Fortinet

Exam Questions NSE5_SSE_AD-7.6

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Which statement about security posture tags in FortiSASE is correct?

A. Multiple tags can be assigned to an endpoint, but only one is used for evaluation.
B. Multiple tags can be assigned to an endpoint and used for evaluation.
C. Tags are static and do not change with endpoint status.
D. Only one tag can be assigned to an endpoint.

Answer: B

NEW QUESTION 2
A FortiGate device is in production. To optimize WAN link use and improve redundancy, you enable and configure SD-WAN.
What must you do as part of this configuration update process? (Choose one answer)

A. Replace references to interfaces used as SD-WAN members in the firewall policies.
B. Replace references to interfaces used as SD-WAN members in the routing configuration.
C. Disable the interface that you want to use as an SD-WAN member.
D. Purchase and install the SD-WAN license, and reboot the FortiGate device.

Answer: A

NEW QUESTION 3
You are configuring SD-WAN to load balance network traffic. Which two facts should you consider when setting up SD-WAN? (Choose two.)

A. When applicable, FortiGate load balances traffic through all members that meet the SLA target.
B. SD-WAN load balancing is possible only when using the manual and the best quality strategies.
C. Only the manual and lowest cost (SLA) strategies allow SD-WAN load balancing.
D. You can select the outsessions hash mode with all strategies that allow load balancing.

Answer: AD

NEW QUESTION 4
How is the Geofencing feature used in FortiSASE? (Choose one answer)

A. To allow or block remote user connections to FortiSASE POPs from specific countries.
B. To restrict access to applications based on the time of day in specific countries.
C. To encrypt data at rest on mobile devices in specific countries.
D. To monitor user behavior on websites and block non-work-related content from specific countries

Answer: A

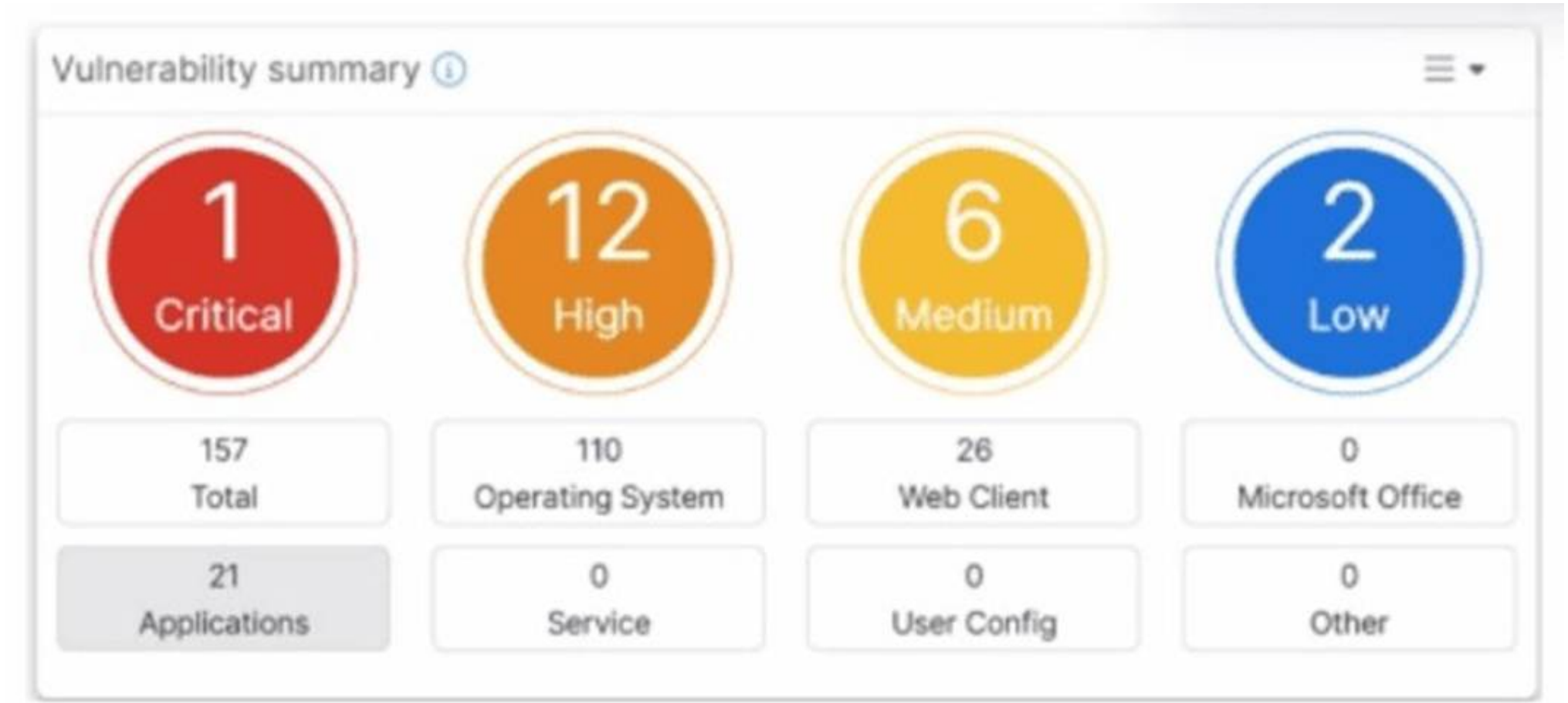
Explanation:
According to theFortiSASE 7.6 Administration Guideand theFCP - FortiSASE 24/25 Administratorstudy materials, theGeofencingfeature is a security measure implemented at the edge of the FortiSASE cloud to control ingress connectivity based on the physical location of the user.
Access Control by Location (Option A): Geofencing allows administrators toallow or block remote user connectionsto the FortiSASE Points of Presence (PoPs) based on the source country, region, or specific network infrastructure (e.g., AWS, Azure, GCP).
Scope of Application: This feature is universal across all SASE connectivity methods. It applies toAgent-based users(FortiClient),Agentless users(SWG/PAC file), andEdge devices(FortiExtender/FortiAP). If a user attempts to connect from a blacklisted country, the connection is dropped at the PoP level before the user can even attempt to authenticate.
Use Case Example: An organization operating exclusively in North America might configure geofencing toblock all connections originating from outside the US and Canada. This significantly reduces the attack surface by preventing brute-force or unauthorized access attempts from high-risk regions or countries where the organization has no legitimate employees.
Configuration Path: In the FortiSASE portal, this is managed underConfiguration>Geofencing. From there, administrators can create an "Allow" or "Deny" list and select the relevant countries from a standardized global database.
Why other options are incorrect:
Option B: While FortiSASE supportsTime-based schedulesfor firewall policies, geofencing is specifically an IP-to-Geography mapping tool for connection admission, not a time-of-day restriction tool.
Option C: Encryption of data at rest on mobile devices is a function of anMDM (Mobile Device Management)solution or local OS features (like FileVault or BitLocker), not a SASE network geofencing feature.
Option D: Monitoring web behavior and blocking non-work content is the role of theWeb FilterandApplication Controlprofiles, which operate on the trafficafterthe connection is allowed by geofencing.

NEW QUESTION 5
What is a key use case for FortiSASE Secure Internet Access (SIA) in an agentless deployment? (Choose one answer)

A. It provides secure web browsing by isolating browser sessions and enforcing data loss prevention for temporary employees.
B. It acts as a secure web gateway (SWG) distributing a PAC file for explicit web proxy use, securing HTTP and HTTPS traffic with a full security stack, and is ideal for unmanaged endpoints like contractors.
C. It distributes a PAC file to secure non-web traffic protocols and applies antivirus protection only for managed endpoints.
D. It requires FortiClient endpoints and supports ZTNA tags to secure all network traffic for unmanaged endpoints.

Answer: B

NEW QUESTION 6
Refer to the exhibit.



Which two statements about the Vulnerability summary dashboard in FortiSASE are correct? (Choose two.)

A. The dashboard shows the vulnerability score for unknown applications.
B. Vulnerability scan is disabled in the endpoint profile.
C. The dashboard allows the administrator to drill down and view CVE data and severity classifications.
D. Automatic vulnerability patching can be enabled for supported applications.

Answer: CD

NEW QUESTION 7
Which three FortiSASE use cases are possible? (Choose three answers)

A. Secure Internet Access (SIA)
B. Secure SaaS Access (SSA)
C. Secure Private Access (SPA)
D. Secure VPN Access (SVA)
E. Secure Browser Access (SBA)

Answer: ABC

NEW QUESTION 8
You have configured the performance SLA with the probe mode as Prefer Passive. What are two observable impacts of this configuration? (Choose two.)

A. FortiGate can offload the traffic that is subject to passive monitoring to hardware.
B. FortiGate passively monitors the member if ICMP traffic is passing through the member.
C. During passive monitoring, the SLA performance rule cannot detect dead members.
D. After FortiGate switches to active mode, the SLA performance rule falls back to passive monitoring after 3 minutes.
E. FortiGate passively monitors the member if TCP traffic is passing through the member.

Answer: CE

NEW QUESTION 9
An existing Fortinet SD-WAN customer who has recently deployed FortiSASE wants to have a comprehensive view of, and combined reports for, both SD-WAN branches and remote users. How can the customer achieve this?

A. Forward the logs from FortiSASE to Fortinet SOCaaS.
B. Forward the logs from FortiGate to FortiSASE.
C. Forward the logs from FortiSASE to the external FortiAnalyzer.
D. Forward the logs from the external SD-WAN FortiAnalyzer to FortiSASE.

Answer: C

NEW QUESTION 10
You want FortiGate to use SD-WAN rules to steer ping local-out traffic. Which two constraints should you consider? (Choose two.)

A. You must configure each local-out feature individually to use SD-WAN.
B. By default, FortiGate uses SD-WAN rules only for local-out traffic that corresponds to ping and traceroute.
C. You can steer local-out traffic only with SD-WAN rules that use the manual strategy.
D. By default, FortiGate uses SD-WAN rules only for local-out traffic that corresponds to ping and traceroute.

Answer: AB

NEW QUESTION 10
Which configuration is a valid use case for FortiSASE features in supporting remote users?

A. Enabling secure SaaS access through SD-WAN integration, protecting against web- based threats with data loss prevention, and monitoring user connectivity with shadow IT visibility.
B. Monitoring SaaS application performance, isolating browser sessions for all websites, and integrating with SD-WAN for data loss prevention.
C. Enabling secure web browsing to protect against threats, providing explicit application access with zero-trust or SD-WAN integration, and addressing shadow IT visibility with data loss prevention.
D. Providing secure web browsing through remote browser isolation, addressing shadow IT with zero-trust access, and protecting data at rest only.

Answer: C

NEW QUESTION 13
Refer to the exhibit

Diagnose output

```
fgt_A # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(8), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x0), gid(0), cfg_order(2), local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


fgt_A # diagnose sys sdwan member | grep HUB1
Member(4): transport-group: 0, interface: HUB1-VPN1, flags=0xd  may_child, gateway: 100.64.1.1,
peer: 192.168.1.29, source 192.168.1.1, priority: 15 1024, weight: 0
Member(5): transport-group: 0, interface: HUB1-VPN2, flags=0xd  may_child, gateway: 100.64.1.9,
peer: 192.168.1.61, source 192.168.1.33, priority: 10 1024, weight: 0
Member(6): transport-group: 0, interface: HUB1-VPN3, flags=0xd  may_child, gateway: 172.16.1.5,
peer: 192.168.1.93, source 192.168.1.65, priority: 1 1024, weight: 0


fgt_A # get router info routing-table all | grep HUB1
S       10.0.0.0/8 [10/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
B       10.0.3.0/24 [200/0] via 192.168.1.2 [3] (recursive is directly connected, HUB1-VPN1), 04:11:41, [1/0]
                    [200/0] via 192.168.1.34 [3] (recursive is directly connected, HUB1-VPN2), 04:11:41, [1/0]
B       10.1.0.0/24 [200/0] via 192.168.1.29 (recursive via HUB1-VPN1 tunnel 100.64.1.1), 04:11:42, [1/0]
                    [200/0] via 192.168.1.61 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 04:11:42, [1/0]
                    [200/0] via 192.168.1.93 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 04:11:42, [1/0]
```

An administrator is troubleshooting SD-WAN on FortiGate. A device behind branch1_fgt generates traffic to the 10.0.0.0/8 network. The administrator expects the traffic to match SD-WAN rule ID 1 and be routed over HUB1-VPN1. However, the traffic is routed over HUB1-VPN3.
Based on the output shown in the exhibit, which two reasons, individually or together, could explain the observed behavior? (Choose two.)

A. HUB1-VPN1 does not have a valid route to the destination.
B. HUB1-VPN3 has a higher member configuration priority than HUB1-VPN1.
C. HUB1-VPN3 has a lower route priority value (higher priority) than HUB1-VPN1.
D. The traffic matches a regular policy route configured with HUB1-VPN3 as the outgoing device.

Answer: AC

NEW QUESTION 14
Which three authentication sources support secure identity verification and access control for FortiSASE remote users? (Choose three.)

A. Security Assertion Markup Language (SAML)
B. OpenID Conned (OIDC)
C. Lightweight Directory Access Protocol (LDAP)
D. Terminal Access Controller Access-Control System Plus (TACACS+)
E. Remote Authentication Dial-in User Service (RADIUS)

Answer: ACE

NEW QUESTION 18
Which two statements about configuring a steering bypass destination in FortiSASE are correct? (Choose two.)

A. Subnet is the only destination type that supports the Apply condition

B. Apply condition allows split tunneling destinations to ae applied to On-ne
C. off-ne
D. or both types of endpoints
E. You can select from four destination types: Infrastructure, FQDN, Local Application, or Subnet
F. Apply condition can be set only to On-net or Off-ne
G. but not both

Answer: BC

Explanation:
According to theFortiSASE 7.6 Feature Administration Guide, steering bypass destinations (also known as split tunneling) allow administrators to optimize bandwidth by redirecting specific trusted traffic away from the SASE tunnel to the endpoint's local physical interface.
Destination Types (Option C): When creating a bypass destination, administrators can select from four distinct types:Infrastructure(pre-defined apps like Zoom/O365),FQDN(specific domains),Local Application(identifying processes on the laptop), orSubnet(specific IP ranges).
Apply Condition (Option B): The "Apply" condition is a flexible setting that allows the administrator to choose when the bypass is active. It can be applied to endpoints that areOn-net(inside the office),Off-net(remote), orBoth. This ensures that if a user is in the office, they don't use the SASE tunnel for local resources, but if they are home, they might still bypass high-bandwidth sites like YouTube to preserve tunnel capacity.
Why other options are incorrect:
Option A: Subnet is one of four types and is not the only type supporting these conditions.
Option D: The system explicitly supports "Both" to ensure consistency across network transitions.

NEW QUESTION 20
Which two delivery methods are used for installing FortiClient on a user's laptop? (Choose two.)

A. Use zero-touch installation through a third-party application store.
B. Download the installer directly from the FortiSASE portal.
C. Send an invitation email to selected users containing links to FortiClient installers.
D. Configure automatic installation through an API to the user's laptop.

Answer: BC

NEW QUESTION 23
Which three factors about SLA targets and SD-WAN rules should you consider when configuring SD-WAN rules? (Choose three answers)

A. When configuring an SD-WAN rule, you can select multiple SLA targets from different performance SLAs.
B. SLA targets are used only by SD-WAN rules that are configured with a Lowest Cost (SLA) strategy.
C. Member metrics are measured only if a rule uses the SLA target.
D. SD-WAN rules can use SLA targets to check whether the preferred members meet the SLA requirements.
E. When configuring an SD-WAN rule, you can select multiple SLA targets if they are from the same performance SLA.

Answer: BDE

NEW QUESTION 25
Which three reports are valid report types in FortiSASE? (Choose three.)

A. Web Usage Summary Report
B. Endpoint Compliance Deviation Report
C. Vulnerability Assessment Report
D. Shadow IT Report
E. Cyber Threat Assessment

Answer: ACD

NEW QUESTION 30
.....

Relate Links

100% Pass Your NSE5_SSE_AD-7.6 Exam with Exambible Prep Materials

https://www.exambible.com/NSE5_SSE_AD-7.6-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/