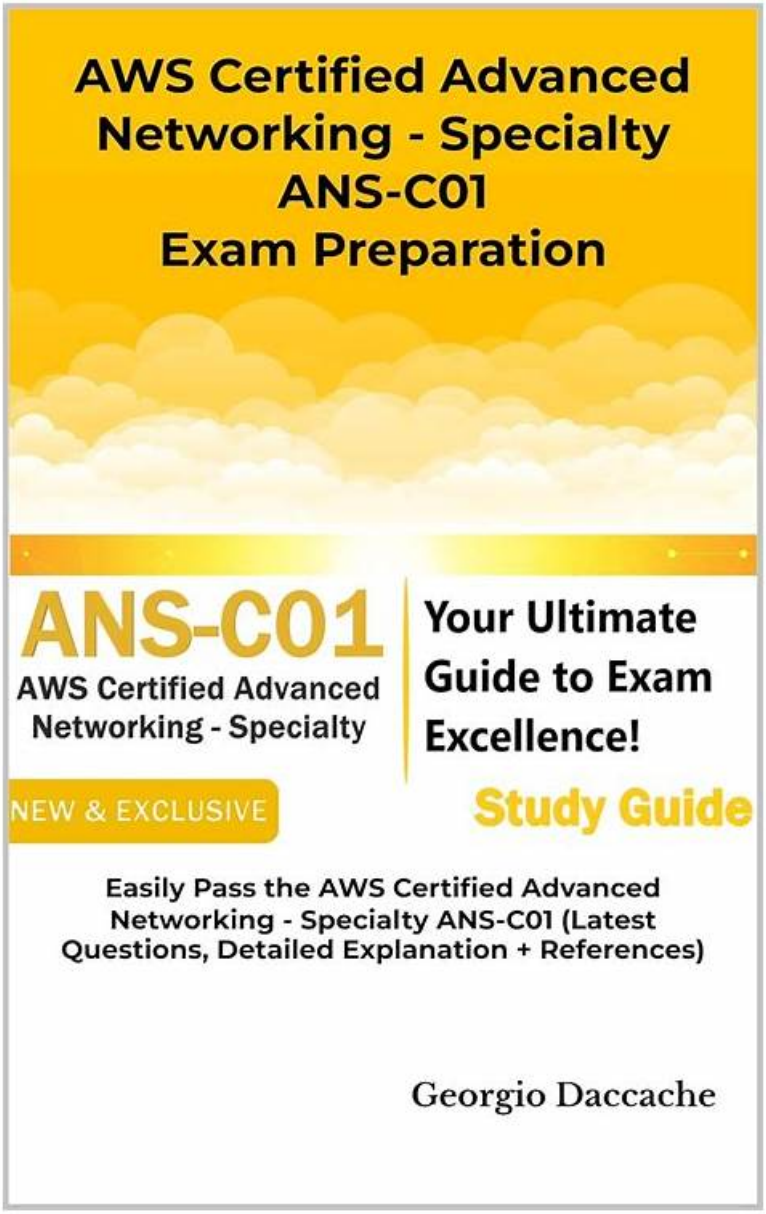
ANS-C01 Exam Online - ANS-C01 Books PDF



What's more, part of that Pass4cram ANS-C01 dumps now are free: https://drive.google.com/open?id=15pLhh_hivdHRq1TfQYqmwG8BKH6Qj0WM

Amazon ANS-C01 Exam is a very hot exam. Although it is difficult to pass the exam, the identification of entry point will make you easy to pass your exam. Pass4cram practice test dumps are your best choice and hit rate is up to 100%. And our exam dumps can help you solve any questions of ANS-C01 exam. As long as you carefully study the questions in the dumps, all problems can be solved. Purchasing Pass4cram certification training dumps, we provide you with free updates for a year. Within a year, as long as you want to update the dumps you have, you can get the latest version. Try it and see for yourself.

To pass the ANS-C01 Exam, candidates must demonstrate a strong understanding of advanced networking concepts and technologies, as well as the ability to apply this knowledge to real-world scenarios. ANS-C01 exam consists of multiple-choice and multiple-response questions, and candidates have 170 minutes to complete it. Passing the exam validates the candidate's technical expertise and opens up new opportunities for career growth in the field of cloud networking.

>> ANS-C01 Exam Online <<

High Pass-Rate ANS-C01 Exam Online offer you accurate Books PDF | Amazon AWS Certified Advanced Networking Specialty Exam

In fact, many candidates have the willing and ambition to pass the ANS-C01 exam and achieve the certification for they want to challege themself to become better. The efficiency of going it alone is very low, and it is easy to go to a dead end. You really need a helper. Take a look at the development of ANS-C01 Guide quiz and you will certainly be attracted to it. The advantages of ANS-C01 study materials are numerous and they are all you need!

To become certified in the Amazon ANS-C01, individuals must possess a deep understanding of AWS networking services, including VPCs, Route 53, Direct Connect, VPN, and Elastic Load Balancing. ANS-C01 Exam covers a wide range of topics, including network design, implementation, optimization, and troubleshooting. It also tests the candidate's knowledge of security, compliance, and governance requirements in AWS networking solutions.

Amazon AWS Certified Advanced Networking Specialty Exam Sample Questions (Q22-Q27):

NEW QUESTION # 22
A Network Engineer needs to be automatically notified when a certain TCP port is accessed on a fleet of Amazon EC2 instances running in an Amazon VPC. Which of the following is the MOST reliable solution?
Response:

- A. Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to notify the Administrator with Amazon SNS each time the TCP port is accessed.
- B. Create an inbound rule in the VPC's network ACL that matches the TCP port. Create an Amazon CloudWatch alarm on the NetworkPackets metric for the ACL that uses Amazon SNS to notify the Administrator when the metric is greater than zero.
- C. Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to publish to a custom Amazon CloudWatch metric each time the TCP port is accessed. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.
- D. Create VPC Flow Logs that write to Amazon CloudWatch Logs, with a metric filter matching connections on the required port. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.

Answer: D

NEW QUESTION # 23
A network engineer is using AWS Direct Connect connections and MACsec to encrypt data from a corporate data center to the Direct Connect location. The network engineer learns that the MACsec secret key might have been compromised. The network engineer needs to update the connection with an uncompromised secure key.
Which solution will meet this requirement?

- A. Modify the existing MACsec secret key. Associate the new pre-shared key. Connection Key Name (CKN). and Connectivity Association Key (CAK) with the connection.
- B. Create a new MACsec secret key that uses an AWS Key Management Service (AWS KMS) AWS managed key. Associate the new pre-shared key, Connection Key Name (CKN). and Connectivity Association Key (CAK) with the connection.
- C. Modify the existing MACsec secret key. Re-associate the existing pre-shared key. Connection Key Name (CKN), and Connectivity Association Key (CAK) with the connection.
- D. Create a new MACsec secret key that uses an AWS Key Management Service (AWS KMS) customer managed key. Associate the new pre-shared key, Connection Key Name (CKN). and Connectivity Association Key (CAK) with the connection.

Answer: B

NEW QUESTION # 24
A network engineer needs to build an encrypted connection between an on-premises data center and a VPC. The network engineer attaches the VPC to a virtual private gateway and sets up an AWS Site-to-Site VPN connection. The VPN tunnel is UP after

configuration and is working.
However, during rekey for phase 2 of the VPN negotiation, the customer gateway device is receiving different parameters than the parameters that the device is configured to support.
The network engineer checks the IPsec configuration of the VPN tunnel. The network engineer notices that the customer gateway device is configured with the most secure encryption algorithms that the AWS Site-to-Site VPN configuration file provides.
What should the network engineer do to troubleshoot and correct the issue?

- A. Check the native virtual private gateway logs. Restrict the VPN tunnel options to the specific VPN parameters that the virtual private gateway requires.
- B. Check the native customer gateway logs. Restrict the VPN tunnel options to the specific VPN parameters that the customer gateway requires.
- C. Check Amazon CloudWatch logs of the customer gateway. Restrict the VPN tunnel options to the specific VPN parameters that the customer gateway requires.
- D. Check Amazon CloudWatch logs of the virtual private gateway. Restrict the VPN tunnel options to the specific VPN parameters that the virtual private gateway requires.

Answer: C

Explanation:
Site-to-Site VPN logs can be published to Amazon CloudWatch Logs. This feature provides customers with a single consistent way to access and analyze detailed logs for all of their Site-to- Site VPN connections.

NEW QUESTION # 25
A company's AWS environment has two VPCs. VPC A has a CIDR block of 192.168.0.0/16. VPC B has a CIDR block of 10.0.0.0/16. Each VPC is deployed in a separate AWS Region. The company has remote users who work outside the company's offices. These users need to connect to an application that is running in the VPCs.
Traffic to and from the VPCs over the internet must be encrypted. A network engineer must set up connectivity between the remote users and the VPCs.
Which combination of steps should the network engineer take to meet these requirements with the LEAST management overhead? (Choose three.)

- A. Establish a VPC peering connection between VPC A and VPC B.
- B. Create an AWS Client VPN endpoint in VPC A and VPC B Add an authorization rule to grant access to VPC A and VPC B.
- C. Create an AWS Client VPN endpoint in VPC A Add an authorization rule to grant access to VPC A and VPC B.
- D. Add a route to the AWS Client VPN endpoint's route table to direct traffic to VPC A.
- E. Establish an AWS Site-to-Site VPN connection between VPC A and VPC B.
- F. Add a route to the AWS Client VPN endpoint's route table to direct traffic to VPC B.

Answer: A,C,F

Explanation:
The procedure for allowing access to a peered VPC outlined below, is only required if the Client VPN endpoint was configured for split-tunnel mode. In full-tunnel mode, access to the peered VPC is allowed by default.
https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-peered.html

NEW QUESTION # 26
A company is migrating critical applications to AWS. The company has multiple accounts and VPCs that are connected by a transit gateway.
A network engineer must design a solution that performs deep packet inspection for any traffic that leaves a VPC network boundary. All inspected traffic and the actions that are taken on the traffic must be logged in a central log account.
Which solution will meet these requirements with the LEAST administrative overhead?

- A. Create a central network VPC that includes an attachment to the transit gateway. Update the VPC and transit gateway route tables to support the new attachment. Deploy an AWS Gateway Load Balancer that is backed by third-party, next-generation firewall appliances to the central network VPC. Create a policy that contains the rules for deep packet inspection. Attach the policy to the firewall appliances.
  Create an Amazon S3 bucket in the central log account. Configure the firewall appliances to capture and save the network flow logs to the S3 bucket.

- B. Deploy network ACLs and security groups to each VPC. Attach the security groups to active network interfaces. Associate the network ACLs with VPC subnets. Create rules for the network ACLs and security groups to allow only the required traffic flows between subnets and network interfaces. Create an Amazon S3 bucket in the central log account. Configure a VPC flow log that captures and saves all traffic flows to the S3 bucket.
- C. Create a central network VPC that includes an attachment to the transit gateway. Update the VPC and transit gateway route tables to support the new attachment. Deploy an AWS Application Load Balancer that is backed by third-party, next-generation firewall appliances to the central network VPC. Create a policy that contains the rules for deep packet inspection. Attach the policy to the firewall appliances.
  Create a syslog server in the central log account. Configure the firewall appliances to capture and save the network flow logs to the syslog server.
- D. Create a central log VPC and an attachment to the transit gateway. Update the VPC and transit gateway route tables to support the new attachment. Deploy an AWS Network Load Balancer (NLB) that is backed by third-party, next-generation intrusion detection system (IDS) security appliances to the central VPC. Activate rules on the security appliances to monitor for intrusion signatures. For each network interface, create a VPC Traffic Mirroring session that sends the traffic to the central VPC's NLB.

Answer: A

NEW QUESTION # 27

.....