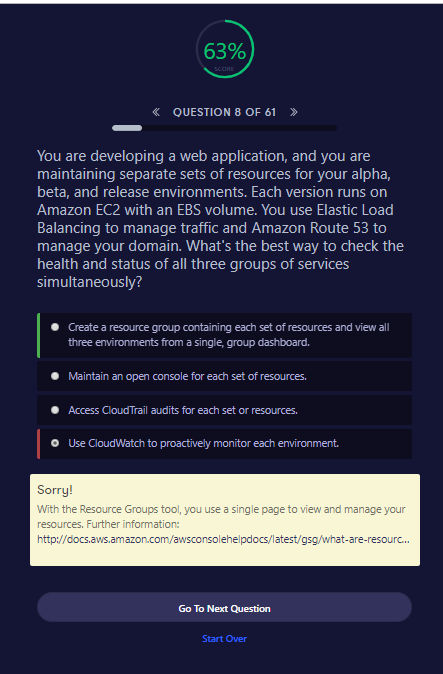
With NAT instances, the most common oversight is forgetting to disable Source/Destination Checks. Further information: <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html#EIP_Disable_SrcDestCheck>

Go To Next QuestionStart Over



##### **Sorry!**

You would either user EBS or EFS. S3 is for object storage, not applications; and Glacier is for data archiving. Further information: <https://aws.amazon.com/products/storage/>



##### **Sorry!**

With the Resource Groups tool, you use a single page to view and manage your resources. Further information: <http://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/what-are-resource-groups.html>