



ANS-C01^{Q&As}

AWS Certified Advanced Networking Specialty Exam

Pass Amazon ANS-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/ans-c01.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

A company has deployed a software-defined WAN (SD-WAN) solution to interconnect all of its offices. The company is migrating workloads to AWS and needs to extend its SD-WAN solution to support connectivity to these workloads. A network engineer plans to deploy AWS Transit Gateway Connect and two SD-WAN virtual appliances to provide this connectivity. According to company policies, only a single SD-WAN virtual appliance can handle traffic from AWS workloads at a given time. How should the network engineer configure routing to meet these requirements?

- A. Add a static default route in the transit gateway route table to point to the secondary SD-WAN virtual appliance. Add routes that are more specific to point to the primary SD-WAN virtual appliance.
- B. Configure the BGP community tag 7224:7300 on the primary SD-WAN virtual appliance for BGP routes toward the transit gateway.
- C. Configure the AS_PATH prepend attribute on the secondary SD-WAN virtual appliance for BGP routes toward the transit gateway.
- D. Disable equal-cost multi-path (ECMP) routing on the transit gateway for Transit Gateway Connect.

Correct Answer: C

A - incorrect, static routes are not possible in TGW B - incorrect, these BGP communities are used for BGP over DX C - correct, AS_PATH prepending is a standard BGP way of influencing return traffic for advertised prefixes and SDWAN supports this. D - incorrect, disabling ECMP will make sure the SDWAN>TGW traffic is not load shared, but the return traffic TGW>SDWAN is not affected and therefore both appliances will process traffic.

QUESTION 2

A company has agreed to collaborate with a partner for a research project. The company has multiple VPCs in the us-east-1 Region that use CIDR blocks within 10.10.0.0/16. The VPCs are connected by a transit gateway that is named TGW-C in us-east-1. TGW-C has an Autonomous System Number (ASN) configuration value of 64520.

The partner has multiple VPCs in us-east-1 that use CIDR blocks within 172.16.0.0/16. The VPCs are connected by a transit gateway that is named TGW-P in us-east-1. TGW-P has an ASN configuration value of 64530.

A network engineer needs to establish network connectivity between the company's VPCs and the partner's VPCs in us-east-1.

Which solution will meet these requirements with MINIMUM changes to both networks?

- A. Create a new VPC in a new account. Deploy a router from AWS Marketplace. Share TGW-C and TGW-P with the new account by using AWS Resource Access Manager (AWS RAM). Associate TGW-C and TGW-P with the new VPC. Configure the router in the new VPC to route between TGW-C and TGW-P.
- B. Create an IPsec VPN connection between TGW-C and TGW-P. Configure the routing between the transit gateways to use the IPsec VPN connection.
- C. Configure a cross-account transit gateway peering attachment between TGW-C and TGW-P. Configure the routing between the transit gateways to use the peering attachment.
- D. Share TGW-C with the partner account by using AWS Resource Access Manager (AWS RAM). Associate the partner VPCs with TGW-C. Configure routing in the partner VPCs and TGW-C.



Correct Answer: C

QUESTION 3

A company hosts its IT infrastructure in an on-premises data center. The company wants to migrate the infrastructure to the AWS Cloud in phases. A network engineer wants to set up a 10 Gbps AWS Direct Connect dedicated connection between the on-premises data center and VPCs. The company's network provider needs 3 months to provision the Direct Connect connection. In the meantime, the network engineer implements a temporary solution by deploying an AWS Site-to-Site VPN connection that terminates to a virtual private gateway. The network engineer observes that the bandwidth of the Site-to-Site VPN connection is capped at 1.25 Gbps despite a powerful customer gateway device. What should the network engineer do to improve the VPN connection bandwidth before the implementation of the Direct Connect connection?

- A. Contact AWS Support to request a bandwidth quota increase for the existing Site-to-Site VPN connection.
- B. Discuss the issue with the hardware vendor. Buy a bigger and more powerful customer gateway device that has faster encryption and decryption capabilities.
- C. Create several additional Site-to-Site VPN connections that terminate on the same virtual gateway. Configure equal-cost multi-path (ECMP) routing to use all the VPN connections simultaneously.
- D. Create a transit gateway. Attach the VPCs to the transit gateway. Create several additional Site-to-Site VPN connections that terminate on the transit gateway. Configure equal-cost multi-path (ECMP) routing to use all the VPN connections simultaneously.

Correct Answer: D

ECMP is not supported for Site-to-Site VPN connections on a virtual private gateway.

You can check this document: <https://docs.aws.amazon.com/vpn/latest/s2svpn/VPNRoutingTypes.html>

QUESTION 4

A company has a 2 Gbps AWS Direct Connect hosted connection from the company's office to a VPC in the ap-southeast-2 Region. A network engineer adds a 5 Gbps Direct Connect hosted connection from a different Direct Connect location in the same Region. The hosted connections are connected to different routers from the office with an iBGP session running in between the routers. The network engineer wants to ensure that the VPC uses the 5 Gbps hosted connection to route traffic to the office. Failover to the 2 Gbps hosted connection must occur when the 5 Gbps hosted connection is down. Which solution will meet these requirements?

- A. Configure an outbound BGP policy from the router that is connected to the 2 Gbps connection. Advertise routes with a longer AS_PATH attribute to AWS.
- B. Advertise a longer prefix route from the router that is connected to the 2 Gbps connection.
- C. Advertise a less specific route from the router that is connected to the 5 Gbps connection.
- D. Configure an outbound BGP policy from the router that is connected to the 5 Gbps connection. Advertise routes with a longer AS_PATH attribute to AWS.

Correct Answer: A

BGP prefers routes with a shorter AS_PATH over routes with a longer AS_PATH.



By advertising routes with a longer AS_PATH attribute from the 2 Gbps connection, you can make those routes less preferable than the routes advertised from the 5 Gbps connection. This way, the VPC will use the 5 Gbps connection to route

traffic to the office, as long as it is available. If the 5 Gbps connection goes down, BGP will fail over to the 2 Gbps connection.

QUESTION 5

A network engineer needs to deploy an AWS Network Firewall firewall into an existing AWS environment. The environment consists of the following: A transit gateway with all VPCs attached to it. Several hundred application VPCs. A centralized egress internet VPC with a NAT gateway and an internet gateway. A centralized ingress internet VPC that hosts public Application Load Balancers. On-premises connectivity through an AWS Direct Connect gateway attachment. The application VPCs have workloads deployed across multiple Availability Zones in private subnets with the VPC route table's default route (0.0.0.0/0) pointing to the transit gateway. The Network Firewall firewall needs to inspect east-west (VPC-to-VPC) traffic and north-south (internet-bound and on-premises network) traffic by using Suricata compatible rules. The network engineer must deploy the firewall by using a solution that requires the least possible architectural changes to the existing production environment. Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

- A. Deploy Network Firewall in all Availability Zones in each application VPC.
- B. Deploy Network Firewall in all Availability Zones in a centralized inspection VPC.
- C. Update the HOME_NET rule group variable to include all CIDR ranges of the VPCs and on-premises networks.
- D. Update the EXTERNAL_NET rule group variable to include all CIDR ranges of the VPCs and on-premises networks.
- E. Configure a single transit gateway route table. Associate all application VPCs and the centralized inspection VPC with this route table.
- F. Configure two transit gateway route tables. Associate all application VPCs with one transit gateway route table. Associate the centralized inspection VPC with the other transit gateway route table.

Correct Answer: BCF

Option B: A centralized inspection VPC approach would lead to a minimal architectural change and efficiently use Network Firewall resources. Option C: HOME_NET is usually defined as your local network. In this case, it would include all your VPCs and on-premises networks.

Option F: Configuring two transit gateway route tables, one associated with all the application VPCs and another with the inspection VPC, will help route traffic effectively for inspection. All outbound traffic from application VPCs would be routed to the inspection VPC for firewall checks, and then the inspected traffic would be routed to its destination (internet or another VPC).

[ANS-C01 PDF Dumps](#)

[ANS-C01 Practice Test](#)

[ANS-C01 Exam Questions](#)