PassQueen
a.k.a dumpsqueen.com

Network Security Expert 8 Written Exam

Fortinet NSE8_812

Version Demo

Total Demo Questions: 12

Total Premium Questions: 127

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, FortiGate	88
Topic 2, FortiManager	8
Topic 3, FortiAnalyzer	2
Topic 4, FortiMail	6
Topic 5, FortiWeb	4
Topic 6, FortiDDoS	2
Topic 7, FortiSandbox	1
Topic 8, FortiNAC	1
Topic 9, FortiSIEM	1
Topic 10, FortiSOAR	1
Topic 11, FortiEDR	2
Topic 12, FortiSwitch	4
Topic 13, FortiAP	1
Topic 14, FortiClient EMS	3
Topic 15, Mix Questions	3
Total	127

QUESTION NO: 1

Refer to the exhibits.

Exhibit A

	FORTIAP 431F
Hardware	
Hardware Type	Indoor AP
Number of Radios	3 + 1 BLE
Number of Antennas	5 Internal + 1 BLE Internal
Antenna Type and Peak Gain	PIFA: 4 dBi for 2.4 GHz, 5 dBi for 5 GHz
Maximum Data Rate	Radio 1: up to 1147 Mbps Radio 2: up to 2402 Mbps Radio 3: scan only
Bluetooth Low Energy Radio	Bluetooth scanning and iBeacon advertisement @ 6 dBm max TX power
Interfaces	1× 100/1000/2500 Base-T RJ45, 1 × 10/100/1000 Base-T RJ45, 1x Type A USB, 1x RS-232 RJ45 Serial Port
Power over Ethernet (PoE)	• 802.3at PoE default • 1 port powered by 802.3at or 2 ports powered by 802.3af - Full System functionality + USB support
Maximum Tx Power (Conducted)	Radio 1: 2.4 GHz 24 dBm / 251 mW (4 chains combined)* Radio 2: 5 GHz 23 dBm / 200 mW (4 chains combined)* Radio 3: NA
Environment	
Power Supply	SP-FAP400-PA-XX or GPI-130
Power Consumption (Max)	24.5 W
Directives	Low Voltage Directive • RoHS
UL2043 Plenum Material	No
Mean Time Between Failures	>10 Years
Surge Protection Built In	Yes
Hit-less PoE Failover	Yes

Exhibit B

	FORTISWITCH 224E-POE	FORTISWITCH 124E-FPOE	FORTISWITCH 248E-FPOE
Hardware Specifications			
Total Network Interfaces	24x GE RJ45 ports and 4x GE SFP ports	24x GE RJ45 and 4x GE SFP	48x GE RJ45 ports and 4x GE SFP ports
Dedicated Management 10/100 Port	1	0	1
RJ-45 Serial Console Port	1	1	1
Form Factor	1 RU Rack Mount	1 RU Rack Mount	1 RU Rack Mount
Power over Ethernet (PoE) Ports	12 (802.3af/802.3at)	24 (802.3af/at)	48 (802.3af/802.3at)
PoE Power Budget	180 W	370 W	740 W
Mean Time Between Failures	> 10 years	> 10 years	> 10 years
Retail Price	$1,000	$1,250	$1,500

A customer wants to deploy 12 FortiAP 431F devices on high density conference center, but they do not currently have any PoE switches to connect them to. They want to be able to run them at full power while having network redundancy

From the FortiSwitch models and sample retail prices shown in the exhibit, which build of materials would have the lowest cost, while fulfilling the customer's requirements?

A. 1x FortiSwitch 248EFPOE

B. 2x FortiSwitch 224E-POE

C. 2x FortiSwitch 248E-FPOE

D. 2x FortiSwitch 124E-FPOE

ANSWER: D

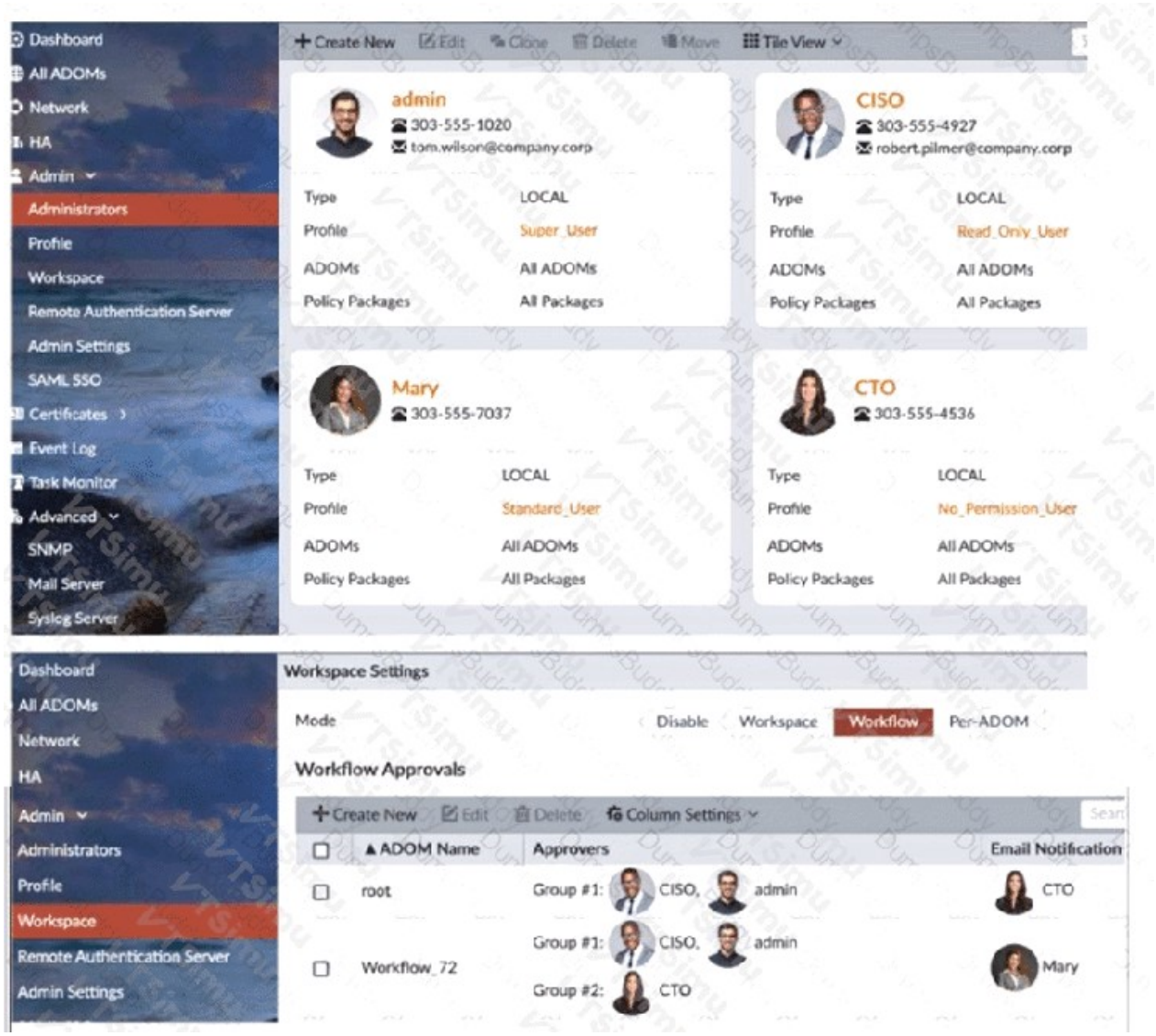
Explanation:

2x FortiSwitch 124E-FPOE satisfies the power, port, redundancy, and cost requirements. A FortiAP 431F requires approximately 24.5 W when powered at its full PoE level. Twelve access points therefore require roughly 294 W. The FortiSwitch 124E-FPOE provides a 370 W PoE budget, so either switch can supply the full PoE demand for all twelve access points while remaining within its available budget. This capacity is important for a resilient design because a single remaining switch can continue to power the AP deployment if the other switch is unavailable.

Using two switches also provides the physical basis for network redundancy: the access points can be connected across the two switches, and the switches can be deployed with redundant uplinks toward the upstream network. The 124E-FPOE provides sufficient PoE-capable access ports for the AP connections while avoiding unnecessary port density and PoE capacity. Based on the retail prices in the exhibit, this pair is the least expensive design that still provides two-switch resiliency and enough full-power PoE capacity. Fortinet lists the FortiAP 431F power requirements on its FortiAP 431F product page. Fortinet PoE configuration and power-management behavior are documented in the FortiSwitchOS Administration Guide.

QUESTION NO: 2

Refer to the exhibit.



The Company Corp administrator has enabled Workflow mode in FortiManager and has assigned approval roles to the current administrators. However, workflow approval does not function as expected. The CTO is currently unable to approve submitted changes.

Given the exhibit, which two possible solutions will resolve the workflow approval problems with the Workflow_72 ADOM? (Choose two.)

A. The CTO must have a defined email address for their admin user account.

B. The CTO and CISO need to swap Approval Groups so that the highest authority is in Group #1.

C. The CTO must have Standard access level or higher for FortiManager.

D. The CISO must have a higher access level than "Read_Only_User" in FortiManager.

E. The CTO needs to be added to "Email Notification" in the Workflow_72 ADOM.

ANSWER: A C

Explanation:

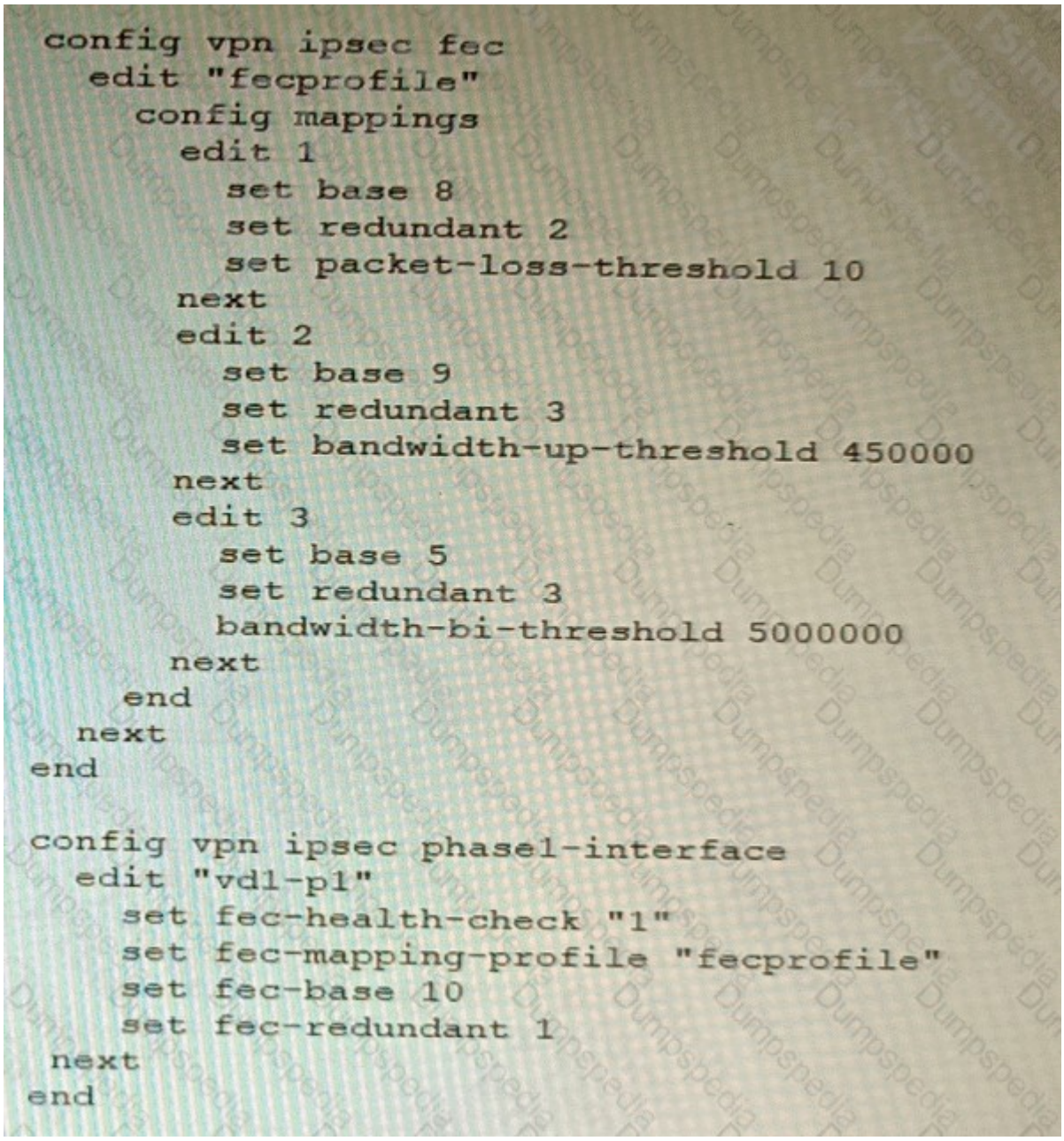
Workflow approval in FortiManager depends on both a valid approver identity and sufficient administrative permissions. The CTO must have a defined email address for their admin user account because FortiManager workflow uses email information to identify and notify workflow participants. Supplying an email address ensures that the assigned approver can receive workflow-related notifications and is configured as a complete workflow user.

The CTO must have Standard access level or higher for FortiManager because an approver must be able to access FortiManager and perform the approval action for submitted revisions or workflow requests. A read-only access level is intended for viewing configuration and status information, while Standard-level administrative access provides the required ability to participate in workflow operations. With a defined email address and Standard or greater administrative access, the CTO can act on approval requests associated with the ADOM's configured approval workflow.

Fortinet documents workflow configuration, approver assignment, and approval processing in the FortiManager Administration Guide. Administrative access profiles and their permissions are also covered in Fortinet's administrator documentation.

QUESTION NO: 3

Review the VPN configuration shown in the exhibit.



```
config vpn ipsec fec
  edit "fecprofile"
    config mappings
      edit 1
        set base 8
        set redundant 2
        set packet-loss-threshold 10
      next
      edit 2
        set base 9
        set redundant 3
        set bandwidth-up-threshold 450000
      next
      edit 3
        set base 5
        set redundant 3
        bandwidth-bi-threshold 5000000
      next
    end
  next
end

config vpn ipsec phase1-interface
  edit "vd1-p1"
    set fec-health-check "1"
    set fec-mapping-profile "fecprofile"
    set fec-base 10
    set fec-redundant 1
 next
end
```

What is the Forward Error Correction behavior if the SD-WAN network traffic download is 500 Mbps and has 8% of packet loss in the environment?

A. 1 redundant packet for every 10 base packets

B. 3 redundant packet for every 5 base packets

C. 2 redundant packet for every 8 base packets

D. 3 redundant packet for every 9 base packets

ANSWER: A

Explanation:

1 redundant packet for every 10 base packets is the applicable Forward Error Correction (FEC) behavior. FEC mappings are selected only when their configured matching criteria are met. In this scenario, the measured packet loss is 8%, which does not meet the packet-loss mapping threshold shown in the configuration for loss greater than 10%. The download traffic rate is 500 Mbps, which also does not meet the configured high-bandwidth threshold of greater than 950 Mbps. As neither conditional mapping applies, FortiGate uses the configured default FEC ratio: 10 base packets followed by 1 redundant packet.

This ratio adds recovery information to the traffic flow without requiring retransmission of a lost packet. The receiving FortiGate can use the redundant packet with the base-packet block to reconstruct packet loss within the recovery capability of that FEC block. FEC is particularly useful for latency-sensitive SD-WAN overlay traffic because it can mitigate loss before a retransmission-based protocol would otherwise recover. Fortinet documents FEC as an IPsec/SD-WAN capability and provides FortiGate configuration documentation through its FortiGate documentation portal. Additional product and feature guidance is available from Fortinet's FortiGate product documentation resources.

QUESTION NO: 4

Refer to the exhibits, which show a topology and diagnostic commands.

Exhibit A

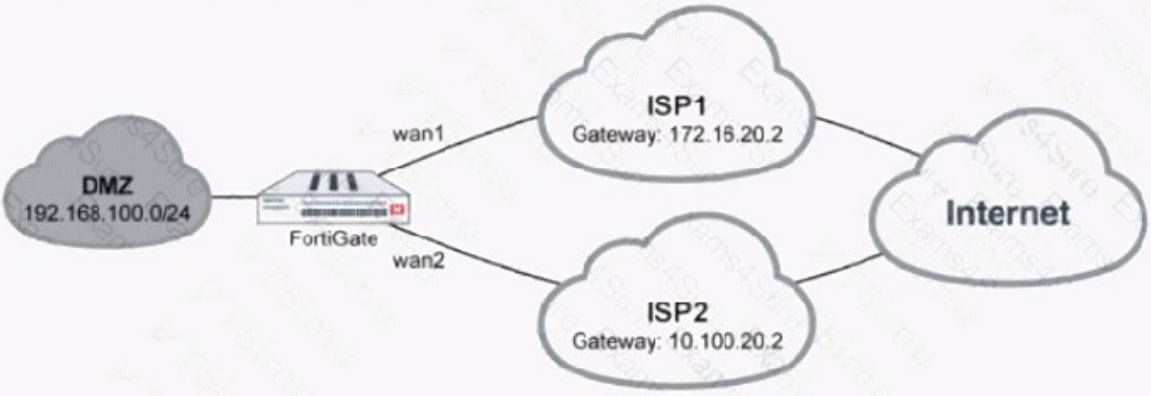


Exhibit B

```
FGT # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(6), TOS(0x0/0x0), Protocol[0: 1->65535), Mode(priority), link-cost-factor(latency),
link-cost-threshold(20), health-check(Default_Gmail)
  Members(2):
    1: Seq_num(1 wan1), alive, latency: 200.177, selected
    2: Seq_num(2 wan2), alive, latency: 167.417, selected
  Src address(1):
        192.168.100.0-192.168.100.255

  Dst address(1):
        0.0.0.0-255.255.255.255

FGT # diagnose sys sdwan health-check
Health Check(Default_Gmail):
Seq(1 wan1): state(alive), packet-loss(2.000%) latency(200.564), jitter(1.277) sla_map=0x1
Seq(2 wan2): state(alive), packet-loss(0.000%) latency(167.877), jitter(1.060) sla_map=0x1

FGT # diagnose sys sdwan member
Member(1): interface: wan1, pricrity: 0, weight: 0
Member(2): interface: wan2, pricrity: 0, weight: 0
```

Which two statements about the path resolution are true? (Choose two.)

A. Latency is the quality criteria.

B. wan1 is currently used as an outgoing interface.

C. wan2 is currently used as an outgoing interface.

D. Packet-loss is the quality criteria.

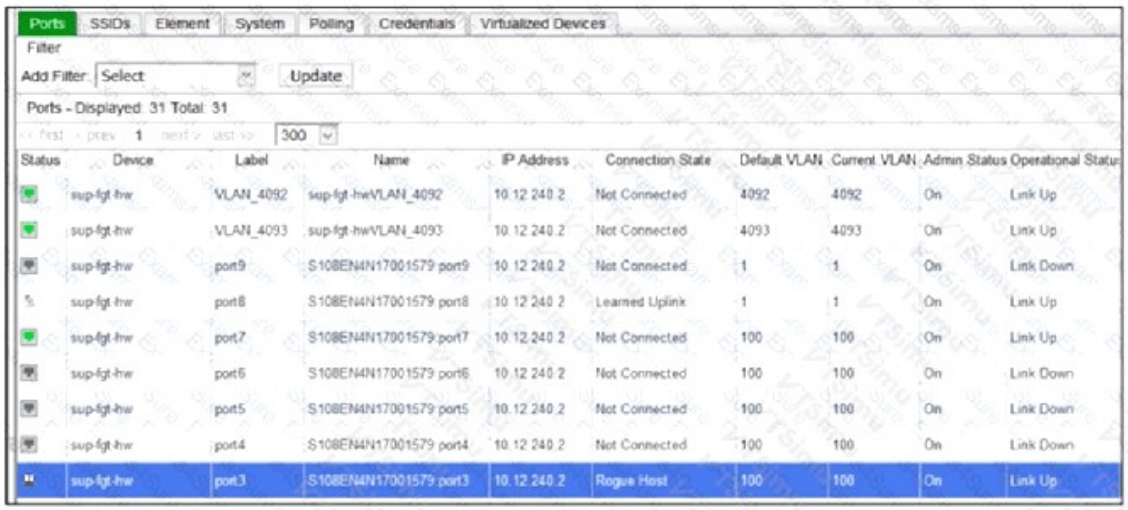
ANSWER: A

Explanation:

Latency is the quality criteria. In FortiGate SD-WAN, performance-SLA health checks can measure latency, jitter, and packet loss for each configured member. An SD-WAN rule can use one or more of those SLA measurements as quality criteria when FortiGate resolves an eligible path. The diagnostic information in the exhibit identifies latency as the configured criterion used for this path-resolution decision. FortiGate continuously evaluates the measured round-trip latency against the configured SLA threshold and uses the health-check state during member selection. This allows traffic to be steered according to measured application-path performance rather than relying solely on a static preference. The selected criterion is therefore the key fact for interpreting the resolution output: the relevant SLA assessment is based on latency. Fortinet documents SD-WAN health checks and their use of latency, jitter, and packet-loss measurements in the FortiGate SD-WAN Administration Guide. Configuration details for performance-SLA settings and their threshold values are also available in the FortiGate CLI Reference: SD-WAN health checks.

QUESTION NO: 5

Refer to the exhibit of a FortiNAC configuration.



In this scenario, which two statements are correct? (Choose two.)

A. A device that is modeled in FortiNAC is connected on VLAN 4093.

B. An unknown host is connected to port3.

C. The IP address of the FortiSwitch is 10.12.240.2.

D. Port8 is connected to a FortiGate in FortiLink mode.

ANSWER: B C

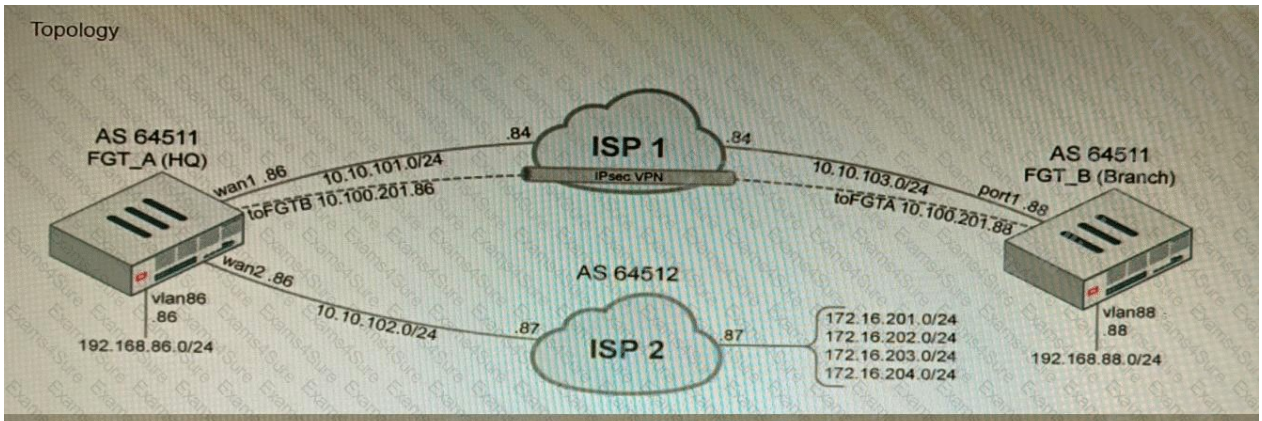
Explanation:

The correct observations are that an unknown host is connected to port3 and that the FortiSwitch has the IP address 10.12.240.2. The FortiNAC port view identifies port3 with the connection classification *Rogue Host*. FortiNAC uses this designation when it detects an endpoint on a managed access port that has not been recognized, registered, or otherwise classified as an authorized endpoint. Thus, the displayed state establishes that an unknown endpoint is physically connected through port3. FortiNAC's host and connection management workflow is documented in the FortiNAC Administration Guide.

The repeated address 10.12.240.2 in the displayed device and port information is the management address associated with the FortiSwitch being viewed. FortiNAC uses this address to identify and communicate with the managed network device while collecting its port, VLAN, link, and endpoint data. This is why the address is associated with the switch record rather than representing a separate endpoint on every displayed port. Fortinet documents FortiSwitch management and device integration concepts in the FortiSwitch Administration Guide.

QUESTION NO: 6

Refer to the exhibits.



Configuration

```
** HQ CONFIGURATION **

config router prefix-list
    edit "route-in"
        config rule
            edit 1
                set prefix 172.16.201.0 255.255.255.0
                set ge 25
                set le 28
            next
            edit 2
                set prefix 172.16.204.0 255.255.255.0
                set ge 23
                set le 25
            next
        end
    next
end
config router bgp
    set as 64511
    set router-id 1.1.1.1
    config neighbor
        edit "10.10.102.87"
            set soft-reconfiguration enable
            set prefix-list-in "route-in"
            set remote-as 64512
        next
    end
end
```

A customer has deployed a FortiGate with iBGP and eBGP routing enabled. HQ is receiving routes over eBGP from ISP 2; however, only certain routes are showing up in the routing table-Assume that BGP is working perfectly and that the only possible modifications to the routing table are solely due to the prefix list that is applied on HQ.

Given the exhibits, which two routes will be active in the routing table on the HQ firewall? (Choose two.)

A. 172.16.204.128/25

B. 172.16.201.96/29

C. 172.62.0.64/27

D. 172.16.204.64/27

ANSWER: A D

Explanation:

172.16.204.128/25 and **172.16.204.64/27** are active because both advertised networks fall within the 172.16.204.0/24 prefix range specified by the applicable prefix-list rule, and their prefix lengths satisfy that rule's permitted subnet-mask range. A prefix-list evaluates both the address portion of a route and, when configured, its prefix length. Consequently, a route need not be identical to the configured base prefix: it can be a more-specific subnet when its network address is contained by the configured prefix and its mask length is allowed by the rule.

For 172.16.204.128/25, the first 24 bits identify the 172.16.204.0/24 network, while the /25 mask makes it a permitted more-specific route. Likewise, 172.16.204.64/27 remains inside 172.16.204.0/24 and has an allowed more-specific prefix length. Because the prefix list is applied to routes received by HQ from ISP 2, matching routes are permitted into BGP's route processing and can be installed as active routes, assuming the stated condition that no other BGP behavior affects route

selection. FortiGate documents prefix lists as route filters that can match a network prefix together with optional minimum and maximum prefix lengths; see the FortiGate BGP documentation and the prefix-list CLI reference.

QUESTION NO: 7

Refer to the exhibit, which shows diagnostic output.

```
FGT-SDW-1 # diagnose sys sdwan health-check status CZ.NIC_DNS
Health Check(CZ.NIC_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%)
latency(79.164), jitter(2.861), bandwidth-up(49988), bandwidth-
dw(49975), bandwidth-bi(99963) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(2.215),
jitter(0.701), bandwidth-up(9991), bandwidth-dw(9990),
bandwidth-bi(19981) sla_map=0x1


FGT-SDW-1 # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority),
link-cost-factor(latency), link-cost-threshold(10), heath-
check(CZ.NIC_DNS)
  Members(2):
    1: Seq_num(2 port2), alive, latency: 2.343, selected
    2: Seq_num(1 port1), alive, latency: 107.004, selected
  Src address(1):
     192.168.1.0-192.168.1.255

  Dst address(1):
     93.190.134.171-93.190.134.171


FGT-SDW-1 # diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00
protocol=0 sport=0-0 iif=7 dport=0-65535 path(1) oif=3(port1)
gwy=198.18.11.254
source(1): 192.168.1.0-192.168.1.255
destination wildcard(1): 93.190.134.0/255.255.255.0
hit_count=21 last_used=2022-07-14 16:59:42

id=2132082689(0x7f150001) vwl_service=1(Internet) vwl_mbr_seq=2
1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=
0 sport=0-65535 iif=0 dport=1-65535 path(2) oif=4(port2) oif=
3(port1)
source(1): 192.168.1.0-192.168.1.255
destination(1): 93.190.134.171-93.190.134.171
hit_count=25 last_used=2022-07-14 16:59:23
```

A customer reports that ICMP traffic flow from 192.168.1.11 to 93.190.134.171 is not corresponding to the SD-WAN setup.

What is the problem in this scenario?

A. SD-WAN Rule is matching only DNS traffic.

B. Port1 is used because it has more available bandwidth.

C. Traffic is matched by policy route.

D. Route for the destination IP is missing in the routing table.

ANSWER: C

Explanation:

Traffic is matched by policy route. The diagnostic flow lookup indicates that a policy route applies to traffic from 192.168.1.11 toward 93.190.134.171. FortiGate evaluates policy routes before its normal route lookup, so a matching policy route can explicitly select an egress interface or next hop and thereby bypass the route-selection behavior expected from the SD-WAN configuration. This is especially important when troubleshooting traffic that appears not to follow an SD-WAN rule: even if the SD-WAN zone, members, health checks, and service rule are configured correctly, an earlier policy-route decision can determine forwarding independently of those settings. The effective solution is to review the matching policy route and either remove it, narrow its source/destination/service match criteria, or modify it so that the traffic can be handled by the intended SD-WAN forwarding logic. Fortinet documents that policy routes provide policy-based forwarding and are checked before the routing table. See the FortiGate policy routes administration guide and the FortiGate SD-WAN rules administration guide.

QUESTION NO: 8

A FortiGate active-passive HA cluster protects a business-critical application. The administrator requires existing sessions to survive a failover whenever possible, including UDP-based application sessions.

Which two statements are correct? (Choose two.)

A. Enable session pickup to synchronize eligible established sessions between cluster members.

B. Enable session-pickup-connectionless to synchronize UDP and ICMP sessions.

C. Enable HA override to synchronize the session table between cluster members.

D. Enable configuration synchronization to preserve active traffic sessions during failover.

ANSWER: A B

Explanation:

Session pickup synchronizes session information from the active FortiGate to the standby FortiGate. When a failover occurs, the new primary can use the synchronized information to continue eligible established sessions instead of treating all traffic as new.

TCP session synchronization is enabled with session pickup. Connectionless protocols such as UDP and ICMP require connectionless session pickup because they do not have TCP state information that can be synchronized through the normal TCP session-pickup mechanism.

Configuration synchronization alone does not synchronize the runtime session table. Enabling HA override affects which member becomes primary after recovery, but it does not provide session continuity.

QUESTION NO: 9

Refer to the exhibits, which show a network topology and VPN configuration.

A network administrator has been tasked with modifying the existing dial-up IPsec VPN infrastructure to detect the path quality to the remote endpoints.

After applying the configuration shown in the configuration exhibit, the VPN clients can still connect and access the protected 172.16.205.0/24 network, but no SLA information shows up for the client tunnels when issuing the diagnose sys link-monitor tunnel all command on the FortiGate CLI.

What is wrong with the configuration?

A. SLA link monitoring does not work with the net-device setting.

B. The admin needs to disable the mode-cfg setting.

C. IPsec Phase1 Interface has to be configured in IPsec main mode.

D. It is necessary to use the IKEv2 protocol in this situation.

ANSWER: A

Explanation:

SLA link monitoring does not work with the net-device setting. For a dial-up IPsec deployment, FortiGate must be able to associate the performance-SLA monitor with each dynamically established client tunnel. Enabling a separate network device for the dial-up tunnel prevents the tunnel-SLA mechanism from obtaining and reporting the per-client tunnel health state expected by `diagnose sys link-monitor tunnel all`. As a result, IPsec connectivity and traffic forwarding can continue normally, while the diagnostic command has no client-tunnel SLA entries to display.

The appropriate design is to configure the dial-up phase-one interface so it can participate in FortiGate's tunnel monitoring model, including disabling the incompatible net-device behavior where required by the dial-up SLA configuration. Once the phase-one configuration and the relevant Performance SLA/link-monitor settings are applied, FortiGate can send probes through the established tunnels, measure reachability and quality metrics, and expose those results through the tunnel link-monitor diagnostic output. Fortinet documents IPsec phase-one interface parameters and monitoring-related configuration in the FortiGate Administration Guide and the available phase-one CLI settings in the FortiGate documentation portal.

QUESTION NO: 10

You are running a diagnose command continuously as traffic flows through a platform with NP6 and you obtain the following output:

```
diag npu np6 dce 1
PDQ_OSW_EHP1 :0000000000001833 [5b]
diag npu np6 dce 1
PDQ OSW EHPI :0000000000000003 [80]
diag npu np6 dce 1
PDQ OSW EHP1 :0000000000000552 [94]
```

Given the information shown in the output, which two statements are true? (Choose two.)

A. Enabling bandwidth control between the ISF and the NP will change the output

B. The output is showing a packet descriptor queue accumulated counter

C. Enable HPE shaper for the NP6 will change the output

D. Host-shortcut mode is enabled.

E. There are packet drops at the XAUI.

ANSWER: B E

Explanation:

The output is showing a packet descriptor queue accumulated counter because the NP6 PDQ diagnostic reports the `PDQ ACCU` field for the applicable XAUI interfaces. This counter records packet descriptors accumulated in the packet descriptor

queue and is useful when monitoring queue utilization and identifying traffic-processing pressure over time. The diagnostic is designed to expose these PDQ statistics per NP6/XAUI path while traffic is being processed.

There are packet drops at the XAUI because the displayed nonzero `PDQ DROP` values identify descriptors dropped at the corresponding XAUI packet descriptor queues. XAUI is the high-speed connection used by the NP6 in the platform data path, and a PDQ drop counter provides direct evidence that packets/descriptors were discarded on that path. Observing both accumulation and drops is therefore relevant when investigating congestion or an imbalance affecting NP6 queue processing. Fortinet documents the NP6 PDQ diagnostic fields and commands in the FortiGate CLI Reference: diagnose np6 pdq. Additional NP6 architecture and packet-flow context is available in the FortiGate Hardware Acceleration Guide.

QUESTION NO: 11

A network administrator is troubleshooting why a client at 10.10.20.15 cannot establish a TCP connection through a FortiGate.

The administrator wants to display a limited number of flow-debug entries only for traffic sourced from that client.

Which three commands are required? (Choose three.)

A. diagnose debug flow filter saddr 10.10.20.15

B. diagnose debug flow trace start 100

C. diagnose debug enable

D. diagnose sniffer packet any "host 10.10.20.15" 4

E. diagnose debug reset

ANSWER: A B C

Explanation:

`diagnose debug flow filter saddr 10.10.20.15` limits flow-debug output to sessions using the specified source address. `diagnose debug flow trace start 100` defines the number of packets or trace entries to capture, and `diagnose debug enable` starts the debug output.

`diagnose debug reset` is useful to clear previous diagnostic settings, but it is not required to run a filtered flow debug. Packet sniffing is a separate diagnostic method and does not display FortiGate policy-routing and session-processing decisions in the same way as flow debug.

QUESTION NO: 12

A FortiGate must be configured to accept VoIP traffic which will include session initiation protocol (SIP) traffic. Which statement about the VoIP configuration options is correct?

A. Restricting SIP requests is only possible when using the SIP Session Helper.

B. Rate tracking of SIP requests is only possible when the application layer gateway (ALG) is set to Flow mode.

C. FortiOS cannot accept SIP traffic if both the SIP Session Helper and the application layer gateway (ALG) are disabled.

D. By default, VoIP traffic will be processed using the SIP Session Helper.

ANSWER: D

Explanation:

By default, VoIP traffic will be processed using the SIP Session Helper. FortiGate registers the SIP session helper for the standard SIP control port, TCP/UDP 5060, in the session-helper configuration. The helper is a kernel-level mechanism that recognizes SIP control sessions and can create the related expectations needed for the dynamically negotiated media

streams, such as RTP. This default behavior allows FortiGate to provide SIP-aware handling without requiring a separate proxy-based SIP ALG configuration for ordinary deployments.

The session helper is visible in the FortiGate configuration under `config system session-helper`, where the SIP helper entry is normally present unless an administrator has intentionally removed it. Administrators may choose a different VoIP handling design—for example, disabling the helper when a SIP provider specifically requires SIP inspection or address translation to be bypassed—but that is a deliberate configuration change rather than the default state. Fortinet's SIP ALG guidance also identifies the SIP session helper as a relevant default component when reviewing or changing SIP handling behavior. See Fortinet's technical note on disabling SIP ALG and the FortiGate Administration Guide.