NSE5_SSE_AD-7.6 Test Pass4sure, NSE5_SSE_AD-7.6 Exam Cram

Additionally, all operating systems also support this format. The third format is the desktop NSE5_SSE_AD-7.6 Practice Exam software. It is ideal for users who prefer offline Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) exam practice. This format is supported by Windows computers and laptops. You can easily install this software in your system to use it anytime to prepare for the examination.

Fortinet NSE5_SSE_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Rules and Routing: This section addresses configuring SD-WAN rules and routing policies to control and direct traffic flow across different links.
Topic 2	• Decentralized SD-WAN: This domain covers basic SD-WAN implementation including configuring members, zones, and performance SLAs to monitor network quality.
Topic 3	• SASE Deployment: This domain covers FortiSASE administration settings, user onboarding methods, and integration with SD-WAN infrastructure.
Topic 4	• Secure Internet Access (SIA) and Secure SaaS Access (SSA): This section focuses on implementing security profiles for content inspection and deploying compliance rules to managed endpoints.
Topic 5	• Analytics: This domain covers analyzing SD-WAN and FortiSASE logs to monitor traffic behavior, identify security threats, and generate reports.

>> NSE5_SSE_AD-7.6 Test Pass4sure <<

High Pass-Rate NSE5_SSE_AD-7.6 Test Pass4sure | Amazing Pass Rate For

NSE5_SSE_AD-7.6: Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator | Professional NSE5_SSE_AD-7.6 Exam Cram

Desktop Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) practice exam software also keeps track of the earlier attempted NSE5_SSE_AD-7.6 practice test so you can know mistakes and overcome them at each and every step. The Desktop NSE5_SSE_AD-7.6 Practice Exam software is created and updated in a timely by a team of experts in this field. If any problem arises, a support team is there to fix the issue.

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Sample Questions (Q33-Q38):

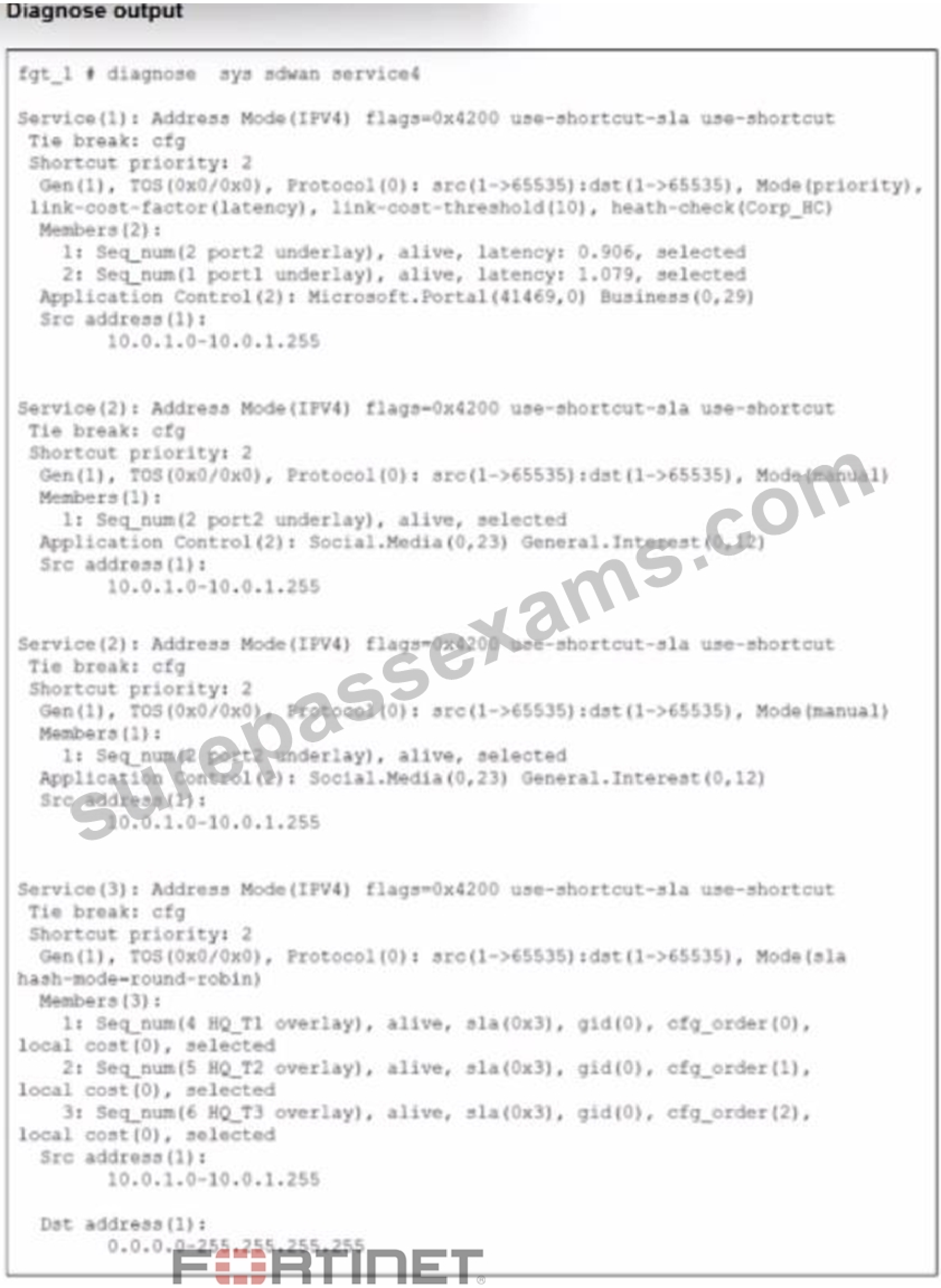
NEW QUESTION # 33
Which two statements about configuring a steering bypass destination in FortiSASE are correct? (Choose two.)

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

Answer: A,D

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 # 34
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(1->65535), Mode(sla
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. When FortiGate cannot recognize the application of the flow, it steers the traffic through the preferred member of rule 3, HQ_T1.

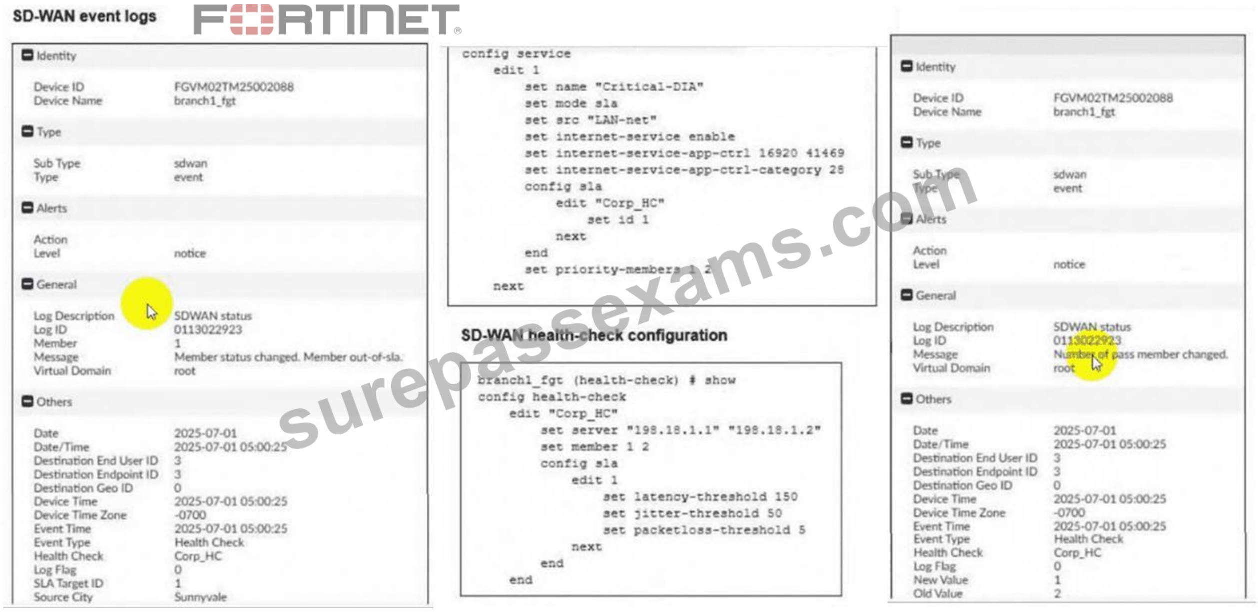
- B. There is no service defined for the Facebook application, so FortiGate applies service rule 3 and directs the traffic to headquarters.
- C. When FortiGate cannot recognize the application of the flow, it load balances the traffic through the tunnels HQ_T1, HQ_T2, HQ_T3.
- D. FortiGate steers traffic for social media applications according to the service rule 2 and steers traffic through port2.

Answer: C,D

Explanation:
"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 # 35

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
    Source City                 Sunnyvale
```

```
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
    Old Value                   2
```

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 skips SD-WAN rule ID 1.
- B. FortiGate uses port1 or port2 to steer the traffic for SD-WAN rule ID 1.
- C. FortiGate uses port1 to steer the traffic for SD-WAN rule ID 1.
- D. FortiGate uses port2 to steer the traffic for SD-WAN rule ID 1.

Answer: D

Explanation:
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 # 36
Refer to the exhibit, which shows the 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(packet loss), link-cost-threshold(0), heath-check(HUB1_HC)
     Members(3):
          1: Seq_num(4 HUB1-VPN1 HUB1), alive, packet loss: 2.000%, selected
          2: Seq_num(5 HUB1-VPN2 HUB1), alive, packet loss: 4.000%, selected
          3: Seq_num(6 HUB1-VPN3 HUB1), alive, packet loss: 12.000%, 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 link-cost-factor packet-loss
          set link-cost-threshold 0
          set priority-members 6 4 5
     next
```

Based on the exhibit, which change in the measured packet loss will make HUB1-VPN3 the new preferred member? (Choose one answer)

- A. When HUB1-VPN1 has 4% packet loss
- B. When HUB1-VPN1 has 12% packet loss
- C. When HUB1-VPN3 has 4% packet loss
- D. When all three members have the same packet loss

Answer: D

Explanation:
According to theSD-WAN 7.6 Core Administratorstudy guide and theFortiOS 7.6 Administration Guide, the selection process for theBest Quality (priority)strategy depends on two primary factors: the measured link quality metric and the configured member priority order.
Based on the provided exhibit (image_b40dfc.png), we can determine the following:
* Strategy and Metric: The rule is in Mode(priority) (Best Quality) using link-cost-factor(packet loss).
* Strict Comparison: The link-cost-threshold is set to0. This means there is no "advantage" given to the current preferred link; the FortiGate performs a strict comparison where the link with the objectively best metric is chosen.
* Tie-Breaker Logic: When multiple links have thesamepacket loss, the FortiGate uses theMember Priority Orderdefined in the rule (set priority-members 6 4 5) as the tie-breaker.
* Member 6 (HUB1-VPN3)is the highest priority.
* Member 4 (HUB1-VPN1)is the second priority.

* Member 5 (HUB1-VPN2)is the lowest priority.
* Current State: HUB1-VPN1 is currently selected because its packet loss (2.000%) is lower than HUB1-VPN2 (4.000%) and HUB1-VPN3 (12.000%). Even though HUB1-VPN3 has a higher configuration priority, its significantly higher packet loss prevents it from being chosen.
Evaluation of Options:
* Option A (Verified): If all three members have thesame packet loss(e.g., they all show 2%), the quality metrics are equal. The SD-WAN engine then refers to the priority-members list. Since HUB1- VPN3 (Seq 6) is the first member in that list, it will immediately become the new preferred member.
* Option B: If HUB1-VPN1 reaches 4%, it matches HUB1-VPN2 (4%). HUB1-VPN3 remains at 12%.
The system will choose between VPN1 and VPN2. Since VPN1 (Seq 4) is higher in the priority list than VPN2 (Seq 5), HUB1-VPN1 stays preferred.
* Option C: If HUB1-VPN1 reaches 12%, it matches HUB1-VPN3. However, HUB1-VPN2 is still better at4.000%. Therefore, HUB1-VPN2 would become the new preferred member, not HUB1-VPN3.
* Option D: If HUB1-VPN3 drops to 4%, it matches HUB1-VPN2. However, HUB1-VPN1 is still the best link at2.000%, so it remains selected.

NEW QUESTION # 37

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

Answer: D

Explanation:
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 # 38

......

- NSE5_SSE_AD-7.6 Reliable Dumps Book □ Valid Braindumps NSE5_SSE_AD-7.6 Pdf □ NSE5_SSE_AD-7.6 Test Lab Questions □ Easily obtain free download of ☀ NSE5_SSE_AD-7.6 □☀□ by searching on ➠ www.examdiscuss.com □ □Exam Dumps NSE5_SSE_AD-7.6 Free
- Real NSE5_SSE_AD-7.6 Exam Answers □ New NSE5_SSE_AD-7.6 Test Tutorial □ NSE5_SSE_AD-7.6 Exam Outline □ Search for 【 NSE5_SSE_AD-7.6 】 and easily obtain a free download on " www.pdfvce.com " □ □NSE5_SSE_AD-7.6 Real Exam Answers
- Download Fortinet NSE5_SSE_AD-7.6 Exam Questions and Start Your Preparation journey Today □ Search for 【 NSE5_SSE_AD-7.6 】 on 《 www.vce4dumps.com 》 immediately to obtain a free download □NSE5_SSE_AD-7.6 Best Study Material
- Hot NSE5_SSE_AD-7.6 Test Pass4sure - Reliable NSE5_SSE_AD-7.6 Exam Tool Guarantee Purchasing Safety □ Easily obtain ▷ NSE5_SSE_AD-7.6 ◁ for free download through [www.pdfvce.com] □NSE5_SSE_AD-7.6 New Braindumps Ebook
- Quiz Fortinet - NSE5_SSE_AD-7.6 –Latest Test Pass4sure □ Download ▷ NSE5_SSE_AD-7.6 ◁ for free by simply searching on [www.testkingpass.com] □Valid Braindumps NSE5_SSE_AD-7.6 Pdf
- Exam Dumps NSE5_SSE_AD-7.6 Free □ NSE5_SSE_AD-7.6 Best Study Material □ NSE5_SSE_AD-7.6 Exam Outline □ Search for ✔ NSE5_SSE_AD-7.6 □✔□ and download exam materials for free through 「 www.pdfvce.com 」 □New NSE5_SSE_AD-7.6 Test Tutorial
- Hot NSE5_SSE_AD-7.6 Test Pass4sure - Reliable NSE5_SSE_AD-7.6 Exam Tool Guarantee Purchasing Safety □ Search for [NSE5_SSE_AD-7.6] and download it for free immediately on （ www.pdfdumps.com ） □ □NSE5_SSE_AD-7.6 Real Exam Answers
- Quiz Fortinet - NSE5_SSE_AD-7.6 –Latest Test Pass4sure □ Search on 【 www.pdfvce.com 】 for ▶ NSE5_SSE_AD-7.6 ◀ to obtain exam materials for free download □Valid NSE5_SSE_AD-7.6 Exam Question
- NSE5_SSE_AD-7.6 Valid Exam Cost □ Reliable NSE5_SSE_AD-7.6 Study Notes □ Pdf Demo NSE5_SSE_AD-7.6 Download ❇ ▶ www.practicevce.com ◀ is best website to obtain ✔ NSE5_SSE_AD-7.6 □✔□ for free download □ □Valid NSE5_SSE_AD-7.6 Exam Camp
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, ncon.edu.sa, Disposable vapes