Fortinet.NSE5_SSE_AD-7.6.v2026-06-13.q17

Exam Code:	NSE5_SSE_AD-7.6
Exam Name:	Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator
Certification Provider:	Fortinet
Free Question Number:	17
Version:	v2026-06-13
# of views:	103
# of Questions views:	170
https://www.freecram.net/torrent/Fortinet.NSE5_SSE_AD-7.6.v2026-06-13.q17.html	

NEW QUESTION: 1
What is the purpose of the on/off-net rule setting in FortiSASE?
A. To enable or disable user authentication for external network access.
B. To define different traffic routing rules for on-premises and cloud-based resources.
C. To determine if an endpoint is connecting from a trusted network or untrusted location.
D. To configure different access policies for users based on their geographical location.
Answer: (SHOW ANSWER)
According to theFortiSASE 24.4 Administration Guideand theFortiSASE Core Administratortraining materials, theOn-net detectionrule setting is a critical component for determining the "trust status" of an endpoint's physical location.
* Endpoint Location Verification: On-net rule sets are used to determine if FortiSASE considers an endpoint to beon-net(trusted) oroff-net(untrusted). An endpoint is considered on-net when it is physically located within the corporate network, which is assumed to already have on-premises security measures (like a FortiGate NGFW).
* Operational Impact: When an endpoint is detected as on-net, FortiSASE can be configured toexempt the endpoint from automatically establishing a VPN tunnel to the SASE cloud. This optimization prevents redundant security inspection and conserves SASE bandwidth since the user is already protected by the local corporate firewall.
* Detection Methods: To classify an endpoint as on-net, administrators configure rule sets that look for specific environmental markers, such as:
* Known Public (WAN) IP: If the endpoint's public IP matches the corporate headquarters' egress IP.
* DHCP Server: If the endpoint receives an IP from a specific corporate DHCP server.
* DNS Server/Subnet: Matching internal DNS infrastructure or specific internal IP ranges.
* Dynamic Policy Application: By accurately determining if an endpoint is on or off-net, FortiSASE ensures that theFortiClientagent only initiates its secure internet access (SIA) tunnel when the user is in an untrusted location (e.g., a home network or public Wi-Fi).
Why other options are incorrect:
* Option A: User authentication is a separate process and is not controlled by the on/off-net detection rules, which focus on the network environment rather than user credentials.
* Option B: While on-net status affectshowtraffic is routed (VPN vs. local), these rules specifically determine the statusitself rather than defining the routing tables for private vs. cloud resources.

* Option D: Geographical location (Geo-location) is a different filtering criterion often used in firewall policies; on-net detection is specifically about the proximity to the trusted corporate perimeter.

NEW QUESTION: 2
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: (SHOW ANSWER)
For customers with hybrid environments (on-premises SD-WAN branches and remote FortiSASE users), the FortiOS 7.6andFortiSASEcurriculum recommends centralized log aggregation for unified visibility.
* Centralized Reporting:The standard architectural best practice is toforward logs from FortiSASE to an external FortiAnalyzer (Option C).
* Unified View:Since the customer's on-premises FortiGate SD-WAN branches are already sending logs to an existing FortiAnalyzer, adding the FortiSASE log stream to that sameFortiAnalyzerallows for the creation ofcombined reports.
* Fabric Integration:This setup leverages theSecurity Fabric, enabling the FortiAnalyzer to provide a single pane of glass for monitoring security events, application usage, and SD-WAN performance metrics across the entire distributed network.
Why other options are incorrect:
* Option A:SOCaaSis a managed service for threat monitoring, not a primary tool for an administrator to generate combined SD-WAN/SASE operational reports.
* Option B:FortiSASE is not designed to act as a log collector or reporting hub for external on-premises FortiGates.
* Option D:Data flows from the source (FortiSASE) to the collector (FortiAnalyzer), not the other way around.

NEW QUESTION: 3
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: (SHOW ANSWER)
According to theFortiSASE 7.6 Administration Guideand theFCP - FortiSASE 24/25 Administrator curriculum, the Agentless deployment mode- commonly referred to asSecure Web Gateway (SWG)mode- is a vital component of the Secure Internet Access (SIA) framework.
* Deployment Mechanism: In an agentless deployment, FortiSASE functions as an explicit web proxy.
This is achieved by distributing aPAC (Proxy Auto-Configuration) fileto the user's browser, which instructs the device to send its web traffic to the nearest FortiSASE Point of Presence (PoP).
* Target Use Case: This mode is specifically designed forunmanaged endpoints, such as those used by contractors, partners, or temporary workers, where the organization does not have the authority or capability to install the FortiClient agent.
* Security Capabilities: Even without an agent, FortiSASE applies afull security stackto the redirected traffic. This includesWeb Filtering,Anti-Malware,SSL Inspection, andInline-CASBto secure HTTP and HTTPS sessions.

* Protocol Limitations: Because it relies on proxy settings, this mode is limited to web protocols (HTTP /HTTPS) and does not inherently secure non-web traffic like ICMP, DNS, or custom TCP/UDP applications unless they are specifically proxied.
Why other options are incorrect:
* Option A: While it provides secure browsing, session isolation (RBI) is a specific feature that can be used in either mode; the defining characteristic of the agentless use case is the proxy-based redirection for unmanaged devices.
* Option C: A PAC file can only secure web traffic (protocols that support proxying), not non-web traffic protocols.
* Option D: Agentless mode is the opposite of requiring FortiClient; ZTNA tags generally require the FortiClient agent to provide the necessary telemetry for tag evaluation.

NEW QUESTION: 4
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: (SHOW ANSWER)
According to theFortiSASE 7.6 Administration GuideandFCP - FortiSASE 24/25 Administrator curriculum, security posture tags (often referred to as ZTNA tags) are the fundamental building blocks for identity-based and posture-based access control.
* Multiple Tag Assignment: A single endpoint can be assigned multiple tags at the same time. For example, an endpoint might simultaneously have the tags"OS-Windows-11","AV-Running", and
"Corporate-Domain-Joined".
* Evaluation Logic: During the policy evaluation process (for both SIA and SPA), FortiSASE or the FortiGate hub considers all tags assigned to the endpoint. Security policies can be configured to use these tags as source criteria. If an administrator defines a policy that requires both "AV-Running" and
"Corporate-Domain-Joined," the system evaluates both tags to decide whether to permit the traffic.
* Dynamic Nature: Contrary to Option C, these tags are highly dynamic. They are automatically applied or removed in real-time based on the telemetry data sent by theFortiClientto the SASE cloud. If a user disables their antivirus, the "AV-Running" tag is removed immediately, and the endpoint's access is revoked by the next policy evaluation.
* Scalability: While the system supports many tags, documentation recommends a baseline of custom tags for optimal performance, though it confirms that multiple tags are standard for reflecting a comprehensive security posture.
Why other options are incorrect:
* Option A: This is incorrect because the system does not pick just one tag; it evaluates the collection of tags against the policy's requirements (e.g., matching any or matching all).
* Option C: This is incorrect because tags are dynamic and change as soon as the endpoint's status (like vulnerability count or software presence) changes.
* Option D: This is incorrect because the architectural advantage of ZTNA is the ability to layer multiple security "checks" (tags) for a single user.

NEW QUESTION: 5
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: (SHOW ANSWER)

Based on theFortiSASE 7.6 (and later 2025 versions)curriculum and administration guides, the Vulnerability summary dashboard is a key component of the endpoint security posture management.

* Drill Down Capability (Option C): According to theFortiSASE Administration Guide, the Vulnerability summary widget on the Security dashboard is interactive. An administrator can click on specific risk categories (e.g., Critical, High) or application types (e.g., Operating System, Web Client) to drill down. This action opens a detailed pane showing the specific affected endpoints, associatedCVE identifiers, and severity classifications based on the CVSS standard.

* Automatic Vulnerability Patching (Option D): In theFortiSASE 7.6/2025feature sets, the endpoint profile configuration (underEndpoint > Configuration > Profiles) includes an "Automatic Patching" section. This feature allows the system to automatically install security updates for supported third- party applications and the underlying operating system (Windows/macOS) when vulnerabilities are detected. Furthermore, administrators can schedule these patches directly from theVulnerability Summarywidget by selecting specific vulnerabilities.

Why other options are incorrect:

* Option A: The dashboard categories (Operating System, Web Client, Microsoft Office, etc.) are based on known software signatures. While there is an "Other" category, the dashboard primarily provides scores for recognized applications where CVE data is available.

* Option B: The exhibit shows active data (157 total vulnerabilities), which indicates that the vulnerability scan is enabledand currently reporting data from the endpoints. If it were disabled, the widget would be empty or show zeros.

NEW QUESTION: 6

How does the FortiSASE security dashboard facilitate vulnerability management for FortiClient endpoints?

(Choose one answer)

A. It automatically patches all vulnerabilities without user intervention and does not categorize vulnerabilities by severity.

B. It shows vulnerabilities only for applications and requires endpoint users to manually check for affected endpoints.

C. It displays only critical vulnerabilities, requires manual patching for all endpoints, and does not allow viewing of affected endpoints.

D. It provides a vulnerability summary, identifies affected endpoints, and supports automatic patching for eligible vulnerabilities.

Answer: (SHOW ANSWER)

According to theFortiSASE 7.6 Administration Guideand theFCP - FortiSASE 24/25 Administrator training materials, the security dashboard is a centralized hub for monitoring and remediating security risks across the entire fleet of managed endpoints.
* Vulnerability Summary: The dashboard includes a dedicatedVulnerability summary widgetthat categorizes risks by severity (Critical, High, Medium, Low) and by application type (OS, Web Client, etc.).
* Identifying Affected Endpoints: The dashboard is fully interactive; an administrator candrill down into specific vulnerability categories to view a detailed list ofCVE dataand, most importantly, identify the specificaffected endpointsthat require attention.
* Automatic Patching: FortiSASE supportsautomatic patching for eligible vulnerabilities(such as common third-party applications and supported OS updates). This feature is configured within the Endpoint Profile, allowing the FortiClient agent to remediate risks without requiring the user to manually run updates.
Why other options are incorrect:
* Option A: While it supports automatic patching, it does not do so forallvulnerabilities (only eligible
/supported ones), and it specificallydoescategorize them by severity.
* Option B: The dashboard shows vulnerabilities for theOperating Systemas well as applications, and it allows theadministratorto identify affected endpoints rather than requiring the end-user to check.
* Option C: The dashboard displaysall levels of severity(not just critical) and explicitly allows the viewing of affected endpoints.

NEW QUESTION: 7
Refer to the exhibits.

SD-WAN event logs

Identity
Device ID FGVM02TM25002088
Device Name branch1_fgt
Type
Sub Type sdwan
Type event
Alerts
Action
Level notice
General
Log Description SDWAN status
Log ID 0113022923
Member 1
Message Member status changed. Member out-of-sla.
Virtual Domain root
Others
Date 2025-07-01
Date/Time 2025-07-01 05:00:25
Destination End User ID 3
Destination Endpoint ID 3
Destination Geo ID 0
Device Time 2025-07-01 05:00:25
Device Time Zone -0700
Event Time 2025-07-01 05:00:25
Event Type Health Check
Health Check Corp_HC
Log Flag 0
SLA Target ID 1

```
config service
    edit 1
        set name "Critical-DIA"
        set mode sla
        set src "LAN-net"
        set internet-service enable
        set internet-service-app-ctrl 16920 41469
        set internet-service-app-ctrl-category 28
        config sla
            edit "Corp_HC"
                set id 1
            next
        end
        set priority-members 1 2
    next
```

SD-WAN health-check configuration

```
branch1_fgt (health-check) # show
config health-check
    edit "Corp_HC"
        set server "198.18.1.1" "198.18.1.2"
        set member 1 2
        config sla
            edit 1
                set latency-threshold 150
                set jitter-threshold 50
                set packetloss-threshold 5
            next
        end
    end
```

Identity
Device ID FGVM02TM25002088
Device Name branch1_fgt
Type
Sub Type sdwan
Type event
Alerts
Action
Level notice
General
Log Description SDWAN status
Log ID 0113022923
Message Number of pass member changed.
Virtual Domain root
Others
Date 2025-07-01
Date/Time 2025-07-01 05:00:25
Destination End User ID 3
Destination Endpoint ID 3
Destination Geo ID 0
Device Time 2025-07-01 05:00:25
Device Time Zone -0700
Event Time 2025-07-01 05:00:25
Event Type Health Check
Health Check Corp_HC
Log Flag 0
New Value 1

Two SD-WAN event logs, the member status, the SD-WAN rule configuration, and the health-check configuration for a FortiGate device are shown.
Immediately after the log messages are displayed, how will the FortiGate steer the traffic based on the information shown in the exhibits? (Choose one answer)

A. FortiGate uses port1 or port2 to steer the traffic for SD-WAN rule ID 1.

B. FortiGate uses port1 to steer the traffic for SD-WAN rule ID 1.

C. FortiGate uses port2 to steer the traffic for SD-WAN rule ID 1.

D. FortiGate skips SD-WAN rule ID 1.

Answer: (SHOW ANSWER)

According to the SD-WAN 7.6 Core Administrator curriculum and the provided exhibits, the traffic steering decision is determined by the interaction between the Lowest Cost (SLA) strategy and the link health status reported in the event logs.

Rule Strategy (Lowest Cost SLA): The SD-WAN rule configuration for ID 1 (named Critical-DIA) is set to mode sla. In this mode, the FortiGate will only steer traffic through member interfaces that satisfy the assigned Performance SLA targets.

Member Preference: The rule defines priority-members 1 2. This means that under normal conditions (where both links are healthy), Member 1 (port1) is the preferred interface because it is listed first.

Event Log Analysis:

The first log message explicitly states: "Member status changed. Member out-of-sla." for Member 1. This indicates that port1 has exceeded one of the thresholds (latency, jitter, or packet loss) defined in the Corp_HC health check.

The second log confirms: "Number of pass member changed. New Value: 1, Old Value: 2". This verifies that while there were previously two links passing the SLA, now only one link (Member 2/port2) remains in a passing state.

Steering Decision: Because the rule strategy is mode sla and the primary preferred member (port1) is now out- of-sla, the FortiGate immediately disqualifies Member 1 from the selection pool for this specific rule. It then moves to the next available member in the priority list that does satisfy the SLA, which is Member 2 (port2).

Why other options are incorrect:

Option A: FortiGate will not load balance or choose between both links because port1 is currently ineligible due to the SLA failure.

Option B: Steering to port1 would violate the "Lowest Cost (SLA)" rule logic, as that link is no longer meeting the required health standards.

Option D: FortiGate does not "skip" the rule unless no members meet the SLA and there is no fallback configured; in this scenario, port2 is still passing and available.

NEW QUESTION: 8

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

A. To restrict access to applications based on the time of day in specific countries.

B. To allow or block remote user connections to FortiSASE POPs from 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: (SHOW ANSWER)

NEW QUESTION: 9

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 (LEAVE A REPLY)
According to theSD-WAN 7.6 Core Administratorstudy guide and theFortiOS 7.6 Administration Guide, when you are migrating a production FortiGate to use SD-WAN, the most critical step involves reconfiguring how traffic is permitted and routed.
* Reference Removal Requirement: Before an interface (such as wan1 or wan2) can be added as anSD- WAN member, it must be "unreferenced" in most parts of the FortiGate configuration. Specifically, if an interface is currently being used in an activeFirewall Policy, the system will prevent you from adding it to the SD-WAN bundle.
* Firewall Policy Migration (Option A): In a production environment, you mustreplace the references to the physical interfacesin your firewall policies with the newSD-WAN virtual interface(or an SD- WAN Zone). For example, if your previous policy allowed traffic from internal to wan1, you must update that policy so theOutgoing Interfaceis now SD-WAN. This allows the SD-WAN engine to take over the traffic and apply its steering rules.
* Modern Tools: While this used to be a purely manual process, FortiOS 7.x includes anInterface Migration Wizard(found underNetwork > Interfaces). This tool automates the "search and replace" function, moving all existing policy and routing references from the physical port to the SD-WAN object to ensure minimal downtime.
Why other options are incorrect:
* Option B: While you do need to update your routing (e.g., creating a static route for 0.0.0.0/0 pointing to the SD-WAN interface), the curriculum specifically emphasizes the replacement of references in firewall policiesas the primary administrative hurdle, as policies are often more numerous and complex than the single static route required for SD-WAN.
* Option C: You donotneed to disable the interface. It must be up and configured, just removed from other configuration references so it can be "absorbed" into the SD-WAN bundle.
* Option D: SD-WAN is abase featureof FortiOS and doesnot require a separate licenseor a reboot to enable.

NEW QUESTION: 10
Refer to the exhibit.

Diagnose output

```
fgt_1 # diagnose  sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
 link-cost-factor(latency), link-cost-threshold(10), heath-check(Corp_HC)
  Members(2):
    1: Seq_num(2 port2 underlay), alive, latency: 0.906, selected
    2: Seq_num(1 port1 underlay), alive, latency: 1.079, selected
  Application Control(2): Microsoft.Portal(41469,0) Business(0,29)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2 underlay), alive, selected
  Application Control(2): Social.Media(0,23) General.Interest(0,12)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2 underlay), alive, selected
  Application Control(2): Social.Media(0,23) General.Interest(0,12)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(
hash-mode-round-robin)
  Members(3):
    1: Seq_num(4 HQ_T1 overlay), alive, sla(0x3), gid(0), cfg_order(0),
local cost(0), selected
    2: Seq_num(5 HQ_T2 overlay), alive, sla(0x3), gid(0), cfg_order(1),
local cost(0), selected
    3: Seq_num(6 HQ_T3 overlay), alive, sla(0x3), gid(0), cfg_order(2),
local cost(0), selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

The exhibit shows output of the command diagnose sys sdwan service collected on a FortiGate device.

The administrator wants to know through which interface FortiGate will steer traffic from local users on subnet 10.0.1.0/255.255.255.192 and with a destination of the social media application Facebook.

Based on the exhibits, which two statements are correct? (Choose two.)

A. FortiGate steers traffic for social media applications according to the service rule 2 and steers traffic through port2.

B. There is no service defined for the Facebook application, so FortiGate applies service rule 3 and directs the traffic to headquarters.

C. When FortiGate cannot recognize the application of the flow, it load balances the traffic through the tunnels HQ_T1, HQ_T2, HQ_T3.

D. When FortiGate cannot recognize the application of the flow, it steers the traffic through the preferred member of rule 3, HQ_T1.

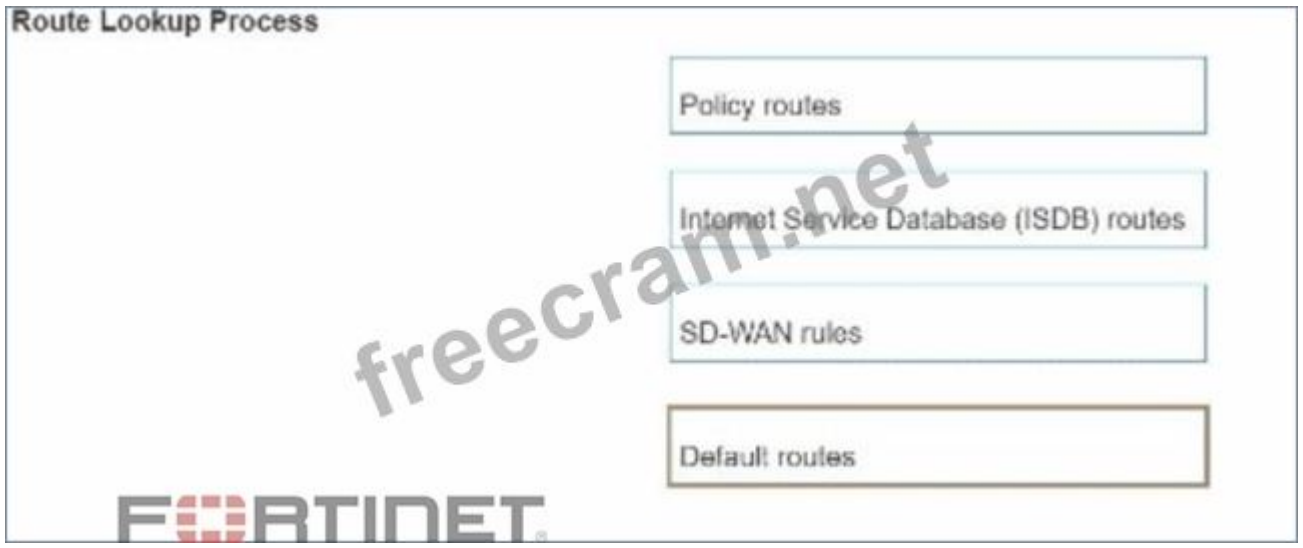
Answer: (SHOW ANSWER)

"If a flow is identified as belonging to a defined application category (such as social media), FortiGate will match it to the corresponding service rule (rule 2) and route it through the specified interface, such as port2.

However, if the application is not recognized during the session setup, the system defaults to load balancing the traffic using the available tunnels according to the policy for unclassified traffic, ensuring continuous connectivity while waiting for application classification." This guarantees both performance and resilience.

NEW QUESTION: 11
In which order does a FortiGate device consider the following elements shown in the left column during the route lookup process?
Select the element in the left column, hold and drag it to a blank position in the column on the right. Place the four correct elements in order, placing the first element in the first position at the top of the column. Once you place an element, you can move it again if you want to change your answer before moving to the next question. You need to drop four elements in the work area.
Select and drag the screen divider to change the viewable area of the source and work areas.

Answer:



NEW QUESTION: 12

Refer to the exhibit.

SD-WAN rule status and configuration

```
branch1_fgt # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(43), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
  link-cost-factor(latency), link-cost-threshold(10), heath-check(HUB1_HC)
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, latency: 96.349, selected
    2: Seq_num(5 HUB1-VPN2 HUB1), alive, latency: 141.278, selected
    3: Seq_num(6 HUB1-VPN3 HUB1), alive, latency: 190.984, selected
  Src address(1):
        10.0.1.0-10.0.1.255
  Dst address(1):
        10.0.0.0-10.255.255.255


branch1_fgt (service) # show
config service
    edit 3
        set name "Corp"
        set mode priority
        set dst "Corp-net"
        set src "LAN-net"
        set health-check "HUB1_HC"
        set priority-members 4 5 6
    next
```

The SD-WAN rule status and configuration is shown. Based on the exhibit, which change in the measured latency will first make HUB1-VPN3 the new preferred member?

A. When HUB1-VPN3 has a latency of 80 ms

B. When HUB1-VPN3 has a lower latency than HUB1-VPN1 and HUB1-VPN2

C. When HUB1-VPN1 has a latency of 200 ms

D. When HUB1-VPN3 has a latency of 90 ms

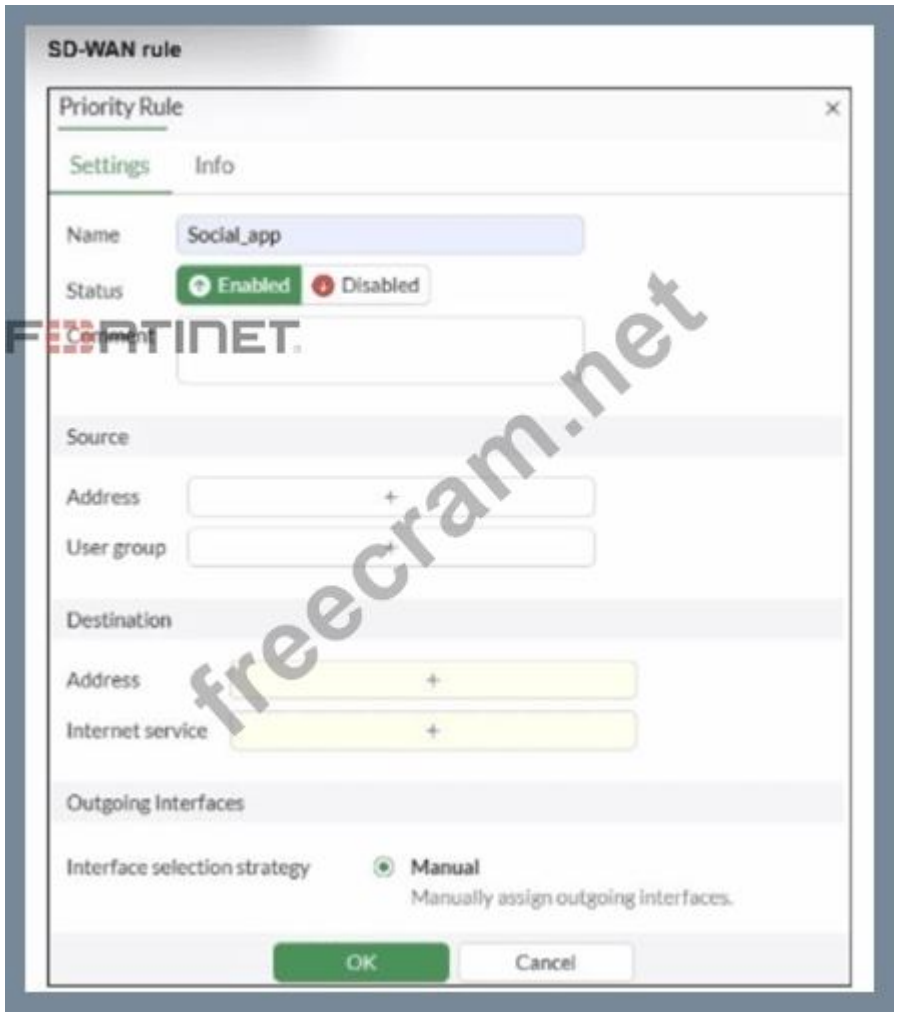
Answer: (SHOW ANSWER)

According to theSD-WAN 7.6 Core Administratorstudy guide and theFortiOS 7.6 Administration Guide, the selection of a preferred member in aBest Quality (priority)rule is determined by the measured quality metric (latency, in this case) and thelink-cost-threshold.

* Rule Logic (Best Quality): In the exhibit, the SD-WAN rule is configured with set mode priority, which corresponds to theBest Qualitystrategy. This strategy ranks members based on the link-cost- factor, which is set tolatency.
* The Link-Cost-Threshold: The exhibit shows link-cost-threshold(10), which is the default 10% value.
This threshold is designed to prevent "link flapping". To replace the current preferred member, a new member must not only have a better latency but must be better bymore than 10%.
* The Calculation:
* The current preferred member isHUB1-VPN1with a real latency of96.349 ms.
* To calculate the "target" latency a lower-priority member must achieve to take over, we use the formula: $Target = \frac{Current\_Latency}{(1 + \frac{Threshold}{100})}$.
* $\frac{96.349}{1.1} = \mathbf{87.59\text{ ms}}$.
* Evaluating Options:
* Option A (80 ms): Since 80 ms is lower than the required 87.59 ms target, HUB1-VPN3 successfully overcomes the 10% advantage of HUB1-VPN1 and becomes the new preferred member.
* Option D (90 ms): While 90 ms is lower than 96.349 ms, it isnotlower than 87.59 ms. Therefore, the 10% threshold prevents a member switch, and HUB1-VPN1 remains preferred.
* Option B: Incorrect because having a "lower" latency is not enough due to the 10% threshold.
* Option C: If HUB1-VPN1 moved to 200 ms, HUB1-VPN2 (at 141.278 ms) would likely become the new preferred member before HUB1-VPN3 (at 190.984 ms).

NEW QUESTION: 13
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-net. off-net. or both types of endpoints
C. You can select from four destination types: Infrastructure, FQDN, Local Application, or Subnet
D. Apply condition can be set only to On-net or Off-net. but not both
Answer: (SHOW ANSWER)
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: 14
Refer to the exhibit.



You configure SD-WAN on a standalone FortiGate device. You want to create an SD-WAN rule that steers traffic related to Facebook and LinkedIn through the less costly internet link. What must you do to set Facebook and LinkedIn applications as destinations from the GUI?

A. Install a license to allow applications as destinations of SD-WAN rules.

B. In the Internet service field, select Facebook and LinkedIn.

C. You cannot configure applications as destinations of an SD-WAN rule on a standalone FortiGate device.

D. Enable the visibility of the applications field as destinations of the SD-WAN rule.

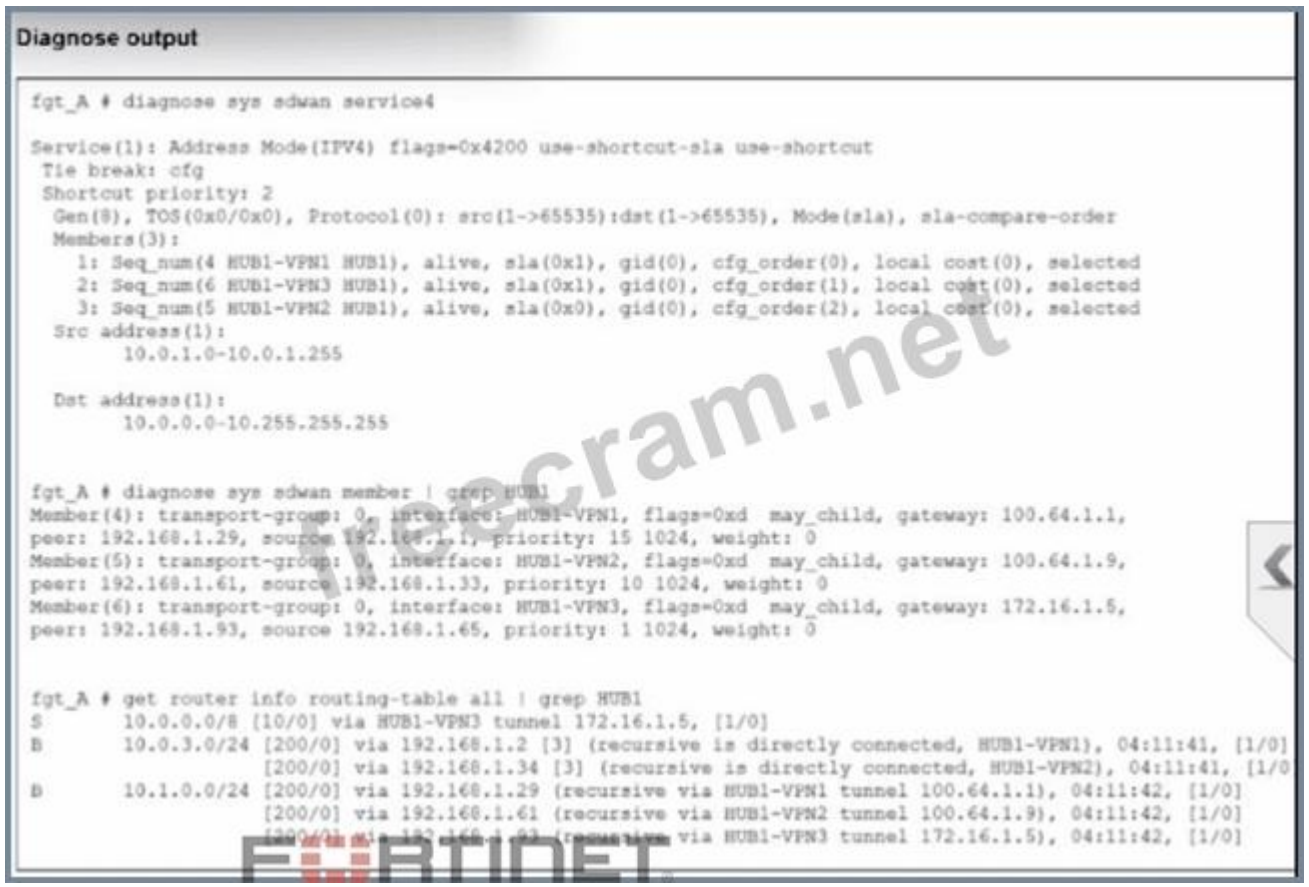
Answer: (SHOW ANSWER)

According to theSD-WAN 7.6 Core Administratorcurriculum and theFortiOS 7.6 Administration Guide, setting common web-based services like Facebook and LinkedIn as destinations in an SD-WAN rule is primarily accomplished through theInternet Service Database (ISDB).

* Internet Service vs. Application Control: In FortiOS, there is a distinction betweenInternet Services (which use a database of known IP addresses and ports to identify traffic at the first packet) and Applications(which require the IPS engine to inspect deeper into the packet flow to identify Layer 7 signatures).
* SD-WAN Efficiency: Fortinet recommends using theInternet service fieldfor services like Facebook and LinkedIn in SD-WAN rules because it allows the FortiGate to steer the traffic immediately upon the first packet. If the "Application" signatures were used instead, the first session might be misrouted because the application is not identified until after the initial handshake.
* GUI Configuration: As shown in the exhibit (image_b3a4c2.png), the "Destination" section of an SD- WAN rule includes anInternet servicefield by default. To steer Facebook and LinkedIn traffic, the administrator simply clicks the "+" icon in that field and selects the entries for Facebook and LinkedIn from the database.

* Feature Visibility (Alternative): While youcanenable a specific "Application" field inSystem > Feature Visibility(by enabling "Application Detection Based SD-WAN"), this is typically used for less common applications that do not have dedicated ISDB entries. For the specific "applications" mentioned (Facebook and LinkedIn), they are natively available in theInternet servicefield, making Option B the most direct and common implementation.
Why other options are incorrect:
* Option A: Licensing for application signatures is part of the standard FortiGuard services and is not a prerequisite specific only to "applications as destinations" in SD-WAN rules.
* Option C: Standalone FortiGate devices fully support application-based and ISDB-based steering in SD-WAN rules.
* Option D: While enabling feature visibility would add anadditionalfield for L7 applications, it is not a "must" for Facebook and LinkedIn, which are already accessible via the Internet Service field provided in the default GUI layout.

NEW QUESTION: 15



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: (SHOW ANSWER)
According to theSD-WAN 7.6 Core Administratorcurriculum and the diagnostic outputs shown in the exhibit, the reason traffic is steered toHUB1-VPN3instead of the expectedHUB1-VPN1(defined in SD-WAN rule ID 1) can be explained by two core routing principles in FortiOS:

* Valid Route Requirement (Option A): In thediagnose sys sdwan service 4output (which corresponds to Rule ID 1), it shows the rule has membersHUB1-VPN1,HUB1-VPN2, andHUB1-VPN3. A key principle of SD-WAN steering is that for a member to be "selectable" by a rule, itmust have a valid route to the destinationin the routing table (RIB/FIB). If the routing table output (the third section of the exhibit) shows a route to 10.0.0.0/8 viaHUB1-VPN3butnotthroughHUB1-VPN1, the SD-WAN engine will skip HUB1-VPN1 entirely because it is considered a "non-reachable" path for that specific destination.
* Policy Route Precedence (Option D): In the FortiOS route lookup hierarchy,Regular Policy Routes (PBR)are evaluatedbeforeSD-WAN rules. If an administrator has configured a traditional Policy Route (found underNetwork > Policy Routes) that matches traffic destined for 10.0.0.0/8 and specifiesHUB1- VPN3as the outgoing interface, the FortiGate will forward the packet based on that policy route and will never evaluate the SD-WAN rulesfor that session. This "bypass" occurs regardless of whether the SD- WAN rule would have chosen a "better" link.
Why other options are incorrect:
* Option B: While member configuration priority (cfg_order) is a tie-breaker in some strategies, the SD- WAN rule logic is only applied if the routing table allows it or if a higher-priority policy route doesn't intercept the traffic first.
* Option C: Lower route priority (which means higher preference in the RIB) affects theImplicit Rule (standard routing). However, SD-WAN rules are designed tooverrideRIB priority for matching traffic.
If HUB1-VPN1 was a valid candidate and no Policy Route existed, the SD-WAN rule would typically ignore RIB priority to enforce its own steering strategy.

NEW QUESTION: 16
Which two statements correctly describe what happens when traffic matches the implicit SD-WAN rule?
(Choose two answers)
A. Traffic is load balanced using the algorithm set for the v4-ecmp-mode setting.
B. Traffic does not match any of the entries in the policy route table.
C. FortiGate flags the session with may_dirty and vwl_default.
D. The traffic is distributed, regardless of weight, through all available static routes.
E. The session information output displays no SD-WAN service id.
Answer: (SHOW ANSWER)
According to theSD-WAN 7.6 Core Administratorstudy guide andFortiOS 7.6 Administration Guide, the
"implicit rule" is the default rule at the bottom of the SD-WAN rule list (ID 0). It is only evaluated if traffic does not match any manually configured SD-WAN rules.
* Policy Route Table Context (Option B): SD-WAN rules are technically a specialized form of policy- based routing. For a packet to match theimplicit rule, it must first pass through the routing hierarchy. If traffic matches the implicit rule, it indicates that it did not match any higher-priority user-defined SD- WAN rules or any specific entries in the manualpolicy route tablethat would have intercepted the traffic earlier.
* Session Information (Option E): When you use the CLI to inspect an active session (e.g., diagnose sys session list), the output contains a field for theSD-WAN Service ID. If traffic is steered by a user- defined rule, it displays the ID of that rule (e.g., service_id=1). However, when traffic falls through to theimplicit rule, the session information displaysno SD-WAN service ID(it often shows as 0 or is omitted), because the implicit rule does not function as a "service" in the same way user-defined rules do.
* Routing Behavior: The implicit rule follows the standard routing table (RIB/FIB) logic. It uses the priorityanddistanceof the static routes to determine the path. If multiple paths have the same distance and priority, it uses the algorithm set by v4-ecmp-mode, but this is a function of the routing engine, not the SD-WAN engine itself.
Why other options are incorrect:

* Option A: While v4-ecmp-mode (e.g., source-ip-based) is used for ECMP routing, this is part of the general FortiOS routing behavior for equal-cost paths in the FIB, whereas the implicit rule simply
"hands over" the decision to that routing table.
* Option C: When traffic matches the implicit rule, the session is actually flagged with vwl_id=0 and potentially dirty if a route change occurs, but vwl_default is not the standard flag name used in this specific context in the curriculum.
* Option D: This is incorrect because the implicit ruledoes respect weight, distance, and priorityas defined in the static routes within the routing table; it does not distribute traffic "regardless" of these values.

NEW QUESTION: 17
SD-WAN interacts with many other FortiGate features. Some of them are required to allow SD-WAN to steer the traffic.
Which three configuration elements must you configure before FortiGate can steer traffic according to SD- WAN rules? (Choose three.)
A. Firewall policies
B. Security profiles
C. Interfaces
D. Routing
E. Traffic shaping
Answer: (SHOW ANSWER)
According to theSD-WAN 7.6 Core Administratorstudy guide and theFortiOS 7.6 Administration Guide, for the FortiGate SD-WAN engine to successfully steer traffic using SD-WAN rules, three fundamental configuration components must be in place. This is because the SD-WAN rule lookup occurs only after certain initial conditions are met in the packet flow:
* Interfaces (Option C):You must first define the physical or logical interfaces (such as ISP links, LTE, or VPN tunnels) asSD-WAN members. These members are then typically grouped intoSD-WAN Zones. Without designated member interfaces, there is no "pool" of links for the SD-WAN rules to select from.
* Routing (Option D):For a packet to even be considered by the SD-WAN engine, there must be a matching route in theForwarding Information Base (FIB). Usually, this is a static route where the destination is the network you want to reach, and the gateway interface is set to theSD-WAN virtual interface(or a specific SD-WAN zone). If there is no route pointing to SD-WAN, the FortiGate will use other routing table entries (like a standard static route) and bypass the SD-WAN rule-based steering logic entirely.
* Firewall Policies (Option A):In FortiOS, no traffic is allowed to pass through the device unless a Firewall Policypermits it. To steer traffic, you must have a policy where theIncoming Interfaceis the internal network and theOutgoing Interfaceis the SD-WAN zone (or the virtual-wan-link). The SD- WAN rule selection happens during the "Dirty" session state, which requires a policy match to proceed with the session creation.
Why other options are incorrect:
* Security Profiles (Option B):While mandatory forApplication-levelsteering (to identify L7 signatures), basic SD-WAN steering based on IP addresses, ports, or ISDB objects does not require security profiles to be active.

* Traffic Shaping (Option E):This is an optimization feature used to manage bandwidth once steering is already determined; it is not a prerequisite for the steering engine itself to function.