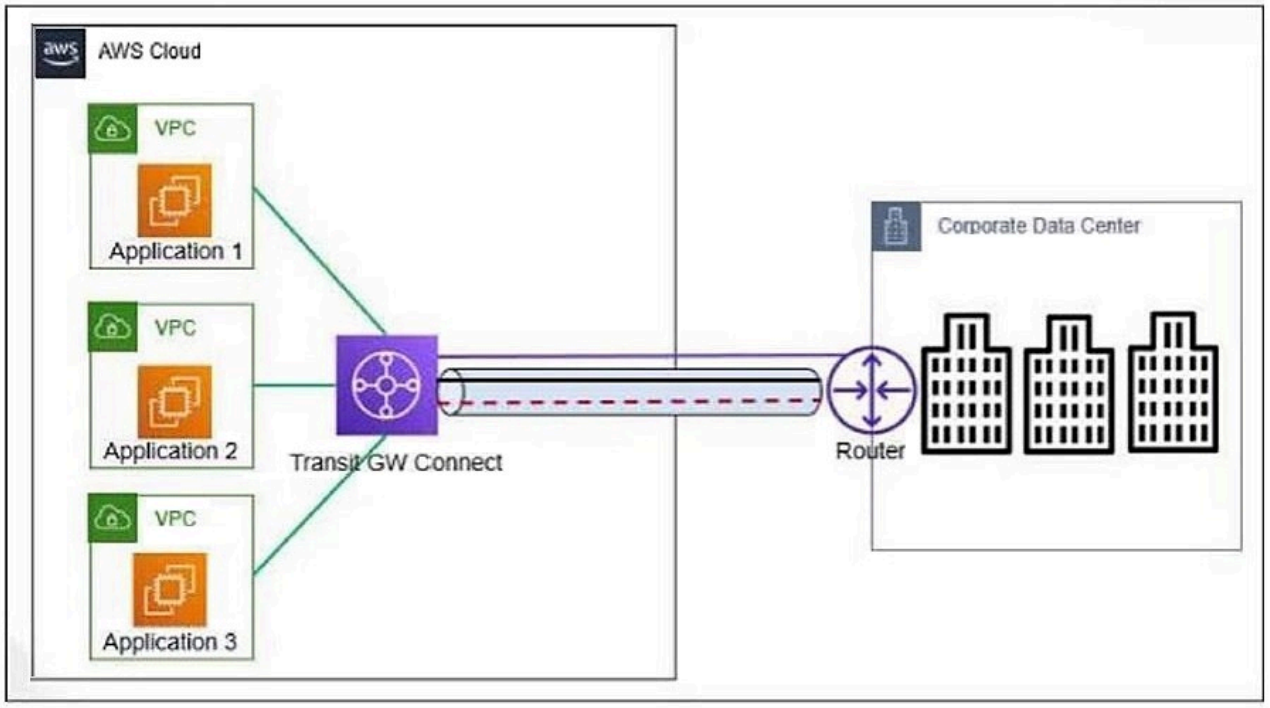
Question #1 *Topic 1*

Refer to the exhibit.



An organization deployed the application servers in the AWS VPC that connects to the corporate data center using Transit Gateway Connect. Demand for the applications has grown and the connection requires more bandwidth.
What is required to achieve higher bandwidth?

A. Use routable public IP addresses instead of private IP addresses for connectivity.

B. You cannot increase bandwidth the connection has a fixed limit.

C. No configuration change is required because GRE tunnels are scaled to provide higher bandwidth.

D. You add a Transit VPC between the organization's VPCs.

Suggested Answer: *C*

Owie 1 week ago

Selected Answer: C

Pls is this updated now

upvoted 1 times

Interrogantis 2 months, 2 weeks ago

WARNING: QUESTIONS ON THIS EXAM IS NOT UPDATED. I only got 2 questions from here.

upvoted 2 times

professa 5 months ago

Exam topic, Please review these questions. I failed teribly

upvoted 3 times

e5c20bb 5 months, 3 weeks ago

Page 61 of the Study Guide C is correct

upvoted 1 times

ipv84 6 months, 1 week ago

C - is correct.

upvoted 1 times

Question #2 *Topic 1*

You want to deploy the Fortinet HA CloudFormation template to stage and bootstrap the FortiGate configuration in the same region in which you created your VPC, which is Ohio US-East-2.
Based on this information, which statement is correct?

A. You create an S3 bucket to stage and bootstrap FortiGate with an FGCP unicast configuration. The S3 bucket can be hosted in any region.

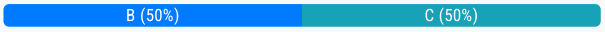
B. The Fortinet HA cloud formation template automatically creates an S3 bucket.

C. You create an S3 bucket to stage and bootstrap FortiGate with an FGCP unicast configuration. The S3 bucket needs to be hosted in the Ohio US-East-2 region.

D. You create a DynamoDB to stage and bootstrap FortiGate with an FGCP unicast configuration. It needs to be hosted in the Ohio US-East-2 region.

Suggested Answer: *C*

Community vote distribution



havokdu 1 month, 2 weeks ago

Selected Answer: C

Answer: C

You must create an S3 bucket to stage and bootstrap the FortiGate configuration, and this S3 bucket must reside in the same region where the VPC and CloudFormation stack are being deployed—in this case, the Ohio (us-east-2) region.

Explanation: The Fortinet HA CloudFormation templates rely on S3 for storing configuration files and bootstrap data for the FortiGate instances. To ensure that the template functions correctly and to comply with AWS regional resource dependencies, the S3 bucket that hosts these files should be in the same region as the resources it supports. In this scenario, since the VPC is created in Ohio (us-east-2), the S3 bucket hosting the bootstrap configuration also needs to be in the Ohio (us-east-2) region.

upvoted 2 times

lucient 3 months, 1 week ago

Selected Answer: B

B. Page 157: This cloud formation template creates an Amazon S3 bucket for writing and storing logs, allows FortiGate CNF read-only access to your VPCs, and grants access to your AWS Security Lake, if applicable.

upvoted 1 times

myrmidon3 3 months, 2 weeks ago

Selected Answer: C

The correct statement is C:

You create an S3 bucket to stage and bootstrap FortiGate with an FGCP unicast configuration. The S3 bucket needs to be hosted in the Ohio US-East-2 region.

This is because when deploying the Fortinet HA CloudFormation template and bootstrapping the FortiGate in a specific region (Ohio US-East-2 in your case), it is important to ensure that resources like S3 buckets used for staging and bootstrapping are in the same region to reduce latency and comply with any regional restrictions.

upvoted 2 times

yerno1 3 months, 4 weeks ago

Selected Answer: B

It is B, This cloud formation template creates an Amazon S3 bucket for writing and storing logs, allows FortiGate CNF read-only access to your VPCs, and grants access to your AWS Security Lake, if applicable.

upvoted 1 times

DataConsult 5 months ago

it is B

upvoted 1 times

ipv84 5 months, 2 weeks ago

Selected Answer: C

i think it's C...

upvoted 1 times

Spawni81 5 months, 3 weeks ago

B - Study Guide 7.4 - Page 136 & 137

upvoted 2 times

myrmidon3 3 months, 2 weeks ago

Based on the information from pages 136 and 137 of the document, there is no indication that the Fortinet HA CloudFormation template automatically creates an S3 bucket. The text explains that CloudFormation templates can automate and streamline the deployment of AWS infrastructure, but it does not specify that the template itself creates an S3 bucket as part of the FortiGate HA setup.
The document does, however, highlight the use of CloudFormation templates to create resources like subnets and IP addresses, but staging and bootstrapping FortiGate typically require manual creation of an S3 bucket in the specified region.

upvoted 1 times

lucient 3 months, 1 week ago

Are you serious? Page 157: This cloud formation template creates an Amazon S3 bucket for writing and storing logs, allows FortiGate CNF read-only access to your VPCs, and grants access to your AWS Security Lake, if applicable.

upvoted 1 times

hecgonvi 2 months ago

He's really serious. Plus, you're mixing up FortiGate CNF and FortiGate VM. It's not in the official docs, but it's mentioned in Fortinet's GitHub repo: ´Create a new S3 bucket in the same region where the template will be deployed. If the bucket is in a different region than the template deployment, bootstrapping will fail and the FGTs will be unaccessable´

upvoted 1 times

e5c20bb 5 months, 3 weeks ago

B - Page 157 of the Study Guide

upvoted 1 times

myrmidon3 3 months, 2 weeks ago

The information on page 156 of the document indicates that a CloudFormation template, when executed in the FortiGate CNF console, automatically creates an S3 bucket for storing logs. However, this applies specifically to FortiGate CNF setup, which might differ slightly from the traditional Fortinet HA CloudFormation template deployment. This suggests that while FortiGate CNF does automate the creation of an S3 bucket, there is no direct mention of this feature in a standard HA deployment scenario.

upvoted 1 times

lucient 3 months, 1 week ago

Again, are you serious? Page 157: This cloud formation template creates an Amazon S3 bucket for writing and storing logs, allows FortiGate CNF read-only access to your VPCs, and grants access to your AWS Security Lake, if applicable.

upvoted 1 times

Question #3 *Topic 1*

An organization has the requirement to connect a data VPC to the on-premises infrastructure of a branch office in a hybrid cloud environment. The connectivity needs the higher bandwidth but the organization does not want to use multiple connections between sites.
Which AWS solution meets the requirement?

A. Transit VPC with IPSec

B. Internet Gateway

C. Transit Gateway multicast

D. Transit Gateway Connect

Suggested Answer: *D*

Community vote distribution

D (100%)

havokdu 1 month, 2 weeks ago

Selected Answer: D

Study guide pages 61 trough 64

upvoted 1 times

myrmidon3 3 months, 2 weeks ago

Selected Answer: D

The correct AWS solution to connect a data VPC to the on-premises infrastructure with higher bandwidth and without using multiple connections is:

Transit Gateway Connect.

Transit Gateway Connect provides a seamless connection between your on-premises network (such as through SD-WAN) and AWS using higher bandwidth with support for Generic Routing Encapsulation (GRE) and Border Gateway Protocol (BGP) for dynamic routing. It simplifies connectivity by creating a centralized transit gateway without needing multiple IPsec tunnels, making it ideal for hybrid cloud environments that require high bandwidth.

upvoted 2 times

myrmidon3 3 months, 2 weeks ago

Here's why the other options are less suitable:

Transit VPC with IPsec: While it can connect VPCs, it involves managing multiple VPN tunnels and does not offer the higher bandwidth performance of Transit Gateway Connect.
Internet Gateway: This is used to provide internet access to VPCs but is not used for connecting on-premises networks to VPCs.
Transit Gateway Multicast: This is used for multicast routing between VPCs and on-premises networks, but it doesn't address the requirement for higher bandwidth or simpler connectivity.

Thus, Transit Gateway Connect is the best solution for this scenario.

upvoted 1 times

Spawni81 5 months, 3 weeks ago

D - Correct. Study Guide 7.4 Page 58

upvoted 2 times

ipv84 6 months, 1 week ago

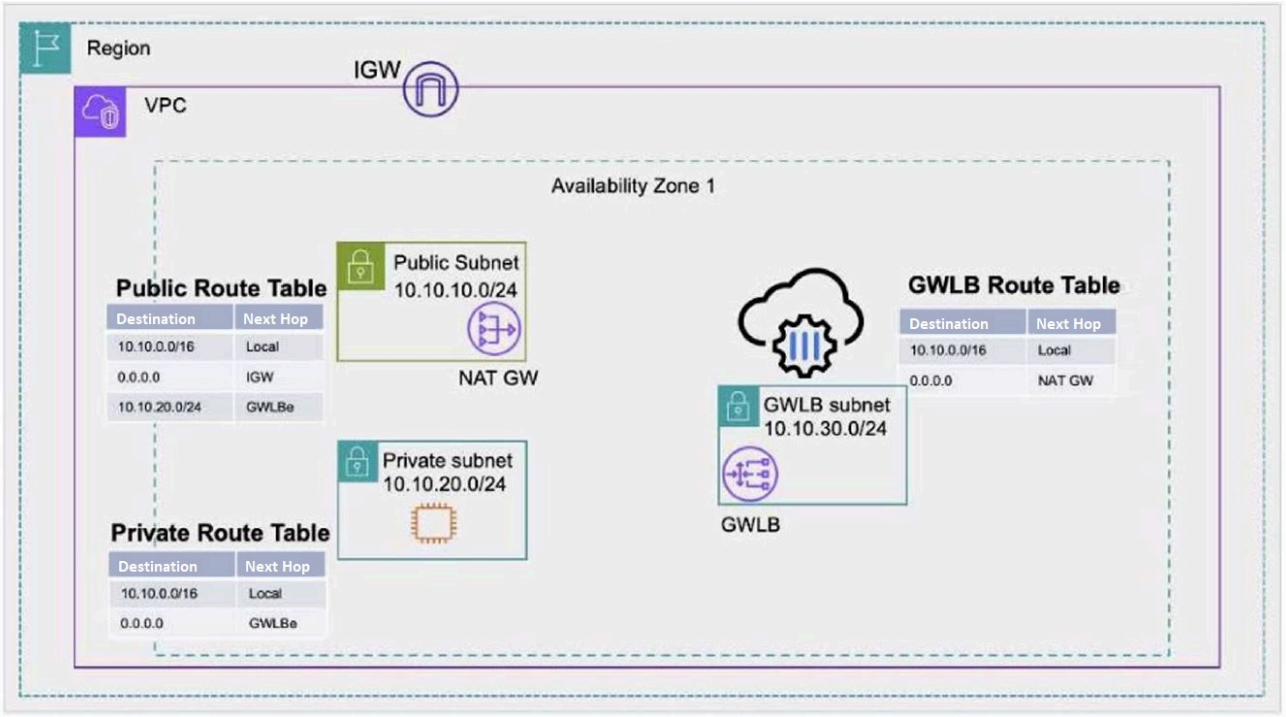
D - Correct.

upvoted 1 times

Question #4 *Topic 1*

Refer to the exhibit.

FortiGate CNF deployment



Traffic is initiated from the EC2 instance and is destined for the internet.
Which traffic flow is correct?

A. EC2 instance > NAT GW > IGW > internet

B. There is no route to the internet in the Private Route Table. The traffic does not reach the internet.

C. EC2 instance > GWLBe > NAT GW > IGW > internet

D. EC2 instance > GWLBe > internet

Suggested Answer: *C*

Community vote distribution

C (100%)

DataConsult 5 months ago
C correct
upvoted 1 times

Spawni81 5 months, 3 weeks ago
C is correct - Study Guide 7.4 Page 159
upvoted 2 times

the_giant 6 months ago
Selected Answer: C
C should be the correct answer
upvoted 1 times

jhoncena 7 months, 2 weeks ago
Selected Answer: C
C should be the correct answer
upvoted 2 times

Question #5 *Topic 1*

A customer has implemented GWLB between the partner and application VPCs. FortiGate appliances are deployed in the partner VPC with multiple AZs to inspect traffic transparently.
Which two things will happen to application traffic based on the GWLB deployment? (Choose two.)

A. Inbound and outbound traffic will go to multiple devices, which will perform load balancing.

B. Inbound and outbound traffic will go to the same device, which will perform stateful processing.

C. The content of the original traffic exchanged between the GWLB and FortiGate will be preserved.

D. The original traffic exchanged between the GWLB and FortiGate will be hashed for data integrity.

Suggested Answer: *BC*

Community vote distribution

jlmadvig Highly Voted 7 months ago

Selected Answer: BC

GWLB ensures that traffic flows are sent to the same appliance to maintain stateful processing. This is critical for the functioning of stateful firewalls like FortiGate, which need to keep track of the state of connections to inspect traffic effectively.
GLB and the virtual appliances exchange application traffic with other using GENEVE, which allows GWLB to preserve the content of the original traffic.

upvoted 8 times

havokdu Most Recent 1 month, 2 weeks ago

Selected Answer: BC

Study guide pages 147 and 150.

upvoted 1 times

havokdu 1 month, 2 weeks ago

Options A and D are incorrect:

A: Suggesting that inbound and outbound traffic will go to multiple devices would break stateful processing. Instead, GWLB ensures that both directions of a flow end up at the same appliance.
D: GWLB does not hash the original traffic content for data integrity. It uses flow-based hashing to ensure symmetrical routing, but the packet content itself remains intact and is not hashed for integrity checks in this manner.

upvoted 1 times

myrmidon3 3 months, 2 weeks ago

Selected Answer: BC

Inbound and outbound traffic will go to the same device, which will perform stateful processing: The Gateway Load Balancer (GWLB) in AWS ensures that traffic is forwarded to the same FortiGate device for stateful inspection. This ensures that the session remains intact during the processing.

The content of the original traffic exchanged between the GWLB and FortiGate will be preserved: The GWLB uses the Generic Network Virtualization Encapsulation (GENEVE) protocol, which preserves the original traffic content during its transmission to and from the FortiGate device for inspection.

These references confirm that GWLB ensures stateful traffic processing and preserves the content of the original traffic when exchanged between the GWLB and FortiGate appliances.

upvoted 2 times

the_giant 6 months ago

Selected Answer: BC

B,C should be correct

upvoted 4 times

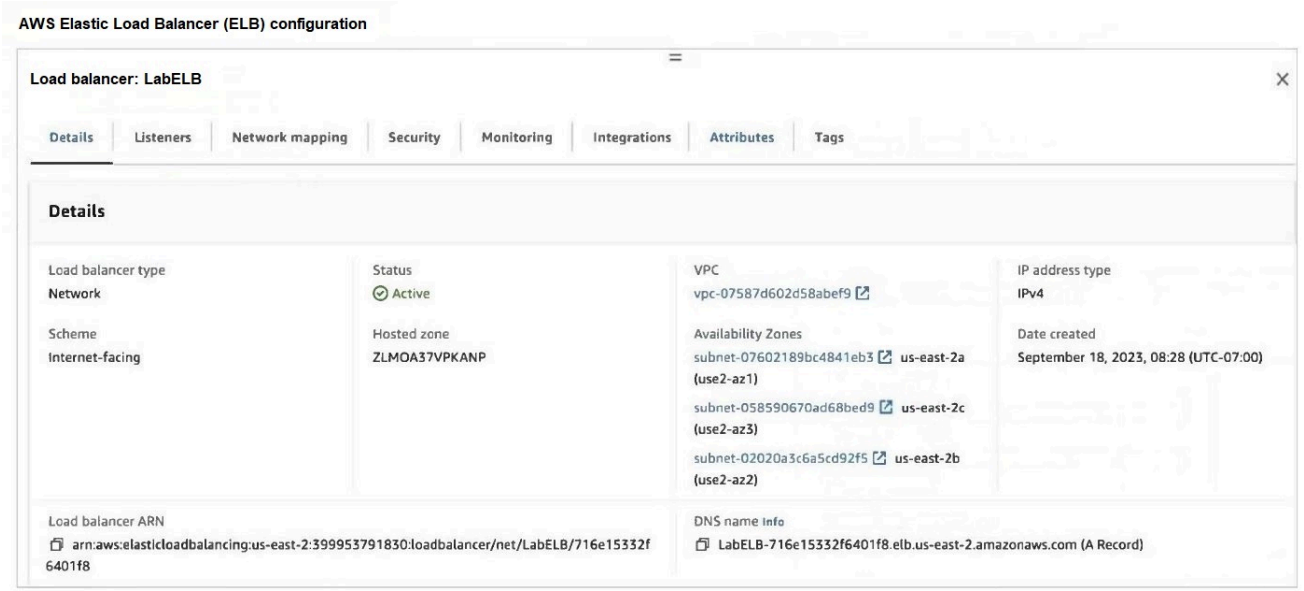
jhoncena 7 months, 2 weeks ago

Answer should be Answer : A, B

upvoted 1 times

Question #6 *Topic 1*

Refer to the exhibit.



A customer is using the AWS Elastic Load Balancer (ELB).
Which two statements are correct about the ELB configuration? (Choose two.)

A. The load balancer is configured to load balance traffic among multiple availability zones.

B. The Amazon Resource Name is used to access the load balancer node and targets.

C. You can use the DNS name to reach the targets behind the ELB.

D. The load balancer is configured for the internal traffic of the virtual public cloud (VPC).

Suggested Answer: *AC*

Community vote distribution

AC (100%)

havokdu 1 month, 2 weeks ago

Selected Answer: AC

Explanation:
A (The load balancer is configured to load balance traffic among multiple availability zones):
The provided ELB configuration shows multiple subnets deployed in different availability zones. ELBs are designed to distribute traffic across multiple AZs to ensure high availability and fault tolerance. This statement is correct.

C (You can use the DNS name to reach the targets behind the ELB):
AWS ELBs provide a DNS name that clients can use to access your applications. Traffic sent to this DNS name is routed to one of the underlying targets (such as EC2 instances) registered with the load balancer. This statement is also correct.
upvoted 1 times

myrmidon3 3 months, 2 weeks ago

Selected Answer: AC

A. The load balancer is configured to load balance traffic among multiple availability zones.

The exhibit shows that the ELB spans multiple availability zones, including us-east-2a, us-east-2b, and us-east-2c, indicating that it is set up for cross-AZ load balancing.

C. You can use the DNS name to reach the targets behind the ELB.

The DNS name (LabELB-716e15332f6401f8.elb.us-east-2.amazonaws.com) provided in the exhibit is used to access the load balancer, which distributes the traffic to the targets behind it.

The other options are incorrect:

B: The Amazon Resource Name (ARN) identifies the load balancer resource but is not used to access the ELB or its targets.
D: The ELB is Internet-facing, as indicated in the exhibit, not configured for internal VPC traffic.
upvoted 2 times

jorgeluis 5 months, 2 weeks ago
not D: scheme = internet facing
not B: not used to reach load balancers
upvoted 1 times

e5c20bb 5 months, 2 weeks ago
A Page 144 & 145 The main types of load balancers covered in this lesson are ELB and the GWI_B. The ELB encompasses the NLB, the ALB, and the CLB. NLB can handle the varying load of your traffic in a single AZ or across multiple AZs.
C. page 45 Amazon Route 53: A scalable and highly available domain name system (DNS) web service, designed to route incoming internet traffic to resources such as web servers, load balancers, and other AWS services.
upvoted 1 times

Question #7 *Topic 1*

Which two statements about the FortiCloud portal are true? (Choose two.)

A. You can gain remote access to your FortiGate VM directly from the portal.

B. To assign permissions in the identity and access management (IAM) portal, you must write a JSON script.

C. You can access the FortiFlex portal only after you purchase a FortiFlex license and register it on FortiCare.

D. You can access only cloud services that you have subscribed to on AWS marketplace.

Suggested Answer: *AD*

Community vote distribution

AC (100%)

jhoncena Highly Voted 7 months, 2 weeks ago

Answer : A, C

upvoted 6 times

havokdu Most Recent 1 month, 2 weeks ago

Selected Answer: AC

Explanation:

A (You can gain remote access to your FortiGate VM directly from the portal):
The FortiCloud portal provides centralized management and monitoring of FortiGate VMs, including features like remote console or web-based GUI access. This statement is true.

C (You can access the FortiFlex portal only after you purchase a FortiFlex license and register it on FortiCare):
FortiFlex is a licensing model that requires you to purchase and register the license through FortiCare before you can access the related portal. This statement is also true.

upvoted 2 times

myrmidon3 3 months, 2 weeks ago

Selected Answer: AC

You can gain remote access to your FortiGate VM directly from the portal: The FortiCloud portal provides product and license information, including the capability to remotely access FortiGate VMs.

You can access the FortiFlex portal only after you purchase a FortiFlex license and register it on FortiCare: The document mentions that after acquiring and registering a FortiFlex license on FortiCare, you can access the FortiFlex portal through FortiCloud

upvoted 2 times

yerno1 3 months, 4 weeks ago

Selected Answer: AC

A StudyGuide p28

C StudyGuide p31

upvoted 2 times

jorgeluis 5 months, 2 weeks ago

not D: You can access any products you have registered, not only those from the marketplace

upvoted 1 times

e5c20bb 5 months, 2 weeks ago

A StudyGuide p28

C StudyGuide p 31

upvoted 3 times

Question #8 *Topic 1*

Which three statements correctly describe FortiGate Cloud-Native Firewall (CNF)? (Choose three.)

A. It provides carrier-grade protection.

B. It scales seamlessly.

C. It uses AWS Elastic Load Balancing (ELB).

D. It is considered to be a Firewall-as-a-Service (FWaaS).

E. It can be managed by FortiManager and AWS firewall manager.

Suggested Answer: *ABD*

Community vote distribution

BDE (100%)

havokdu 1 month, 2 weeks ago

Selected Answer: BDE

Why the others are not correct:

A (It provides carrier-grade protection):
While FortiGate solutions offer enterprise-level security, the term "carrier-grade" typically refers to solutions designed specifically for telecommunications service providers with extremely high availability and scale requirements. CNF is not specifically marketed as "carrier-grade."

C (It uses AWS Elastic Load Balancing (ELB)):
FortiGate CNF leverages AWS services in a native manner. While load balancing is a fundamental concept, CNF integrates more closely with AWS Gateway Load Balancer (GWLB) rather than just a standard ELB. The statement as given is not entirely accurate.

upvoted 1 times

myrmidon3 3 months, 2 weeks ago

B. It scales seamlessly.

FortiGate CNF leverages the cloud's native scaling capabilities, ensuring that firewall resources can dynamically scale with the needs of the cloud environment.

D. It is considered to be a Firewall-as-a-Service (FWaaS).

FortiGate CNF is a cloud-native solution, meaning it is delivered as a service (FWaaS), offering firewall functionality without the need for managing underlying infrastructure.

E. It can be managed by FortiManager and AWS Firewall Manager.

FortiGate CNF integrates with both FortiManager for centralized management and AWS Firewall Manager for security policies across multiple AWS accounts and resources.

The other options are incorrect:

A: Carrier-grade protection is not a specific feature attributed to FortiGate CNF.
C: FortiGate CNF does not use AWS Elastic Load Balancing (ELB) directly for its firewall functionality.

upvoted 2 times

yerno1 3 months, 4 weeks ago

Selected Answer: BDE

Answer: B, D & E are correct,
Study guide page 154.

upvoted 1 times

jorgeluis 5 months, 2 weeks ago

Answer: B, D & E

Documentation say nothing about carrier grade protection

upvoted 1 times

jhoncena 7 months, 2 weeks ago

Answer : B, D,E

upvoted 4 times

Question #9 *Topic 1*

AWS native network services offer vast functionality and inter-connectivity between the cloud and on-premises networks.
Which three additional functions can FortiGate for AWS offer to complement the native services offered by AWS? (Choose three.)

A. Higher VPN throughput

B. Web filtering

C. OSPF over IPSec

D. Advanced dynamic routing

E. Secure SD-WAN with application visibility

Suggested Answer: *ABE*

Community vote distribution

B0bs 2 months, 2 weeks ago
where do i get the study guide?
upvoted 1 times

myrmidon3 3 months, 2 weeks ago
Selected Answer: BCE
The three additional functions that FortiGate for AWS can offer to complement the native services offered by AWS are:
B. Web filtering
FortiGate provides advanced web filtering capabilities, allowing administrators to block or allow access to specific websites and categories, which is not a feature of native AWS services.

C. OSPF over IPSec
FortiGate supports advanced routing protocols like OSPF (Open Shortest Path First) over IPSec VPNs, which enhances routing capabilities in a hybrid cloud setup, complementing AWS's native routing services.

E. Secure SD-WAN with application visibility

FortiGate offers Secure SD-WAN with advanced application visibility and traffic shaping, providing more granular control over how traffic flows between different networks and optimizing performance, something AWS native services don't provide by default.
upvoted 2 times

DataConsult 5 months ago
study guide 97 C,D,E is correct in my opinion
upvoted 3 times

ipv84 6 months ago
Selected Answer: BCE
B, C, and E in my opinion.
upvoted 2 times

the_giant 6 months ago
Selected Answer: BCD
B,C,E is correct
upvoted 2 times

Question #10 *Topic 1*

Your organization is deciding between deploying an active-active (A-A) or active-passive (A-P) FortiGate high availability (HA) cluster in AWS cloud.
Which two statements are true about A-A clusters compared to A-P clusters? (Choose two.)

A. For A-A clusters, FortiGate must perform SNAT inbound to ensure symmetric traffic flow.

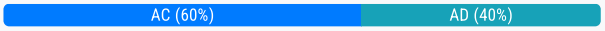
B. A-A clusters rely on API calls for failovers.

C. A-A clusters always require a load balancer.

D. A-A clusters can use a software-defined network (SDN) to perform a failover.

Suggested Answer: *AC*

Community vote distribution



myrmidon3 3 months, 2 weeks ago

Selected Answer: AC

a. For A-A clusters, FortiGate must perform SNAT inbound to ensure symmetric traffic flow.

In an active-active cluster, traffic distribution is split between multiple FortiGate units. To maintain symmetric traffic flow across the units, Source NAT (SNAT) must be used. This ensures that the return traffic follows the same path as the inbound traffic.

c. A-A clusters always require a load balancer.

Active-active clusters need a load balancer to distribute traffic across multiple active FortiGate units to ensure they both process traffic simultaneously. The load balancer helps manage traffic across both active devices in the cluster.

The other options are less accurate:

b. API calls are primarily involved in managing failovers for active-passive (A-P) clusters, not active-active.
d. Active-passive clusters typically utilize SDN for failover, while active-active clusters rely more on load balancers for traffic distribution.

These distinctions help to clarify the key differences between A-A and A-P setups.
upvoted 2 times

yerno1 3 months, 3 weeks ago

Selected Answer: AC

A and C, are correct.
upvoted 1 times

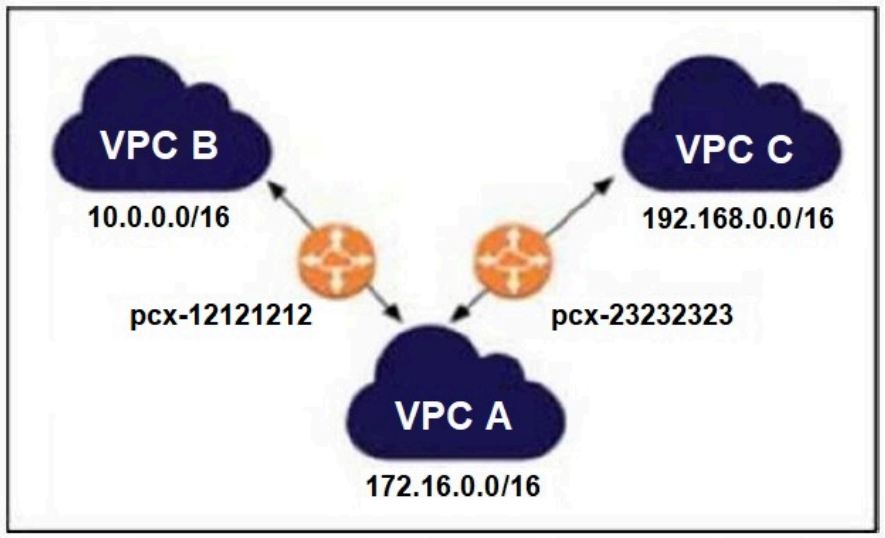
the_giant 6 months ago

Selected Answer: AD

A,C Study Guide Page 146
upvoted 2 times

Question #11 *Topic 1*

Refer to the exhibit.



Which statement is correct about the VPC peering connections shown in the exhibit?

A. To route packets directly from VPC B to VPC C through VPC A, you must add a route for network 192.168.0.0/16 in the VPC A routing table.

B. You cannot route packets directly from VPC B to VPC C through VPC A.

C. You can associate VPC ID pcx-23232323 with VPC B to form a VPC peering connection between VPC B and VPC C.

D. You cannot create a separate VPC peering connection between VPC B and VPC C to route packets directly.

Suggested Answer: *B*

Community vote distribution

B (100%)

havokdu 1 month, 2 weeks ago

Selected Answer: B

Because VPC peering doesn't support transitivity.

upvoted 1 times

the_giant 6 months ago

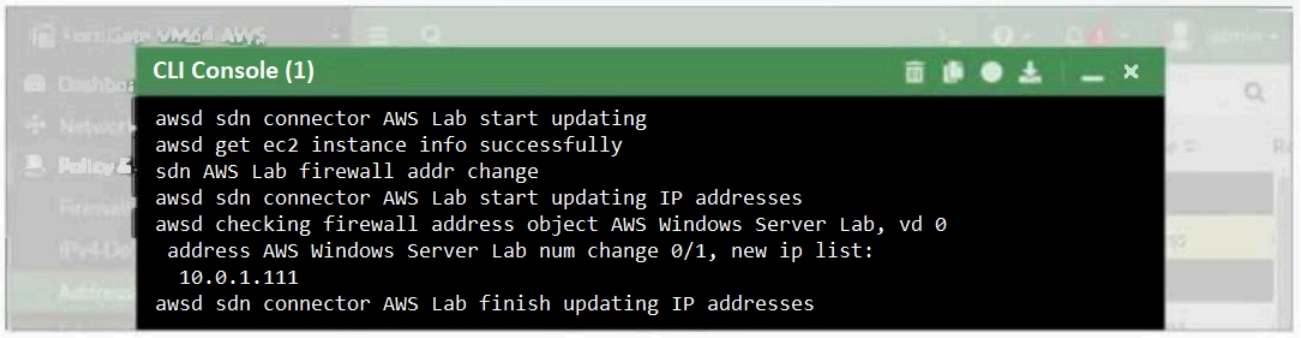
Selected Answer: B

B is correct

upvoted 2 times

Question #12 *Topic 1*

Refer to the exhibit.



What two conclusions can you draw from the FortiGate debug output? (Choose two.)

A. The dynamic address object is automatically updated if the IP changes.

B. The address object AWS Windows Server Lab can be manually changed on FortiGate.

C. The SDN connector is correctly configured and authorized.

D. The AWS user account used for software-defined network (SDN) integration must have full administrative rights.

Suggested Answer: *AC*

Community vote distribution

AC (100%)

myrmidon3 3 months, 2 weeks ago

Selected Answer: AC

A. The dynamic address object is automatically updated if the IP changes.
The output shows that the SDN connector starts updating IP addresses and successfully updates the dynamic address object (AWS Windows Server Lab). This indicates that the IP address (10.0.1.111) is dynamically updated, reflecting any changes.
C. The SDN connector is correctly configured and authorized.
The output shows successful steps in retrieving instance information (get ec2 instance info successfully) and updating IP addresses, indicating that the SDN connector is correctly configured and authorized for integration with AWS.

Options B and D are incorrect because:
B suggests manual changes, but the output refers to automatic updates through the SDN connector.
D is not directly supported by the debug, as it doesn't mention the AWS account's specific permissions or roles required beyond what's already configured for SDN integration.

upvoted 1 times

the_giant 6 months ago

Selected Answer: AC

A,C is correct

upvoted 1 times

Question #13 *Topic 1*

Which three statements are correct about VPC flow logs? (Choose three.)

A. Flow logs do not capture traffic to and from 169.254.169.254 for instance metadata.

B. Flow logs do not capture DHCP traffic.

C. Flow logs can capture traffic to the reserved IP address for the default VPC router.

D. Flow logs can be used as a security tool to monitor the traffic that is reaching the instance.

E. Flow logs can capture real-time log streams for the network interfaces.

Suggested Answer: *ABD*

Community vote distribution

ABD (100%)

myrmidon3 3 months, 2 weeks ago

Selected Answer: ABD

a. Flow logs do not capture traffic to and from 169.254.169.254 for instance metadata.

VPC flow logs do not capture metadata traffic to the instance metadata IP address (169.254.169.254), which is used for instance metadata queries.

b. Flow logs do not capture DHCP traffic.

DHCP traffic is not captured by VPC flow logs, as they exclude certain types of traffic such as DHCP and traffic to the Amazon DNS server.

d. Flow logs can be used as a security tool to monitor the traffic that is reaching the instance.

VPC flow logs are useful for security monitoring, allowing administrators to see accepted and rejected traffic at the instance level and diagnose potential security issues.

The other options are incorrect:

c. VPC flow logs do not capture traffic to the reserved IP address of the default VPC router.
e. Flow logs do not capture real-time log streams. Instead, they capture data asynchronously, which may not be in real-time.

upvoted 1 times

Spawni81 5 months, 3 weeks ago

Correct - Study Guide 7.4 Page 70

upvoted 2 times

the_giant 6 months ago

Selected Answer: ABD

A, B, D should be correct

upvoted 2 times

Question #14 *Topic 1*

An administrator is adding a web application to be protected by FortiWeb Cloud.
Which two steps are necessary to successfully onboard the application? (Choose two.)

A. Wait for the EC2 instance to be created.

B. Provide a web application name.

C. Create DNS records in the domain server that hosts the application.

D. Enable a content delivery network (CDN) in the same region where your application is located.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

myrmidon3 3 months, 2 weeks ago

Selected Answer: BC

B. Provide a web application name.

When adding a new application to be protected, you need to specify the name of the web application in the FortiWeb Cloud console.

C. Create DNS records in the domain server that hosts the application.

You must update the DNS records to ensure traffic is routed through FortiWeb Cloud for protection before it reaches the web application.

The other options are not required:

A: Waiting for an EC2 instance creation is not relevant to FortiWeb Cloud onboarding since FortiWeb Cloud is a SaaS-based WAF and does not require EC2 instances in the onboarding process.
D: Enabling a CDN is optional and not required for successfully onboarding an application in FortiWeb Cloud.

upvoted 2 times

e5c20bb 5 months, 2 weeks ago

Correct P.117

upvoted 2 times

the_giant 6 months ago

Selected Answer: BC

B,C should be correct

upvoted 2 times

Question #15 *Topic 1*

An administrator must deploy a web application firewall (WAF) solution to protect the web applications of their organization.
Why would the administrator choose FortiWeb Cloud over AWS WAF with Fortinet managed rules?

A. WAF signatures must be manually updated by FortiGuard.

B. The solution must meet PCI 6.6 compliance.

C. SSL inspection is a requirement.

D. Traffic must be inspected for malware.

Suggested Answer: *B*

Community vote distribution

C (100%)

havokdu 1 month, 2 weeks ago

Selected Answer: D

Study guide page 111
Both Fortiweb cloud and AWS WAF with Fortinet managed rules supports "Meet PCI 6.6 compliance" and "SSL inspection".

There is no malware protection in AWS WAF partner rules because there is no engine to protect malware. FortiWeb Cloud, on the other hand, extends beyond signature-based web protection and can inspect the traffic for malware.

upvoted 2 times

myrmidon3 3 months, 2 weeks ago

Selected Answer: C

C. SSL inspection is a requirement.

FortiWeb Cloud offers SSL inspection capabilities, allowing it to inspect encrypted traffic (HTTPS) and provide deeper protection for web applications. If SSL inspection is a key requirement, FortiWeb Cloud would be preferred over AWS WAF with Fortinet managed rules, as AWS WAF does not natively support SSL decryption and inspection without additional configuration.

Here's why the other options are less relevant:

A: WAF signatures are automatically updated by FortiGuard, so manual updates are not required for either solution.
B: Both FortiWeb Cloud and AWS WAF with Fortinet managed rules can help meet PCI 6.6 compliance.
D: Traffic inspection for malware is typically handled by a security solution beyond just WAF functionality. FortiWeb Cloud provides more advanced protection, but malware inspection is not the primary factor in this comparison.

upvoted 2 times

e5c20bb 5 months, 2 weeks ago

D. Both offer SSL inspection.

upvoted 1 times

Spawni81 5 months, 3 weeks ago

D should be correct. WAF & Forti can do Web Attack Signatures, PCI 6.6 Comp. and SSL Inspection. Study Guide 7.4 Page 11 -> WAF cannot do Antivirus/Antimalware, while FortiWeb can.

upvoted 2 times

yakisiklisubay 5 months, 3 weeks ago

Should be C

upvoted 1 times

the_giant 6 months ago

Selected Answer: C

C should be correct

upvoted 1 times

sclu650 7 months, 3 weeks ago

Explanation:

SSL inspection is a requirement:

Correct: FortiWeb Cloud provides advanced SSL inspection capabilities, which allow it to decrypt and inspect SSL/TLS traffic to detect threats hidden in encrypted traffic. AWS WAF, on the other hand, typically requires additional configuration or integration with other services to handle SSL inspection effectively.

upvoted 1 times

sclu650 7 months, 3 weeks ago

this answer is SSL inspection, as both options offer PCI 6.6. Compliance.

upvoted 1 times

Question #16 *Topic 1*

A customer is attempting to deploy an active-passive high availability (HA) cluster using the software-defined network (SDN) connector in the AWS cloud.
What is an important consideration to ensure a successful formation of HA, failover, and traffic flow?

A. Both cluster members must be in the same availability zone.

B. VDOM exceptions must be configured.

C. Unicast FortiGate Clustering Protocol (FGCP) must be used.

D. Both cluster members must show as healthy in the elastic load balancer (ELB) configuration.

Suggested Answer: *C*

Community vote distribution

C (100%)

havokdu 1 month, 2 weeks ago

Selected Answer: C

Unicast FortiGate Clustering Protocol (FGCP) must be used.

upvoted 1 times

havokdu 1 month, 2 weeks ago

B. VDOM exceptions must be configured is also right

upvoted 1 times

myrmidon3 3 months, 2 weeks ago

Selected Answer: C

C. Unicast FortiGate Clustering Protocol (FGCP) must be used.

When deploying an active-passive high availability (HA) cluster in AWS, it is important to use Unicast FGCP, which is specifically designed for cloud environments like AWS. FGCP manages the heartbeat communication between FortiGate instances in the cluster and ensures proper failover mechanisms are in place.

Here's why the other options are less relevant:

A: Both cluster members do not need to be in the same availability zone; in fact, deploying in different AZs is typically recommended for redundancy.
B: VDOM exceptions are not specifically required for HA deployment or traffic flow.
D: While health checks are important in general, FortiGate HA clusters do not rely on the Elastic Load Balancer (ELB) for managing failovers, as FGCP handles this internally.

upvoted 2 times

Spawni81 5 months, 3 weeks ago

C is correct. Study Guide 7.4 Page 128

upvoted 3 times

the_giant 6 months ago

Selected Answer: C

C is correct

upvoted 1 times

Question #17 *Topic 1*

A cloud administrator is tasked with protecting web applications hosted in AWS cloud.
Which three Fortinet cloud offerings can the administrator choose from to accomplish the task? (Choose three.)

A. AWS WAF

B. FortiEDR

C. FortiGate Cloud-Native Firewall (CNF)

D. Fortinet Managed Rules for AWS WAF

E. FortiWeb Cloud

Suggested Answer: *CDE*

Community vote distribution

CDE (100%)

havokdu 1 month, 2 weeks ago

Selected Answer: CDE

Not Selected:

AWS WAF: While AWS WAF is a web application firewall, it is an AWS-native service, not a Fortinet offering.

upvoted 1 times

the_giant 6 months ago

Selected Answer: CDE

C, D, E is correct

upvoted 1 times

Question #18 *Topic 1*

Refer to the exhibit.

FortiGate debug output

```
FortiGate-VM64-AWS # diagnose debug enable

FortiGate-VM64-AWS # diagnose debug application awsd -1
Debug messages will be on for 24 minutes.

FortiGate-VM64-AWS # awsd sd connector AWS Lab prepare to update
awsd sdn connector AWS Lab start updating
aws curl response err, 401
<?xml version="1.0" encoding="UTF-8"?>
<Response><Errors><Error><Code>AuthFailure</Code><Message>AWS was not able to validate
the provided access credentials</Message></Error></Errors><RequestID>b3c08dfe-8
97d-4307-b039-ece48519f1b8</RequestID></Response>
aws access/secret key invalid
awsd sdn connector AWS Lab failed to get instance list
awsd reap child pid: 14257
sdn AWS Lab firewall addr change
awsd sdn connector AWS Lab prepare to update
awsd sdn connector AWS Lab start updating
aws curl response err, 401
<?xml version="1.0" encoding="UTF-8"?>
<Response><Errors><Error><Code>AuthFailure</Code><Message>AWS was not able to validate
the provided access credentials</Message></Error></Errors><RequestID>befa40a0-
17d-4819-a281-5daa7dd63a7c</RequestID></Response>
aws access/secret key invalid
awsd sdn connector AWS Lab failed to get instance list
awsd reap child pid: 14259
sdn AWS Lab firewall addr change
awsd sdn connector AWS Lab prepare to update
awsd sdn connector AWS Lab start updating
aws curl response err, 401
<?xml version="1.0" encoding= "UTF-8"?>
<Response><Errors><Error><Code>AuthFailure</Code><Message>AWS was not able to validate
the provided access credentials</Message></Error></Errors><RequestID>8e82eecd-
290-4e05-8c6b-85e7004ee48a</RequestID></Response>
aws access/secret key invalid
awsd sdn connector AWS Lab failed to get instance list
awsd reap child pid: 14262
```

An administrator configured a FortiGate device to connect to the AWS API to retrieve resource values from the AWS console to create dynamic objects for the FortiGate policies. The administrator is unable to retrieve AWS dynamic objects on FortiGate.
Which two reasons can explain why? (Choose two.)

A. The AWS API call is not supported on XML version 1.0.

B. AWS was not able to validate credentials provided by the AWS Lab SDN connector because of a clock skew between FortiGate and AWS.

C. The AWS Lab SDN connector is configured with an invalid AWS access or secret key.

D. The AWS Lab SDN connector failed to connect on port 401.

E. The AWS Lab SDN did not find any instances in the configured VPC.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

myrmidon3 3 months, 2 weeks ago

Selected Answer: BC

B. AWS was not able to validate credentials provided by the AWS Lab SDN connector because of a clock skew between FortiGate and AWS.

The 401 error code with the message "AWS was not able to validate the provided access credentials" could be related to time synchronization issues (clock skew), which is a common issue when using API calls with AWS.

C. The AWS Lab SDN connector is configured with an invalid AWS access or secret key.

The error message explicitly mentions "aws access/secret key invalid," which directly points to invalid credentials being used by the AWS Lab

SDN connector.

Both of these reasons align with the error messages observed in the debug output.

upvoted 3 times

the_giant 6 months ago

Selected Answer: BC

B,C is correct

upvoted 1 times