Jonathan A nderson

AWS

Certified Solutions Architect

Associate

The ultimate guide for the

SAA-C03

Imagen que contiene lego, juguete

Descripción generada automáticamenteE X A M

**AWS Direct Connection**

AWS Direct Connect hace posible que una red local y Amazon VPC creen un enlace dedicado. Puede configurar una conexión privada entre su centro de datos y AWS, oficina o área de colocación con AWS Direct Connect. Este enlace privado minimizará los costos de red, mejorará el rendimiento del ancho de banda y proporcionará una experiencia de red más confiable que otras conexiones a Internet.

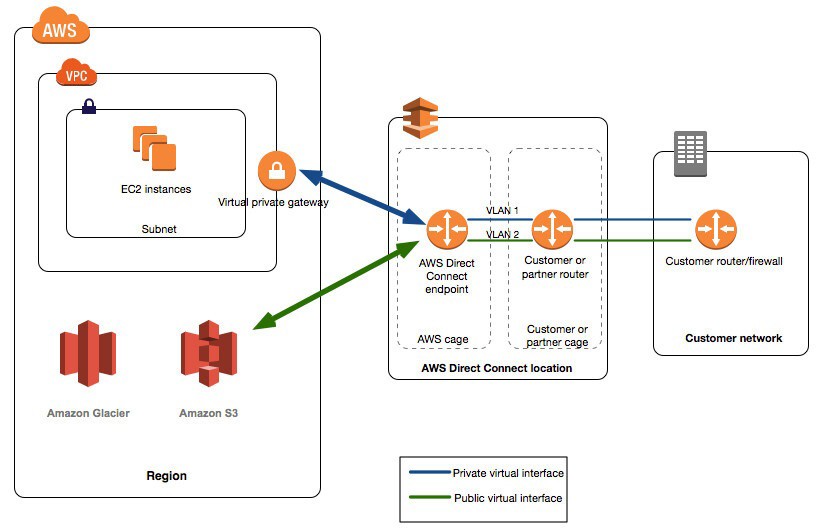
AWS Direct Connect le permite establecer conexiones de red dedicadas de 1 Gbps o 10 Gbps (o varias conexiones) entre las redes de AWS y cualquiera de las ubicaciones de AWS Direct Connect. Utiliza VLAN estándar para obtener acceso a instancias de Amazon Elastic Compute Cloud (Amazon EC2) que se ejecutan en una Amazon VPC mediante direcciones IP privadas. Puede seleccionar entre un ecosistema de proveedores de servicios WAN para integrar su punto de enlace de AWS Direct Connect en un sitio de AWS Direct Connect con sus redes externas. La siguiente figura ilustra este modelo. También puede trabajar con su operador para crear una conexión sub-1G o utilizar un grupo de agregación de enlaces (LAG) para agrupar varias conexiones de 1 gigabit o 10 gigabits en un único punto de enlace de AWS Direct Connect para que pueda manejarlas como una conexión unificada.

## AWS Direct Connect + VPN

AWS Direct Connect + VPN le permite combinar una o más conexiones de red dedicadas de AWS Direct Connect con Amazon VPC VPN. Esta combinación proporciona una conexión privada cifrada IPsec que también reduce los costos de red, aumenta el rendimiento del ancho de banda y proporciona una experiencia de red más consistente que la VPN basada en Internet. Conexiones.

Para establecer un enlace de red dedicado entre la red, puede utilizar AWS Direct Connect y establecer una conexión lógica con los recursos públicos de AWS, como un punto de enlace IPsec para la gateway privada virtual de Amazon. Este enfoque incorpora la baja latencia, el mayor ancho de banda, los beneficios más confiables del enfoque de AWS Direct Connect y un enlace IPsec seguro de extremo a extremo con las ventajas administradas por AWS de la solución VPN.

Esta opción se ilustra con la siguiente imagen



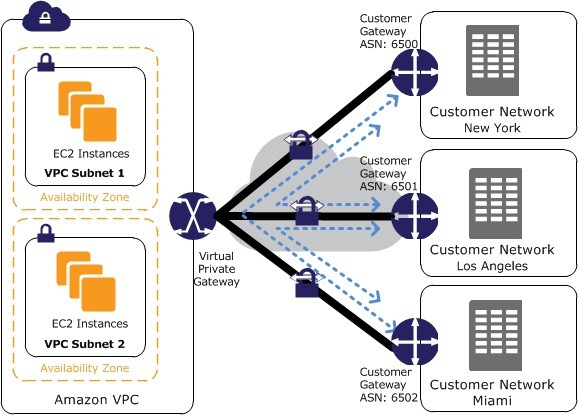
## AWS VPN CloudHub

Según las opciones de AWS Managed VPN y AWS Direct Connect descritas anteriormente, puede comunicarse de forma segura de un sitio a otro mediante AWS VPN CloudHub. AWS VPN CloudHub funciona en un modelo estrella simple que puede usar con o sin VPC. Utilice este diseño si tiene varias sucursales y conexiones a Internet existentes y desea implementar un modelo estrella práctico y potencialmente rentable para la o conexiones de copia de seguridad entre estas oficinas remotas.

La siguiente imagen ilustra la arquitectura de AWS VPN CloudHub, con líneas azules discontinuas que indican el tráfico de red entre sitios remotos enrutados a través de sus conexiones de AWS VPN.

AWS VPN CloudHub administra una gateway privada virtual de Amazon VPC con varias gateways y cada una utiliza números de sistema autónomos (ASN) BGP únicos. Sus puertas de enlace promoverán las rutas correctas (prefijos BGP) a través de

sus conexiones VPN.



## Software VPN

Amazon VPC le ofrece la flexibilidad de controlar completamente ambos lados de la conectividad de Amazon VPC mediante el establecimiento de una conexión VPN entre su red remota y un dispositivo VPN de software ejecutándose en su red de Amazon VPC.

Esta opción se recomienda si necesita administrar ambos extremos de la conexión VPN para el cumplimiento o si desea usar dispositivos de puerta de enlace que actualmente no son compatibles con la solución VPN de Amazon VPC. La siguiente figura ilustra esta opción.

Puede elegir entre un ecosistema de varios socios y comunidades de código abierto que han producido dispositivos VPN de software que se ejecutan en Amazon EC2. Estos incluyen productos de compañías de seguridad conocidas como

Check Point, Astaro, OpenVPN Technologies y Microsoft, así como herramientas populares de código abierto como OpenVPN, Openswan e IPsec-Tools. Esta opción incluye la responsabilidad de administrar el dispositivo de software, centrándose en la configuración, los parches y las actualizaciones.

**Tenga en cuenta** que este diseño introduce un posible punto único de error en el diseño de la red, ya que el dispositivo VPN de software se ejecuta en una instancia Amazon EC2.

## Exam Essentials

* Comprender el concepto de VPC, sus elementos clave y opcionales. Una Amazon VPC consta de los siguientes elementos básicos: subredes (públicas, privadas y vpn solamente), tablas de enrutamiento, conjuntos de opciones DHCP, grupos de seguridad y ACL de red. Los elementos opcionales incluyen un IGW, direcciones EIP, puntos finales, conexiones de emparejamiento, instancias NAT, VPG, CGI y conexiones VPN.
* Comprender el propósito de una subred. Una subred es un segmento del intervalo de direcciones IP de Amazon VPC en el que puede colocar grupos de recursos aislados. Las subredes están definidas por bloques CIDR (por ejemplo, 10.0.1.0/24 y 10.0.2.0/24) y se encuentran en un área de disponibilidad.
* Identifique la distinción entre una subred pública, una subred privada y una VPN de solo subred. Cuando el tráfico se enruta desde una subred a un IGW, la subred se denomina subred pública. Si una subred no tiene ninguna ruta al IGW, la subred se denomina subred privada. Si una subred no tiene ninguna ruta al IGW, pero el tráfico se reenvía a un VPG, la subred se denomina subred solo VPN.
* Comprender el propósito de una tabla de enrutamiento. La tabla de enrutamiento es un conjunto de reglas (denominadas rutas) que se utiliza para determinar hacia dónde se dirige el tráfico de red. Una tabla de enrutamiento permite que las instancias Amazon EC2 de diferentes subredes se comuniquen entre sí (dentro de la misma Amazon VPC).
* Comprenda lo que los conjuntos de opciones DHCP proporcionan para una Amazon VPC. Mediante el elemento de conjuntos de opciones DHCP de una Amazon VPC, puede dirigir la asignación de nombres de host de Amazon EC2 a sus recursos. Puede introducir un nombre de dominio de instancia en una Amazon VPC y marcar las direcciones IP de los servidores DNS, NTP y NetBIOS personalizados.
* Comprenda la diferencia entre una dirección IP pública para una Amazon VPC y una dirección EIP. Una dirección IP pública es una dirección IP de AWS que se puede asignar a instancias que se crean automáticamente en una subred. Una dirección EIP es una dirección IP pública de AWS que se asigna a su cuenta y a instancias o interfaces de red previa solicitud.
* Comprenda qué puntos de enlace pueden ofrecer una Amazon VPC. Con un punto de enlace de Amazon VPC, puede establecer una conexión privada entre su Amazon VPC y otro servicio de AWS sin necesidad de acceso desde Internet o a través de una instancia NAT, una conexión VPN o AWS Direct Connect. Las terminales solo admiten servicios en la región.
* Comprender el emparejamiento de Amazon VPC. Una conexión de emparejamiento de Amazon VPC es una conexión de red entre dos Amazon VPC que permite que las instancias de ambas VPC de Amazon se comuniquen entre sí como si estuvieran en una red similar. Además, a través de un protocolo de solicitud / aceptación, se crean conexiones pares. No se permite el emparejamiento transitivo y, dentro de la misma región, el emparejamiento solo es posible entre las VPC de Amazon.
* Conozca la diferencia entre una ACL de red y una comunidad de seguridad. El nivel de instancia hace referencia a una categoría de protección. En muchas subredes que forman parte de las mismas clases de protección, puede tener varias instancias. Las clases de protección tienen estado, lo que garantiza que, independientemente de las leyes de salida, el tráfico de retorno se permita automáticamente. Se aplica una ACL de red en el nivel de subred y el tráfico permanece sin estado. Debe permitir el tráfico entrante y saliente en la ACL de red para que las instancias Amazon EC2 de una subred puedan comunicarse mediante un protocolo específico.
* Comprenda lo que ofrece una NAT para una Amazon VPC. Una instancia NAT o una puerta de enlace NAT permite que las instancias de una subred privada inicien el tráfico saliente a Internet. Esto permite que las comunicaciones salientes de Internet descarguen parches y actualizaciones. Sin embargo, evita que las instancias reciban tráfico entrante iniciado por alguien en Internet.
* Para crear un enlace VPN desde una red a una Amazon VPC, comprenda los componentes necesarios. Un VPG es el concentrador de VPN entre las dos redes en el lado de AWS de la conexión VPN. La conexión VPN debe establecerse en el lado CGW, y esta conexión consta de dos túneles IPSec.

**Review Questions**

1. What is the range of permitted IPv4 prefix lengths for a VPC CIDR block?

A. /16 to /28

B. /16 to /56

C. /8 to /30

D. /56 only

1. You've created a VPC with the CIDR 192.168.16.0/24. You want to assign a secondary CIDR to this VPC. Which CIDR can you use?

A. 172.31.0.0/16 B. 192.168.0.0/16 C. 192.168.0.0/24

D. 192.168.16.0/23

1. You need to create two subnets in a VPC that has a CIDR of 10.0.0.0/16. Which of the following CIDRs can you assign to one of the subnets while leaving room for an additional subnet? (Choose all that apply.)

A. 10.0.0.0/24

B. 10.0.0.0/8

C. 10.0.0.0/16

D. 10.0.0.0/23

1. What is the minimum subnet size you can have in an Amazon VPC? A. / 24

B. / 26

C. / 28

D. / 30

1. You made a new subnet and then added a route that uses an IGW to route traffic from that subnet to the Internet and to your routing table. What kind of subnet have you built?
   1. An internal subnet
   2. A private subnet with a private net
   3. An External Subnet
   4. A subnet for the public
2. When you create a new Amazon VPC, what happens?
3. By default, the main route table is generated.
4. By default, three subnets are established, one for every Availability Region.
5. Three subnets are created by default in an availability zone.
6. An IGW is created by default.
7. In East US 1, you built a new VPC and added three subnets in that Amazon VPC. Which of the following statements is true?
8. These subnets are not capable of communicating with each other by default; you need to build routes.
9. By default, every subnet is public.
10. Both subnets can communicate by default with each other.
11. Each subnet has similar CIDR blocks.
12. How many IGWs can you connect to an Amazon VPC at the same time?
13. 1
14. 2
15. 3
16. 4
17. What is a stateful feature of an Amazon VPC?
18. ACL network
19. Groups of defence
20. DynamoDB Amazon
21. The S3 Amazon
22. With private and public subnets, you have created a custom Amazon VPC. You have a NAT instance generated, and this instance is deployed on a public subnet. You've added an EIP address to the routing table and also added your NAT. Unfortunately, the Internet is still unreachable by instances in your private subnet. What could be the cause?
23. Your NAT is on a public subnet but must be on a private subnet.
24. Your NAT must be behind an Elastic Load Balancer.
25. You must disable source/destination controls for NAT.
26. Your NAT is deployed on a Windows instance, but your other instances are Linux. It would help if you redeployed NAT on a Linux instance.
27. When an Amazon EC2 instance sponsored by Amazon Elastic Block Store (Amazon EBS) in an Amazon VPC with an associated EIP is halted and restarted, which of the following events will occur? (Choose 2 answers).
28. The EIP will be disconnected from the procedure.
29. All data on the instance storage devices will be destroyed.
30. All the data on Amazon EBS computers will be lost.
31. ENI remains Freestanding.
32. The host child of the case becomes shifted.
33. How many VPC peering links for four VPCs located in the same AWS area are required to send traffic to others?

A.3

1. 4
2. 5
3. 6
4. 13. To resolve DNS names outside of AWS, which of the following AWS tools will you use to acquire an EC2 VPC instance?
5. A VPC peering connection
6. A set of DHCP options
7. A routing rule
8. An IGW
9. Which of the following is the Amazon side connected to an Amazon VPN?
10. An EIP
11. A CGW
12. An IGW
13. A VPG
14. What is the default limit for the number of Amazon VPCs that a client may have in an area?
15. 5
16. 6
17. 7
18. There is no maximum limit for VPCs available within a region by design.

**Answer to Review Questions**

* 1. A. The allowed range of prefix lengths for a VPC CIDR is between /16 and

/28 inclusive. The maximum possible prefix length for an IP subnet is /32, hence, /56 is not a valid length.

* 1. C. A secondary CIDR may come from similar RFC 1918 address range as the primary option, but it may not overlap the primary CIDR. 192.168.0.0/24 comes from the same address range (192.168.0.0–192.168.255.255) as the primary option and does not overlap with 192.168.16.0/24. 192.168.0.0/16 and 192.168.16.0/23 both overlap with 192.168.16.0/24. 172.31.0.0/16 is not in the same range as the primary CIDR.
  2. A, D. 10.0.0.0/24 and 10.0.0.0/23 are within the VPC CIDR and they leave room for a second subnet. 10.0.0.0/8 is wrong because prefix lengths less than

/16 aren't allowed. 10.0.0.0/16 doesn't leave room for another subnet.

* 1. A. The maximum subnet size you can have in a VPC is / 16.
  2. D. By creating a route to the Internet using an IGW, you have made this subnet public.
  3. A. When you create an Amazon VPC, a route table is created by default. It would be helpful if you manually created subnets and an IGW.
  4. C. When you set up an Amazon VPC, all subnets can communicate by default.
  5. A. You can only have one IGW for each Amazon VPC.
  6. B. Security groups are stateful, while network ACLs are stateless.
  7. C. You must disable source/destination checks for NAT.
  8. B, E. In the EC2-Classic network, the EIP is disconnected from the instance; in the EC2-VPC network, the EIP remains connected to the instance. The stop/start option of an Amazon EBS-based Amazon EC2 instance always changes the host computer regardless of the underlying network.
  9. D. Six VPC peering connections are required for each of the four VPCs to send traffic to each other.
  10. B. With a set of DHCP options, clients can define DNS servers for DNS name resolution, set domain names for instances within an Amazon VPC, define NTP servers, and define the NetBIOS name servers.
  11. D. A CGW is the client side of a VPN connection, and a network is linked to the Internet by an IGW. The Amazon side of a VPN connection is a VPG.
  12. A. The default limit on the number of Amazon VPCs a customer can have in a region is 5.