

Fortinet.NSE8_812.v2026-04-18.q51

Exam Code:	NSE8_812
Exam Name:	Fortinet NSE 8 - Written Exam (NSE8_812)
Certification Provider:	Fortinet
Free Question Number:	51
Version:	v2026-04-18
# of views:	118
# of Questions views:	510
https://www.freepdfdumps.com/Fortinet.NSE8_812.v2026-04-18.q51.html	

NEW QUESTION: 1

What is the benefit of using FortiGate NAC LAN Segments?

- A. It provides support for multiple DHCP servers within the same VLAN.
- B. It provides physical isolation without changing the IP address of hosts.
- C. It provides support for IGMP snooping between hosts within the same VLAN
- D. It allows for assignment of dynamic address objects matching NAC policy.

Answer: B (LEAVE A REPLY)

FortiGate NAC LAN Segments are a feature that allows users to assign different VLANs to different LAN segments without changing the IP address of hosts or bouncing the switch port. This provides physical isolation while maintaining firewall sessions and avoiding DHCP issues. One benefit of using FortiGate NAC LAN Segments is that it allows for assignment of dynamic address objects matching NAC policy. This means that users can create firewall policies based on dynamic address objects that match the NAC policy criteria, such as device type, OS type, MAC address, etc. This simplifies firewall policy management and enhances security by applying different security profiles to different types of devices. References: <https://docs.fortinet.com/document/fortigate/7.0.0/new-features/856212/nac-lan-segments-7-0-1>
<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/856212/nac-lan-segments-7-0-1>

NEW QUESTION: 2

You deployed a fully loaded FG-7121F in the data center and enabled sslvpn-load-balance. Based on the behavior of this feature which statement is correct?

- A. You can use src-ip or dst-ip-dport on dp-load-distribution-method to make SSL VPN load balancing work as expected.
- B. If an FPM goes down, SSL VPN IP pool IP addresses will be re-allocated to the remaining FPMs.
- C. To have better traffic distribution you should use IP pools that increment in multiples of 12.
- D. Enabling SSL VPN load balancing will clear the session table.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 3

You must configure an environment with dual-homed servers connected to a pair of FortiSwitch units using an MCLAG.

Multicast traffic is expected in this environment, and you should ensure unnecessary traffic is pruned from links that do not have a multicast listener.

In which two ways must you configure the igmps-flood-traffic and igmps-flood-report settings? (Choose two.)

- A. disable on ICL trunks
- B. enable on ICL trunks
- C. disable on the ISL and FortiLink trunks
- D. enable on the ISL and FortiLink trunks

Answer: B,C ([LEAVE A REPLY](#))

<https://docs.fortinet.com/document/fortiswitch/7.0.8/devices-managed-by-fortios/801194/deploying-mclag-topologies>

NEW QUESTION: 4

Refer to the exhibit of a FortiNAC configuration.

Status	Device	Label	Name	IP Address	Connection State	Default VLAN	Current VLAN	Admin Status	Operational Status
✓	sup-fgt-hw	VLAN_4092	sup-fgt-hwVLAN_4092	10.12.240.2	Not Connected	4092	4092	On	Link Up
✓	sup-fgt-hw	VLAN_4093	sup-fgt-hwVLAN_4093	10.12.240.2	Not Connected	4093	4093	On	Link Up
✗	sup-fgt-hw	port9	S108EN4N17001579:port9	10.12.240.2	Not Connected	1	1	On	Link Down
⚙	sup-fgt-hw	port8	S108EN4N17001579:port8	10.12.240.2	Learned Uplink	1	1	On	Link Up
✓	sup-fgt-hw	port7	S108EN4N17001579:port7	10.12.240.2	Not Connected	100	100	On	Link Up
✗	sup-fgt-hw	port6	S108EN4N17001579:port6	10.12.240.2	Not Connected	100	100	On	Link Down
✗	sup-fgt-hw	port5	S108EN4N17001579:port5	10.12.240.2	Not Connected	100	100	On	Link Down
✗	sup-fgt-hw	port4	S108EN4N17001579:port4	10.12.240.2	Not Connected	100	100	On	Link Down
⚙	sup-fgt-hw	port3	S108EN4N17001579:port3	10.12.240.2	Rogue Host	100	100	On	Link Up

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

- A. The IP address of the FortiSwitch is 10.12.240.2.
- B. An unknown host is connected to port3.
- C. A device that is modeled in FortiNAC is connected on VLAN 4093.
- D. Port8 is connected to a FortiGate in FortiLink mode.

Answer: A,B ([LEAVE A REPLY](#))

NEW QUESTION: 5

Refer to the exhibit.



What is happening in this scenario?

- A. The user status changed at FortiClient EMS to off-net.
- B. The user has not authenticated on their external browser.
- C. The user is authenticating against a FortiGate Captive Portal.
- C The user is authenticating against an IdP.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 6

Review the Application Control log.

```
1: date=2021-03-09 time=18:56:08 eventtime=1615344968811546102 tz="-0800" logid="1059028704" type="utm" subtype="app-ctrl" eventtype="signature"
level="information" vd="vd1" appid=49899 srcip=10.1.100.191 dstip=172.16.200.169 srcport=43946 dstport=771 srcintf="port10" srcintfrole="undefined"
dstintf="port9" dstintfrole="undefined" proto=6 service="RLDNP3" direction="outgoing" policyid=1 sessionid=1204 applist="test" action="pass"
appcat="Industrial" app="RealPort.DNP3_Confirm" incidentserialno=88083404 msg="Industrial: RealPort.DNP3_Confirm," clouduser="34 -> 34" filename="Null"
apprisk="elevated" cloudaction="Other"
```

Which configuration caused the IPS engine to generate this log?

```
config ips global
  set anomaly-mode continuous
end
```

A.

```
config ips global
  set exclude-signatures none
end
```

B.

```
config ips global
    set database extended
end
```

C.

```
config ips global
    set inspect-mode full
end
```

D.

Answer: B (LEAVE A REPLY)

<https://docs.fortinet.com/document/fortigate/7.0.2/administration-guide/419589/ips-configuration-options>

NEW QUESTION: 7

You are responsible for recommending an adapter type for NICs on a FortiGate VM that will run on an ESXi Hypervisor. Your recommendation must consider performance as the main concern, cost is not a factor.

Which adapter type for the NICs will you recommend?

- A. Native ESXi Networking with E1000
- B. Virtual Function (VF) PCI Passthrough
- C. Native ESXi Networking with VMXNET3
- D. Physical Function (PF) PCI Passthrough

Answer: D (LEAVE A REPLY)

The FortiGate VM is a virtual firewall appliance that can run on various hypervisors, such as ESXi, Hyper-V, KVM, etc. The adapter type for NICs on a FortiGate VM determines the performance and compatibility of the network interface cards with the hypervisor and the physical network. There are different adapter types available for NICs on a FortiGate VM, such as E1000, VMXNET3, SR-IOV, etc. If performance is the main concern and cost is not a factor, one option is to use native ESXi networking with VMXNET3 adapter type for NICs on a FortiGate VM that will run on an ESXi hypervisor. VMXNET3 is a paravirtualized network interface card that is optimized for performance in virtual machines and supports features such as multiqueue support, Receive Side Scaling (RSS), Large Receive Offload (LRO), IPv6 offloads, and MSI/MSI-X interrupt delivery. Native ESXi networking means that the FortiGate VM uses the standard virtual switch (vSwitch) or distributed virtual switch (dvSwitch) provided by the ESXi hypervisor to connect to the physical network.

This option can provide high performance and compatibility for NICs on a FortiGate VM without requiring additional hardware or software components. References:

<https://docs.fortinet.com/document/fortigate/7.0.0>

[/vm-installation-for-vmware-esxi/19662/installing-fortigate-vm-on-vmware-esxi](https://docs.fortinet.com/document/fortigate/7.0.0/vm-installation-for-vmware-esxi/19662/installing-fortigate-vm-on-vmware-esxi)<https://docs.fortinet.com>

[/document/fortigate/7.0.0/vm-installation-for-vmware-esxi/19662/networking](https://docs.fortinet.com/document/fortigate/7.0.0/vm-installation-for-vmware-esxi/19662/networking)

NEW QUESTION: 8

Refer to the exhibit, which shows diagnostic output.

```
FGT-SDW-1 # diagnose sys sdwan health-check status C2.NIC_DNS
Health Check(C2.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), health-
check(C2.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. Port1 is used because it has more available bandwidth.
- B. SD-WAN Rule is matching only DNS traffic.
- C. Route for the destination IP is missing in the routing table.
- D. Traffic is matched by policy route.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 9

Refer to the CLI output:

```
FortiWeb Security Service:
2022-01-03
Last Update Time: 2022-02-17 Method: Scheduled
Signature Build Number-0.00177
FortiWeb Antivirus Service:
2022-01-03
Last Update Time: 2022-02-17 Method: Scheduled
Regular Virus Database Version-42.00885
Extended Virus Database Version-42.00814
FortiWeb IP Reputation Service:
2022-01-03
Last Update Time: 2022-02-17 Method: Scheduled
Signature Build Number-3.00315
System files MD5SUM: 5660BD9FA1F6C86E8A31B2A139045F17
CLI files MD5SUM: 71BF206315679018536D9E19B37CBEAE
```

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

- A. Geographical IP policies are enabled and evaluated after local techniques.
- B. Attackers can be blocked before they target the servers behind the FortiWeb.
- C. The IP Reputation feature has been manually updated
- D. An IP address that was previously used by an attacker will always be blocked
- E. Reputation from blacklisted IP addresses from DHCP or PPPoE pools can be restored

Answer: B,E (LEAVE A REPLY)

The CLI output shown in the exhibit indicates that FortiWeb has enabled IP Reputation feature with local techniques enabled and geographical IP policies enabled after local techniques (set geoip-policy-order after- local). IP Reputation feature is a feature that allows FortiWeb to block or allow traffic based on the reputation score of IP addresses, which reflects their past malicious activities or behaviors. Local techniques are methods that FortiWeb uses to dynamically update its own blacklist based on its own detection of attacks or violations from IP addresses (such as signature matches, rate limiting, etc.). Geographical IP policies are rules that FortiWeb uses to block or allow traffic based on the geographical location of IP addresses (such as country, region, city, etc.). Therefore, based on the output, one correct statement is that attackers can be blocked before they target the servers behind the FortiWeb. This is because FortiWeb can use IP Reputation feature to block traffic from IP addresses that have a low reputation score or belong to a blacklisted location, which prevents them from reaching the servers and launching attacks. Another correct statement is that reputation from blacklisted IP addresses from DHCP or PPPoE pools can be restored. This is because FortiWeb can use local techniques to remove IP addresses from its own blacklist if they stop sending malicious traffic for a certain period of time (set local-techniques-expire-time), which allows them to regain their reputation and access the servers. This is useful for IP addresses that are dynamically assigned by DHCP or PPPoE and may change frequently. References:

<https://docs.fortinet.com/document/fortiweb/6.4.0/administration-guide/19662/ip-reputation>

<https://docs.fortinet.com/document/fortiweb/6.4.0/administration-guide/19662/geographical-ip-policies>

<https://docs.fortinet.com/document/fortiweb/7.4.2/administration-guide/608374/ip-reputation-blocklisting-source-ips-with-poor-reputation> Fortinet compiles a reputation for each public IP address. Clients will have poor reputations if they have been participating in attacks, willingly or otherwise. Because blacklisting innocent clients is equally undesirable, Fortinet also restores the reputations of clients that improve their behavior. This is crucial when an infected computer is cleaned, or in DHCP or PPPoE pools where an innocent client receives an IP address that was previously leased by an attacker.

NEW QUESTION: 10

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	1x 100/1000/2500 Base-T RJ45, 1 x 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 248E-FPOE
- B. 2x FortiSwitch 224E-POE
- C. 2x FortiSwitch 248E-FPOE
- D. 2x FortiSwitch 124E-FPOE

Answer: D (LEAVE A REPLY)

the access point will require about 24.5 W of power and the 124E-FPOE has a Capacity of about 370 meaning

$25 \times 12 = 300$ so you left with about 70 W on the switch meaning you can still add two more access point on that switch.

NEW QUESTION: 11

You are migrating the branches of a customer to FortiGate devices. They require independent routing tables on the LAN side of the network.

After reviewing the design, you notice the firewall will have many BGP sessions as you have two data centers (DC) and two ISPs per DC while each branch is using at least 10 internal segments. Based on this scenario, what would you suggest as the more efficient solution, considering that in the future the number of internal segments, DCs or internet links per DC will increase?

- A. No change in design is needed as even small FortiGate devices have a large memory capacity.
- B. Acquire a FortiGate model with more capacity, considering the next 5 years growth.
- C. Implement network-id, neighbor-group and increase the advertisement-interval
- D. Redesign the SD-WAN deployment to only use a single VPN tunnel and segment traffic using VRFs on BGP

Answer: D (LEAVE A REPLY)

<https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/810981/sd-wan-segmentation-over-a-single-overlay>

NEW QUESTION: 12

Refer to the exhibits.

Dictionary Profile

Name: Catch-All

Dictionary Entries

+ New... Edit... Delete

Records per page: 50 Total: 1

Enable	Pattern	Type	Weight	Maximum Weight	Enable Maximum Weight	Scan Area
☒	*	Wildcard	1	1	☒	Header

Recipient

Inbound Outbound

+ New... Clone... Edit... Delete Move Policy Lookup...

Records per page: 50 Domain: acme.com Show system policy

Search:

Total: 1

Enabled	ID	Domain Name	Sender Patte...	Recipient Pat...	AntiSpam	AntiVirus	Content	Resource
☒	1	acme.com	*@	*@acme.com	AS_Inbound	AV_Discard	CF_Inbound	Res_Default

Topology

Mail Server acme.com

FortiMail mail.acme.com

FortiSandbox

Internet

srv.thirdparty.com 100.64.0.72

The exhibits show a FortiMail network topology, Inbound configuration settings, and a Dictionary Profile.

You are required to integrate a third-party's host service (srv.thirdparty.com) into the e-mail processing path.

All inbound e-mails must be processed by FortiMail antispam and antivirus with FortiSandbox integration. If the email is clean, FortiMail must forward it to the third-party service, which will send the email back to FortiMail for final delivery, FortiMail must not scan the e-mail again.

Which three configuration tasks must be performed to meet these requirements? (Choose three.)

- A.** Change the scan order in FML-GW to antispam-sandbox-content.
- B.** Apply the Catch-Ail profile to the CFInbound profile and configure a content action profile to deliver to the srv. thirdparty. com FQDN
- C.** Create an access receive rule with a Sender value of srv. thirdparcy.com, Recipient value of *@acme.com, and action value of Safe
- D.** Apply the Catch-All profile to the ASinbound profile and configure an access delivery rule to deliver to the 100.64.0.72 host.

E. Create an IP policy with a Source value of 100.64.0.72/32, enable precedence, and place the policy at the top of the list.

Answer: A,B,E (LEAVE A REPLY)

* A is correct because the scan order must be changed to antispam-sandbox-content in order for FortiMail to scan the email for spam and viruses before forwarding it to the third-party service.

* B is correct because the Catch-All profile must be applied to the CFInbound profile in order for FortiMail to forward clean emails to the third-party service.

* E is correct because an IP policy must be created with a Source value of 100.64.0.72/32 in order to allow emails from the third-party service to be delivered to FortiMail.

The other options are not necessary to meet the requirements. Option C is not necessary because the access receive rule will already allow emails from the third-party service to be received by FortiMail. Option D is not necessary because the Catch-All profile already allows emails to be delivered to any destination.

Here are some additional details about integrating a third-party service into the FortiMail email processing path:

* The third-party service must be able to receive emails from FortiMail and send them back to FortiMail.

* The third-party service must be able to communicate with FortiMail using the SMTP protocol.

* The third-party service must be able to authenticate with FortiMail using the SMTP AUTH protocol.

Once the third-party service is integrated into the FortiMail email processing path, all inbound emails will be processed by FortiMail as usual. If the email is clean, FortiMail will forward it to the third-party service. The third-party service will then send the email back to FortiMail for final delivery. FortiMail will not scan the email again.

NEW QUESTION: 13

Refer to the exhibit.

```
config vpn ipsec phase1-interface
edit MyVPN1
    set remote-gw 1.2.3.4
    set interface {{WAN}}
    set peertype any
    set proposal aes256-sha256
    set psksecret Fortinet!!Fortinet
next
end
config vpn ipsec phase2-interface
edit MyVPN1
    set phase1name MyVPN1
    set proposal aes256-sha256
    set auto-negotiate enable
next
end
```

FortiManager is configured with the Jinja Script under CLI Templates shown in the exhibit.

Which two statements correctly describe the expected behavior when running this template?

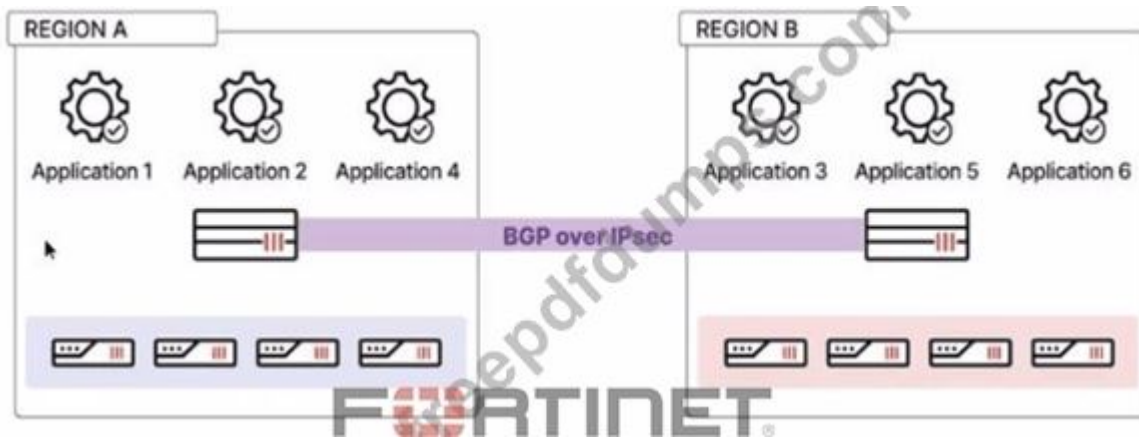
(Choose two.)

- A. The template will work if you change the variable format to \$(WAN).
- B. The template will work if you change the variable format to {{ WAN }}.
- C. The template will fail because this configuration can only be applied with a CLI or TCL script.
- D. The Jinja template will automatically map the interface with "WAN" role on the managed FortiGate.
- E. The administrator must first manually map the interface for each device with a meta field.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 14

Refer to the exhibit, which shows a multi-region SD-WAN architecture.



Given this scenario, which two statements are true? (Choose two.)

- A. If eBGP is used, ADVPN can be established only for branch-to-branch traffic within each region.
- B. If eBGP is used, ADVPN can be established for branch-to-branch traffic across regions.
- C. If iBGP is used, cross-regional spoke-to-hub shortcuts cannot be used.
- D. If iBGP is used, cross-regional spoke-to-hub shortcuts can be established.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 15

Refer to the exhibits.

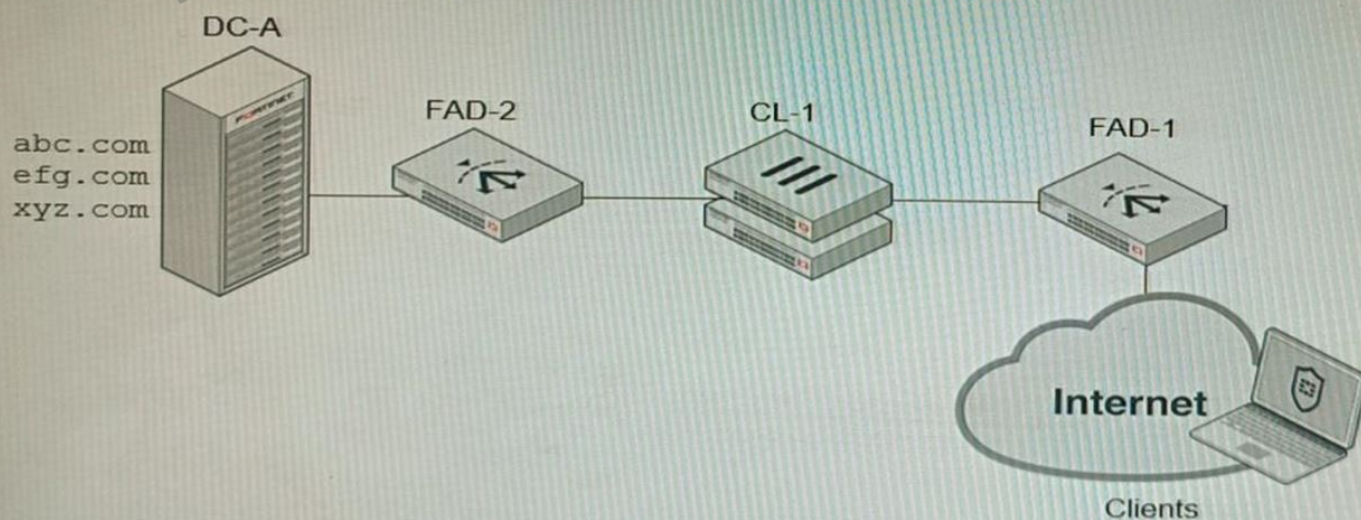
Configuration



```
config firewall profile-protocol-options
  edit "SSL-Offload"
    set comment "For FAD decrypted traffic"
    config http
      set ports 80
      unset options
      unset post-lang
    end
    config ftp
      set ports 21
      set options splice
    end
    config imap
      set ports 143
      set options fragmail
    end
    ...output omitted...
  next
end

config application list
  edit "SSL-Offload-App-Detect"
    set comment "App detect in decrypted traffic"
    config entries
      edit 1
        set action pass
      next
    end
  next
end
```

Topology



A FortiGate cluster (CL-1) protects a data center hosting multiple web applications. A pair of FortiADC devices are already configured for SSL decryption (FAD-1), and re-encryption (FAD-2). CL-1 must accept unencrypted traffic from FAD-1, perform application detection on the plain-text traffic, and forward the inspected traffic to FAD-2.

The SSL-Offload-App-Detect application list and SSL-Offload protocol options profile are applied to the firewall policy handling the web application traffic on CL-1.

Given this scenario, which two configuration tasks must the administrator perform on CL-1?

(Choose two.)

- ```
config firewall profile-protocol-options
 edit SSL-Offload
 config http
 set ssl-offloaded yes
 end
 next
end
```
- A.
- ```
config firewall profile-protocol-options
    edit SSL-Offload
        config http
            set options splice
        end
    next
end
```
- B.
- ```
config firewall ssl-server
 edit FAD-1
 set ip <FAD-1 IP address>
 set ssl-mode full
 next
end
```
- C.
- ```
config application list
    edit SSL-Offload-App-Detect
        set force-inclusion-ssl-di-sigs enable
    next
end
```
- D.
- ```
config application list
 edit SSL-Offload-App-Detect
 set deep-app-inspection enable
 next
end
```
- E.
- FORTINET**

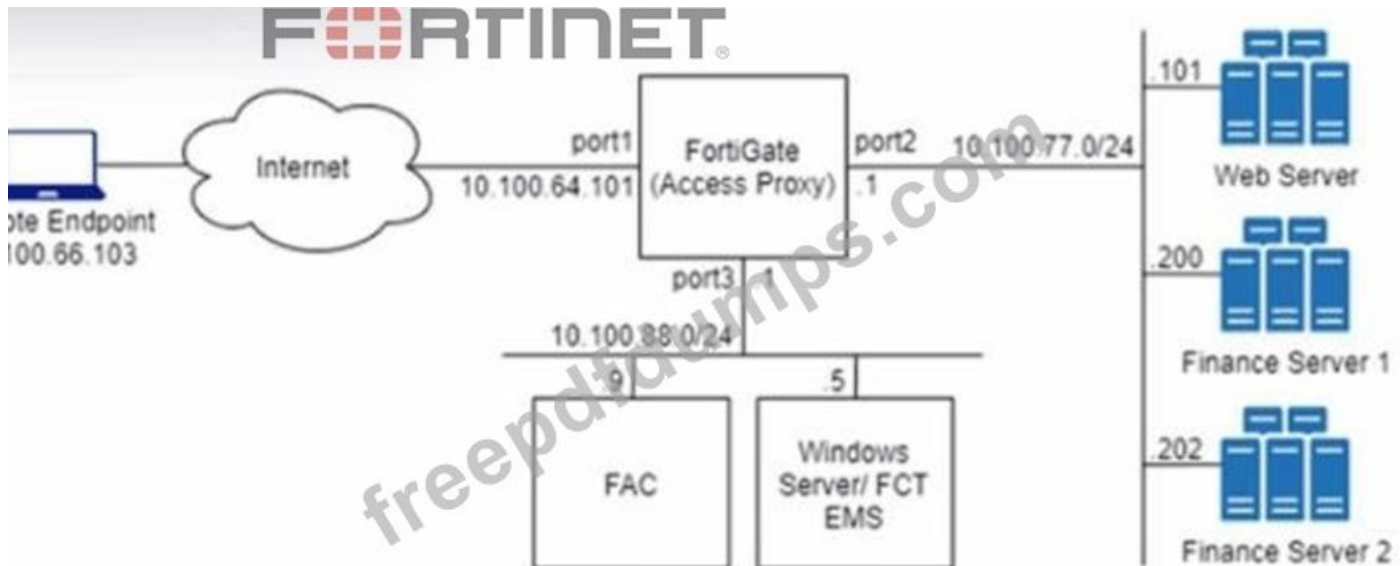
A. Option A

- B. Option D
- C. Option C
- D. Option B

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 16

Refer to the exhibit.



An HTTPS access proxy is configured to demonstrate its function as a reverse proxy on behalf of the web server it is protecting. It verifies user identity, device identity, and trust context, before granting access to the protected source. It is assumed that the FortiGate EMS fabric connector has already been successfully connected.

You need to ensure that ZTNA access through the FortiGate will redirect users to the FortiAuthenticator to perform username/password and multifactor authentication to validate access prior to accessing resources behind the FortiGate.

In this scenario, which two further steps need to be taken on the FortiGate? (Choose two.)

- A. Create a SAML user/server object referring to the FortiAuthenticator.
- B. Create a firewall rule that allows access from the remote endpoint to the resources behind the FortiGate.
- C. Create an authentication scheme with the "method" as SAML.
- D. Create an authentication rule that sets the sso-auth-method to the FortiAuthenticator.

Answer: A,C ([LEAVE A REPLY](#))

**Valid NSE8\_812 Dumps** shared by Actual4test.com for Helping Passing NSE8\_812 Exam!

Actual4test.com now offer the **newest NSE8\_812 exam dumps**, the Actual4test.com

NSE8\_812 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NSE8\_812 dumps with Test Engine here:

Special Discount: **Freepdfdumps**)

**NEW QUESTION: 17**

A FortiGate running FortiOS 7.2.0 GA is configured in multi-vdom mode with a vdom set to vdom type Admin and another vdom set to vdom type Traffic.

Which two GUI sections are available on both VDOM types? (Choose two.)

- A. FortiClient configuration
- B. Security Fabric topology and external connectors
- C. Certificates
- D. Packet capture
- E. Interface configuration

**Answer: D,E** ([LEAVE A REPLY](#))

**NEW QUESTION: 18**

On a FortiGate Configured in Transparent mode, which configuration option allows you to control Multicast traffic passing through the?

```
A. config system settings
 set multicast-skip-policy disable
end
```

```
B. config system settings
 set multicast-forward enable
end
```

```
C. config system settings
 set multicast-forward disable
end
```

```
D. config system settings
 set multicast-skip-policy enable
end
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A** ([LEAVE A REPLY](#))

When multicast-skip-policy is enabled, no check is performed based on multicast policy. A multicast packet received on an interface is flooded unconditionally to all interfaces (except the incoming interface) belonging to the same forwarding domain. Multicast packets are forwarded even when there is no multicast policy or the multicast policy is set to deny. To forward multicast traffic based on multicast policy, multicast-skip-policy must be disabled. In transparent mode, there is a per-VDOM configuration to skip policy check and forward all multicast traffic. This command is only available in transparent mode, and is disabled by default.

**NEW QUESTION: 19**

Which two types of interface have built-in active bypass in FortiDDoS devices? (Choose two.)

- A. SFP
- B. LC
- C. QSFP+
- D. Copper
- E. SFP+

**Answer: B,D** ([LEAVE A REPLY](#))

[https://help.fortinet.com/fddos/4-3-0/FortiDDoS/Built\\_in\\_bypass.htm](https://help.fortinet.com/fddos/4-3-0/FortiDDoS/Built_in_bypass.htm)

**NEW QUESTION: 20**

Refer to the exhibit that shows VPN debugging output.



A customer has deployed a FortiGate 300E with virtual domains (VDOMs) enabled in the multi-VDOM mode. There are three VDOMs: Root is for management and internet access, while VDOM 1 and VDOM 2 are used for segregating internal traffic. AccountVlnk and SalesVlnk are standard VDOM links in Ethernet mode.

Given the exhibit, which two statements below about VDOM behavior are correct? (Choose two.)

- A. The VDOM links are in Ethernet mode because they have IP addressed assigned on both sides.
- B. You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode
- C. Traffic on AccountVlnk and SalesVlnk will not be accelerated.
- D. Root VDOM is an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs.
- E. OSPF routing can be configured between VDOM 1 and Root VDOM without any configuration changes to AccountVlnk

**Answer: B,C** ([LEAVE A REPLY](#))

#### NEW QUESTION: 22

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 :00000000000000001833 [5b]
diag npu np6 dce 1
PDQ OSW EHPI :00000000000000000003 [80]
diag npu np6 dce 1
PDQ OSW EHP1 :00000000000000000552 [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** ([LEAVE A REPLY](#))

The diagnose command shown in the output is used to display information about NP6 packet descriptor queues. The output shows that there are 16 NP6 units in total, and each unit has four XAUI ports (XA0-XA3).

The output also shows that there are some non-zero values in the columns PDQ ACCU (packet descriptor queue accumulated counter) and PDQ DROP (packet descriptor queue drop counter). These values indicate that there are some packet descriptor queues that have reached their maximum capacity and have dropped some packets at the XAUI ports. This could be caused by congestion or misconfiguration of the XAUI ports or the ISF (Internal Switch Fabric). References: <https://docs.fortinet.com/document/fortigate/7.0.0/cli-reference/19662/diagnose-np6-pdq> The output is showing a packet descriptor queue accumulated counter, which is a measure of the number of packets that have been dropped by the NP6 due to congestion. The counter will increase if there are more packets than the NP6 can handle, which can happen if the bandwidth between the ISF and the NP is not sufficient or if the HPE shaper is enabled.

The output also shows that there are packet drops at the XAUI, which is the interface between the NP6 and the FortiGate's backplane. This means that the NP6 is not able to keep up with the traffic and is dropping packets.

The other statements are not true. Host-shortcut mode is not enabled, and enabling bandwidth control between the ISF and the NP will not change the output. HPE shaper is a feature that can be enabled to improve performance, but it will not change the output of the diagnose command.

Reference: <https://docs.fortinet.com/document/fortigate/7.4.0/hardware-acceleration/48875/diagnose-npu-np6-dce-np6-id-number-of-dropped-np6-packets>

### **NEW QUESTION: 23**

Refer to the exhibit.

```

data "vsphere_datacenter" "datacenter" {
 name = "dc-01"
}

data "vsphere_datastore" "datastore" {
 name = "datastore-01"
 datacenter_id =
data.vsphere_datacenter.datacenter.id
}

data "vsphere_compute_cluster" "cluster" {
 name = "cluster-01"
 datacenter_id =
data.vsphere_datacenter.datacenter.id
}

data "vsphere_network" "network" {
 name = "VM Network"
 datacenter_id =
data.vsphere_datacenter.datacenter.id
}

data "vsphere_virtual_machine" "template" {
 name = "FortiGate-VM-Vanilla"
 datacenter_id =
data.vsphere_datacenter.datacenter.id
}

resource "vsphere_virtual_machine" "vm" {
 name = "Test-FortiGate"
 resource_pool_id =
data.vsphere_compute_cluster.cluster.resource_pool_id

 datastore_id =
data.vsphere_datastore.datastore.id
 num_cpus = 1
 memory = 1024
 guest_id = "other3xLinux64Guest"
 network_interface {
 network_id = data.vsphere_network.network.id
 }
 dynamic "disk" {
 for_each =
data.vsphere_virtual_machine.template.disks
 content {
 label = "Disk${disk.key}"
 size = disk.value.size
 unit_number = disk.key
 }
 }

 clone {
 template_uuid =
data.vsphere_virtual_machine.template.id
 }
}

```

A customer wants to automate the creation and configuration of FortiGate VM instances in a VMware vCenter environment using Terraform. They have the creation part working with the code shown in the exhibit.

Which code snippet will allow Terraform to automatically connect to a newly deployed FortiGate if its IP was dynamically assigned by VMware NSX-T?

A.

```
provider "fortios" {
 hostname = vsphere_virtual_machine.vm.default_ip_address
 token = "jn3t3Nw7qckQzt955Htkfj5hwQ6jdb"
 insecure = "true"
}
```

B.

```
provider "fortinet_fortigate" {
 hostname = vsphere_virtual_machine.vm.default_ip_address
 token = "jn3t3Nw7qckQzt955Htkfj5hwQ6jdb"
 insecure = "true"
}
```

C.

```
provider "fortinet_fortigate" {
 hostname = module.vsphere_virtual_machine.default_ip_address
 token = "jn3t3Nw7qckQzt955Htkfj5hwQ6jdb"
 insecure = "true"
```

```
provider "fortios" {
 hostname = module.vsphere_virtual_machine.default_ip_address
 token = "jn3t3Nw7qckQzt955Htkfj5hwQ6jdb"
 insecure = "true"
}
```

D.

Answer: A ([LEAVE A REPLY](#))

## NEW QUESTION: 24

A customer has FortiAP devices in three branch offices managed from a FortiGate in the HQ. Each FortiAP is connected to a dedicated management VLAN.

The customer wants the users connected to the FortiAP SSIDs to use the branch local internet connection, but each branch uses a different VLAN ID for the bridge. HQ users travel to different branches and connect to the same SSID.

Which configuration option will solve this requirement?

A. Set each FortiAP to a wtp-group and use set vlan-pooling wtp-group on the VAP configuration with the corresponding VLAN ID configuration for each group.

**B.** Set a FortiAuthenticator for 802.1x authentication with the Tunnel-Type attribute set to VLAN and use set dynamic-vlan enable on the VAP configuration.

**C.** Use set vlan-pooling hash on the VAP configuration with the corresponding vlan-pool.

**D.** Use set vlan-pooling round-robin on the VAP configuration with the corresponding vlan-pool.

**Answer: B** ([LEAVE A REPLY](#))

#### **NEW QUESTION: 25**

You are performing a packet capture on a FortiGate 2600F with the hyperscale licensing installed. You need to display on screen all egress/ingress packets from the port16 interface that have been offloaded to the NP7.

Which three commands need to be run? (Choose three.)

**A.** diagnose npu sniffer filter selector 0

**B.** diagnose sniffer packet port16

**C.** diagnose npu sniffer filter dir 2

**D.** diagnose sniffer packet npudbg

**E.** diagnose npu sniffer filter intf port16

**Answer: C,D,E** ([LEAVE A REPLY](#))

#### **NEW QUESTION: 26**

Refer to the exhibit.

The screenshot shows the FortiManager interface. The top section displays four administrators:

| Administrator | Type  | Profile            | ADOMs     | Policy Packages |
|---------------|-------|--------------------|-----------|-----------------|
| admin         | LOCAL | Super_User         | All ADOMs | All Packages    |
| CISO          | LOCAL | Read_Only_User     | All ADOMs | All Packages    |
| Mary          | LOCAL | Standard_User      | All ADOMs | All Packages    |
| CTO           | LOCAL | No_Permission_User | All ADOMs | All Packages    |

The bottom section shows the 'Workspace Settings' for the 'Workflow' mode. The 'Workflow Approvals' table is as follows:

| ADOM Name   | Group #1    | Group #2 | Email Notification |
|-------------|-------------|----------|--------------------|
| root        | CISO, admin |          | CTO                |
| Workflow_72 | CISO, admin | CTO      | Mary               |

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 CISO must have a higher access level than "Read\_Only\_User" in FortiManager.
- B. The CTO must have a defined email address for their admin user account.
- C. The CTO must have Standard access level or higher for FortiManager.
- D. The CTO needs to be added to "Email Notification" in the Workflow\_72 ADOM.
- E. The CTO and CISO need to swap Approval Groups so that the highest authority is in Group #1.

**Answer: B,C** ([LEAVE A REPLY](#))

## NEW QUESTION: 27

Refer to the exhibit showing an SD-WAN configuration.

```

edit 3
 set interface "port15"
 set zone "z1"
 set gateway 172.16.209.2
next
edit 4
 set interface "port16"
 set zone "z1"
 set gateway 172.16.210.2
next
end
config health-check
 edit "1"
 set server "10.1.100.2"
 set members 4 3 2 1
 config sla
 edit 1
end
config service
 edit 1
 set name "1"
 set mode sla
 set dst "all"
 set src "172.16.205.0"
 config sla
 edit "1"
 set id 1
 next
 end
 set priority-members 1 2 3 4
 set tie-break fib-best-match
 next
end
end

```

```
#####
```

```
FGT_A (root) # diagnose sys sdwan service
```

```

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-
compare-order
 Members(4):
 1: Seq_num(1 port1), alive, sla(0x1), gid(0), cfg_order(0),
cost(0), selected
 2: Seq_num(2 dmz), alive, sla(0x1), gid(0), cfg_order(1),
cost(0), selected
 3: Seq_num(3 port15), alive, sla(0x1), gid(0), cfg_order(2),
cost(0), selected
 4: Seq_num(4 port16), alive, sla(0x1), gid(0), cfg_order(3),
cost(0), selected
 Src address(1):
 172.16.205.0-172.16.205.255
 Dst address(1):
 0.0.0.0-255.255.255.255

```

```
#####
```

```
FGT_A (root) # get router info routing-table static
```

```

Routing table for VRF=0
S* 0.0.0.0/0 [1/0] via 172.16.200.2, port1
 [1/0] via 172.16.208.2, dmz
 [1/0] via 172.16.209.2, port15
 [1/0] via 172.16.210.2, port16
S 10.1.100.22/32 [10/0] via 172.16.209.2, port15
 [10/0] via 172.16.210.2, port16

```

According to the exhibit, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, which outgoing interfaces will be used?

- A. port16 and port1
- B. port1 and port1
- C. port16 and port15
- D. port1 and port15

**Answer: D** ([LEAVE A REPLY](#))

<https://docs.fortinet.com/document/fortigate/7.2.8/administration-guide/686587/ecmp-support-for-the-longest-match-in-sd-wan-rule-matching>

### NEW QUESTION: 28

Refer to the exhibit showing a FortiView monitor screen.



After a Secure SD-WAN implementation a customer reports that in FortiAnalyzer under FortiView Secure SD-WAN Monitor there is No Device for selection.

What can cause this issue?

- A. sla-fail-log-period and sla-pass-log-period on FortiGate health check is not set.
- B. Upload option from FortiGate to FortiAnalyzer is not set as a real time.
- C. ADOM 1 is set as a Fabric ADOM.
- D. Extended logging is not enabled on FortiGate.

**Answer: B** ([LEAVE A REPLY](#))

### NEW QUESTION: 29

Refer to the exhibits.

GUI Access

Site title: FortiAuthenticator

GUI idle timeout: 480 minutes (1-480 mins)

Maximum HTTP header length: 4 (4-16 KB)

HTTPS Certificate: Default-Server-Certificate | CN=Default-Server-Certificate-7D895AD8

☐ HTTP Strict Transport Security (HSTS) Expiry

Certificate authority type: Local CA **Trusted CA**

CA certificate that issued the server certificate: Fortinet\_CA1\_Root | emailAddress=support@fortinet.com

☒ Allow all hosts/domain names

Public IP/FQDN for FortiToken Mobile: 100.64.1.76

Configuration

```
FG-1 # show system ftm-push
config system ftm-push
 set server-cert "self-sign"
 set server "10.0.1.150"
 set status enable
end

FG-1# show system interface port1
config system interface
 edit "port1"
 set vdom "root"
 set ip 100.64.1.41 255.255.255.0
 set allowaccess ping
 set type physical
 set alias "WAN"
 set role wan
 set snmp-index 1
 next
end
```

Topology

An administrator has configured a FortiGate and Forti Authenticator for two-factor authentication with FortiToken push notifications for their SSL VPN login. Upon initial review of the setup, the administrator has discovered that the customers can manually type in their two-factor code and authenticate but push notifications do not work. Based on the information given in the exhibits, what must be done to fix this?

- A. On FG-1 port1, the ftm access protocol must be enabled.
- B. FAC-1 must have an internet routable IP address for push notifications.
- C. On FG-1 CLI, the ftm-push server setting must point to 100.64.141.
- D. On FAC-1, the FortiToken public IP setting must point to 100.64.1.41

**Answer:** (SHOW ANSWER)

<https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-FortiToken-Push-on->

### NEW QUESTION: 30

A remote IT Team is in the process of deploying a FortiGate in their lab. The closed environment has been configured to support zero-touch provisioning from the FortiManager, on the same network, via DHCP options. After waiting 15 minutes, they are reporting that the FortiGate received an IP address, but the zero-touch process failed.

The exhibit below shows what the IT Team provided while troubleshooting this issue:

```
FGT # diagnose fdsm fmg-auto-discovery-status
dhcp: fmg-ip=172.18.60.115, fmg-domain-name='', config-touched=1(/bin/dhcpd)
```

Which statement explains why the FortiGate did not install its configuration from the FortiManager?

- A. The FortiGate was not configured with the correct pre-shared key to connect to the FortiManager
- B. The DHCP server was not configured with the FQDN of the FortiManager
- C. The DHCP server used the incorrect option type for the FortiManager IP address.
- D. The configuration was modified on the FortiGate prior to connecting to the FortiManager

**Answer: D** ([LEAVE A REPLY](#))

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-perform-zero-touch-provisioning-with/ta-p/197623>

### NEW QUESTION: 31

A remote worker requests access to an SSH server inside the network. You deployed a ZTNA Rule to their FortiClient. You need to follow the security requirements to inspect this traffic.

Which two statements are true regarding the requirements? (Choose two.)

- A. FortiGate can perform SSH access proxy host-key validation.
- B. You need to configure a FortiClient SSL-VPN tunnel to inspect the SSH traffic.
- C. SSH traffic is tunneled between the client and the access proxy over HTTPS
- D. Traffic is discarded as ZTNA does not support SSH connection rules

**Answer: (**[SHOW ANSWER](#)**)**

ZTNA supports SSH connection rules that allow remote workers to access SSH servers inside the network through an HTTPS tunnel between the client and the access proxy (FortiGate). The access proxy acts as an SSH client to connect to the real SSH server on behalf of the user, and performs host-key validation to verify the identity of the server. The user can use any SSH client that supports HTTPS proxy settings, such as PuTTY or OpenSSH.

References:<https://docs.fortinet.com/document/fortigate/7.0.0/ztna-deployment/899992/configuring-ztna-rules-to-control-access>

<https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/29927/ztna-ssh-access-proxy-example>

**Valid NSE8\_812 Dumps** shared by Actual4test.com for Helping Passing NSE8\_812 Exam! Actual4test.com now offer the **newest NSE8\_812 exam dumps**, the Actual4test.com NSE8\_812 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NSE8\_812 dumps with Test Engine here:

[https://www.actual4test.com/NSE8\\_812\\_examcollection.html](https://www.actual4test.com/NSE8_812_examcollection.html) (107 Q&As Dumps, **30%OFF**

**Special Discount: Freepdfdumps)**

#### NEW QUESTION: 32

An administrator discovers that CPU utilization of a FortiGate-200F is high and determines that no traffic is being accelerated by hardware.

Why is no traffic being accelerated by hardware?

- A. strict-dirty-session-check is enabled in global config.
- B. Oper-session-accounting is enabled under np6xlite config.
- C. delay-tcp-npu-session is enabled under the firewall policy.
- D. check-protocol-header is set to strict in the global config.

**Answer:** ([SHOW ANSWER](#))

#### NEW QUESTION: 33

A customer wants to use the FortiAuthenticator REST API to retrieve an SSO group called SalesGroup. The following API call is being made with the 'curl' utility:

```
curl -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS" -X PUT -d '{"name":"SalesGroup"}' -H 'Content-Type: application/json' https://10.10.10.22/api/v1/ssogroup/100/
```

Which two statements correctly describe the expected behavior of the FortiAuthenticator REST API? (Choose two.)

- A. Only users with the "Full permission" role can access the REST API
- B. This API call will fail because it requires that API version 2
- C. If the REST API web service access key is lost, it cannot be retrieved and must be changed.
- D. The syntax is incorrect because the API calls needs the get method.

**Answer: B,D** ([LEAVE A REPLY](#))

To retrieve an SSO group called SalesGroup using the FortiAuthenticator REST API, the following issues need to be fixed in the API call:

\* The API version should be v2, not v1, as SSO groups are only supported in version 2 of the REST API.

\* The HTTP method should be GET, not POST, as GET is used to retrieve information from the server, while POST is used to create or update information on the server. Therefore, a correct API call would look like this: curl -X GET -H "Authorization: Bearer <token>"

<https://fac.example.com/api/v2/sso>

/groups/SalesGroup References: <https://docs.fortinet.com/document/fortiauthenticator/6.4.1/rest-api-solution-guide/927311/sso-groups>

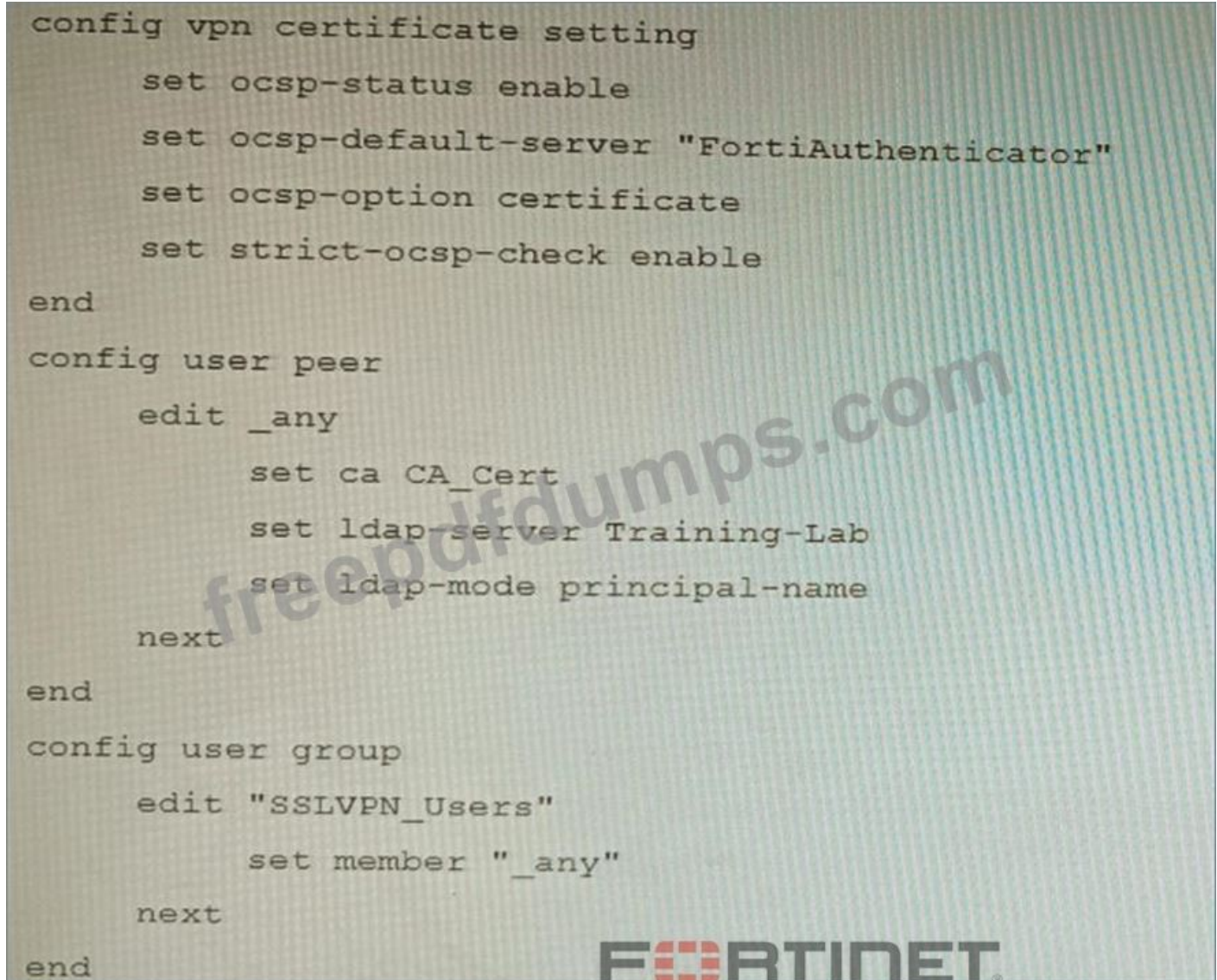
### NEW QUESTION: 34

An administrator has configured a FortiGate device to authenticate SSL VPN users using digital certificates.

A FortiAuthenticator is the certificate authority (CA) and the Online Certificate Status Protocol (OCSP) server.

Part of the FortiGate configuration is shown below:

```
config vpn certificate setting
 set ocsp-status enable
 set ocsp-default-server "FortiAuthenticator"
 set ocsp-option certificate
 set strict-ocsp-check enable
end
config user peer
 edit _any
 set ca CA_Cert
 set ldap-server Training-Lab
 set ldap-mode principal-name
 next
end
config user group
 edit "SSLVPN_Users"
 set member "_any"
 next
end
```

A screenshot of a FortiGate configuration interface showing the configuration for SSL VPN users. The configuration is displayed in a terminal-like window with a light blue background. The text is in a monospaced font. A large, semi-transparent watermark "freedumps.com" is overlaid diagonally across the middle of the configuration. At the bottom right, the "FORTINET" logo is visible in a bold, sans-serif font.

Based on this configuration, which two statements are true? (Choose two.)

- A. OCSP checks will always go to the configured FortiAuthenticator
- B. The OCSP check of the certificate can be combined with a certificate revocation list.
- C. OCSP certificate responses are never cached by the FortiGate.
- D. If the OCSP server is unreachable, authentication will succeed if the certificate matches the CA.

**Answer: A,B** ([LEAVE A REPLY](#))

References:

Configuring SSL VPN authentication using digital certificates | FortiGate / FortiOS 7.2.0 - Fortinet Document Library  
Online Certificate Status Protocol (OCSP) | FortiGate / FortiOS 7.2.0 - Fortinet Document Library  
Certificate Revocation Lists (CRLs) | FortiGate / FortiOS 7.2.0 - Fortinet Document Library

### NEW QUESTION: 35

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, priority: 0, weight: 0
Member(2): interface: wan2, priority: 0, weight: 0
```

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

- A. wan2 is currently used as an outgoing interface.
- B. wan1 is currently used as an outgoing interface.
- C. Packet-loss is the quality criteria.
- D. Latency is the quality criteria.

**Answer:** ([SHOW ANSWER](#))

### NEW QUESTION: 36

Refer to the exhibits.

## FortiSandbox

**FortiSandbox**

FortiSandbox Inspection ☒ Statistics...

FortiSandbox type: Appliance Cloud **Enhanced Cloud**

Server name/IP:

Notification email:

Statistics interval:  (minutes)

Scan timeout:  (minutes)

Scan result expires in:  (minutes)

## AV Profile

AntiVirus Profile

☒ FortiSandbox

Scan mode: Submit and wait for result **Submit only**

☒ Attachment analysis

|                 |                     |          |           |
|-----------------|---------------------|----------|-----------|
| Malicious/Virus | Action: --Default-- | + New... | ✕ Edit... |
| High risk       | Action: --Default-- | + New... | ✕ Edit... |
| Medium risk     | Action: --Default-- | + New... | ✕ Edit... |
| Low risk        | Action: --Default-- | + New... | ✕ Edit... |
| No Result       | Action: --None--    | + New... | ✕ Edit... |

☐ URL analysis

|                 |                     |          |           |
|-----------------|---------------------|----------|-----------|
| Malicious/Virus | Action: --Default-- | + New... | ✕ Edit... |
| High risk       | Action: --Default-- | + New... | ✕ Edit... |
| Medium risk     | Action: --Default-- | + New... | ✕ Edit... |
| Low risk        | Action: --Default-- | + New... | ✕ Edit... |
| No Result       | Action: --None--    | + New... | ✕ Edit... |

You must integrate a FortiMail and FortiSandbox Enhanced Cloud solution for a customer who is concerned about the e-mails being delayed for too long.

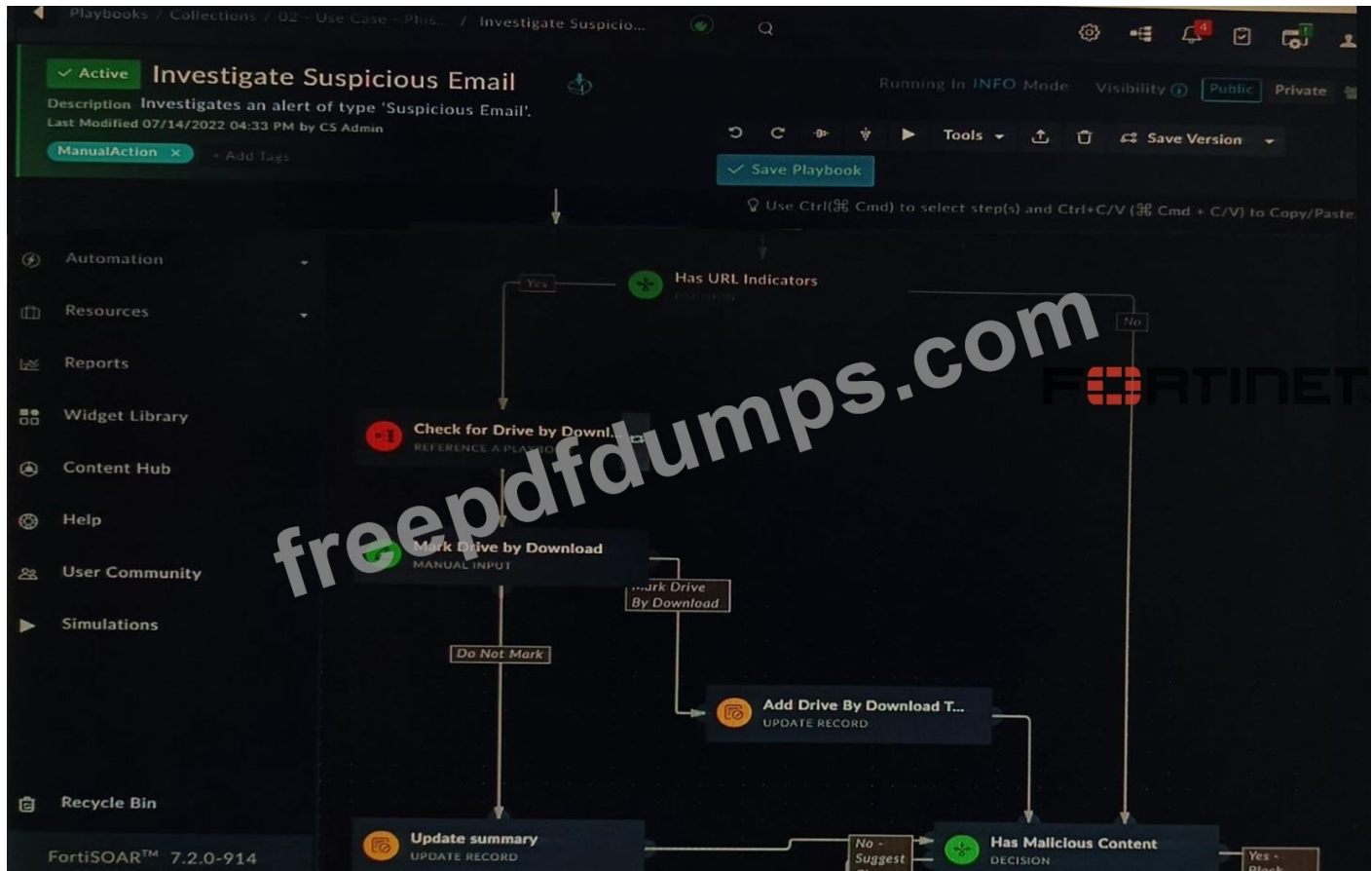
According to the configuration shown in the exhibits, which would be an expected behavior?

- A.** FortiMail will ignore the timeout value if content disarm and reconstruction (CDR) is enabled.
- B.** If an attachment is sent to the FortiSandbox while the job queue is full, the e-mail might be delayed for up to 30 minutes, then e-mail will be relayed to the mail server.
- C.** FortiMail will not wait for results but only for attachments that have been already submitted to the FortiSandbox in the last 60 minutes.
- D.** FortiMail will relay valid e-mails to the mail server as soon as it is done with other local inspections.

**Answer:** ([SHOW ANSWER](#))

## NEW QUESTION: 37

Refer to the exhibit showing a FortiSOAR playbook.



You are investigating a suspicious e-mail alert on FortiSOAR, and after reviewing the executed playbook, you can see that it requires intervention.

What should be your next step?

- A. Go to the Incident Response tasks dashboard and run the pending actions
- B. Click on the notification icon on FortiSOAR GUI and run the pending input action
- C. Run the Mark Drive by Download playbook action
- D. Reply to the e-mail with the requested Playbook action

**Answer: A** ([LEAVE A REPLY](#))

The exhibited playbook requires intervention, which means that the playbook has reached a point where it needs a human operator to take action. The next step should be to go to the Incident Response tasks dashboard and run the pending actions. This will allow you to see the pending actions that need to be taken and to take those actions.

The other options are not correct. Option B will only show you the notification icon, but it will not allow you to run the pending input action. Option C will run the Mark Drive by Download playbook action, but this is not the correct action to take in this case. Option D is not a valid option.

Here are some additional details about pending actions in FortiSOAR:

Pending actions are actions that need to be taken by a human operator.

Pending actions are displayed in the Incident Response tasks dashboard.

Pending actions can be run by clicking on the action in the dashboard.

## NEW QUESTION: 38

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

Configuration

```
config firewall policy
 edit 1
 set name "DC-1-Traffic-In"
 set srcintf "port1"
 set dstintf "port2"
 set srcaddr "all"
 set dstaddr "DC-1-VIP-GRP"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set ssl-ssh-profile "DC1-Certs"
 set av-profile "servers"
 set webfilter-profile "servers"
 set logtraffic all
 next
end

config firewall ssl-ssh-profile
 edit "DC1-Certs"
 config https
 set ports 443
 set status deep-inspection
 end
 ...omitted output...
 set server-cert-mode replace
 set server-cert "abc" "efg"
 set supported-alpn http2
 next
end
```

Topology

The diagram illustrates a network topology. On the left, a server rack labeled 'DC-1' is shown with the domain names 'abc.com', 'efg.com', and 'xyz.com' listed below it. A line connects DC-1 to a FortiGate device labeled 'FG-1' at 'port2'. Another line connects FG-1 to a cloud labeled 'Internet' at 'port1'. A laptop icon labeled 'Clients' is shown within the Internet cloud. A large 'FORTINET' logo is visible in the background of the configuration section.

An administrator has configured an inbound SSL inspection profile on a FortiGate device (FG-1) that is protecting a data center hosting multiple web pages-Given the scenario shown in the exhibits, which certificate will FortiGate use to handle requests to xyz.com?

- A. FortiGate will fall-back to the default Fortinet\_CA\_SSL certificate.
- B. FortiGate will reject the connection since no certificate is defined.
- C. FortiGate will use the Fortinet\_CA\_Untrusted certificate for the untrusted connection,
- D. FortiGate will use the first certificate in the server-cert list-the abc.com certificate

**Answer: (SHOW ANSWER)**

<https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/850344/define-multiple-certificates-in-an-ssl-profile-in-replace-mode> If there is no matched server certificate in the list, then the first server certificate in the list is used as a replacement.

### **NEW QUESTION: 39**

A customer's cybersecurity department needs to implement security for the traffic between two VPCs in AWS, but these belong to different departments within the company. The company uses a single region for all their VPCs.

Which two actions will achieve this requirement while keeping separate management of each department's VPC? (Choose two.)

- A.** Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster.
- B.** Migrate all the instances to the same VPC and create IAM accounts for each department, then implement a new subnet for a FortiGate auto-scaling group and use routing tables to force the traffic through the FortiGate cluster.
- C.** Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPC to force routing through the FortiGate cluster
- D.** Create an IAM account for the cybersecurity department to manage both existing VPC, create a FortiGate HA Cluster on each VPC and IPSEC VPN to force traffic between the VPCs through the FortiGate clusters

**Answer: (SHOW ANSWER)**

To implement security for the traffic between two VPCs in AWS, while keeping separate management of each department's VPC, two possible actions are:

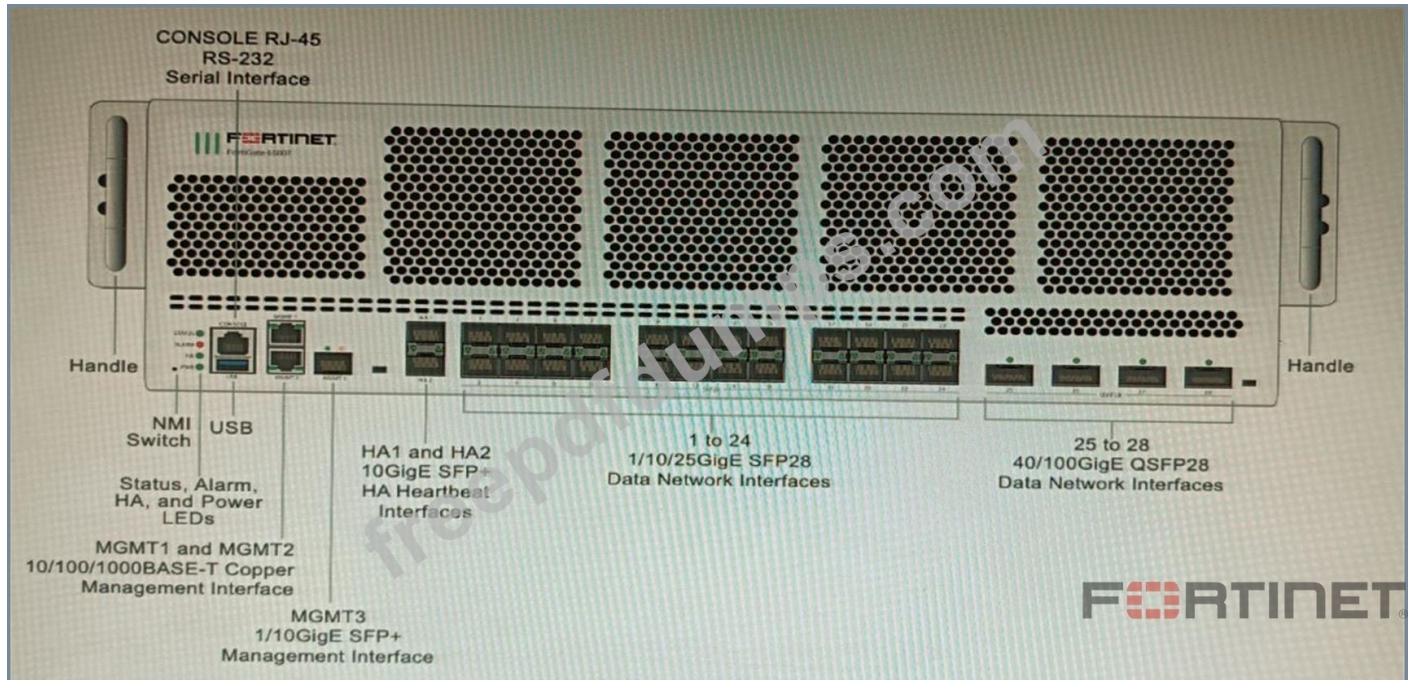
- \* Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster. This option allows the cybersecurity department to manage the transit VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The VPC peering connections enable direct communication between the VPCs without using public IPs or gateways. The routing tables can be configured to direct all inter-VPC traffic to the transit VPC.
- \* Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPCs to force routing through the FortiGate cluster. This option also allows the cybersecurity department to manage the security VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The Transit Gateway acts as a network hub that connects multiple VPCs and on-premises networks. The routing tables can be configured to direct all inter-VPC traffic to the security VPC. References:

<https://docs.fortinet.com/document/fortigate-public-cloud/7.2.0/aws-administration-guide/506140/connecting-a-local-fortigate-to-an-aws-vpc-vpn>

<https://docs.fortinet.com/document/fortigate-public-cloud/7.0.0/sd-wan-architecture-for-enterprise/166334/sd-wan-configuration>

### NEW QUESTION: 40

Refer to the exhibit.



You are deploying a FortiGate 6000F. The device should be directly connected to a switch. In the future, a new hardware module providing higher speed will be installed in the switch, and the connection to the FortiGate must be moved to this higher-speed port.

You must ensure that the initial FortiGate interface connected to the switch does not affect any other port when the new module is installed and the new port speed is defined.

How should the initial connection be made?

- A. Connect the switch on any interface between ports 21 to 24
- B. Connect the switch on any interface between ports 25 to 28
- C. Connect the switch on any interface between ports 1 to 4
- D. Connect the switch on any interface between ports 5 to 8.

**Answer: (SHOW ANSWER)**

Reference:

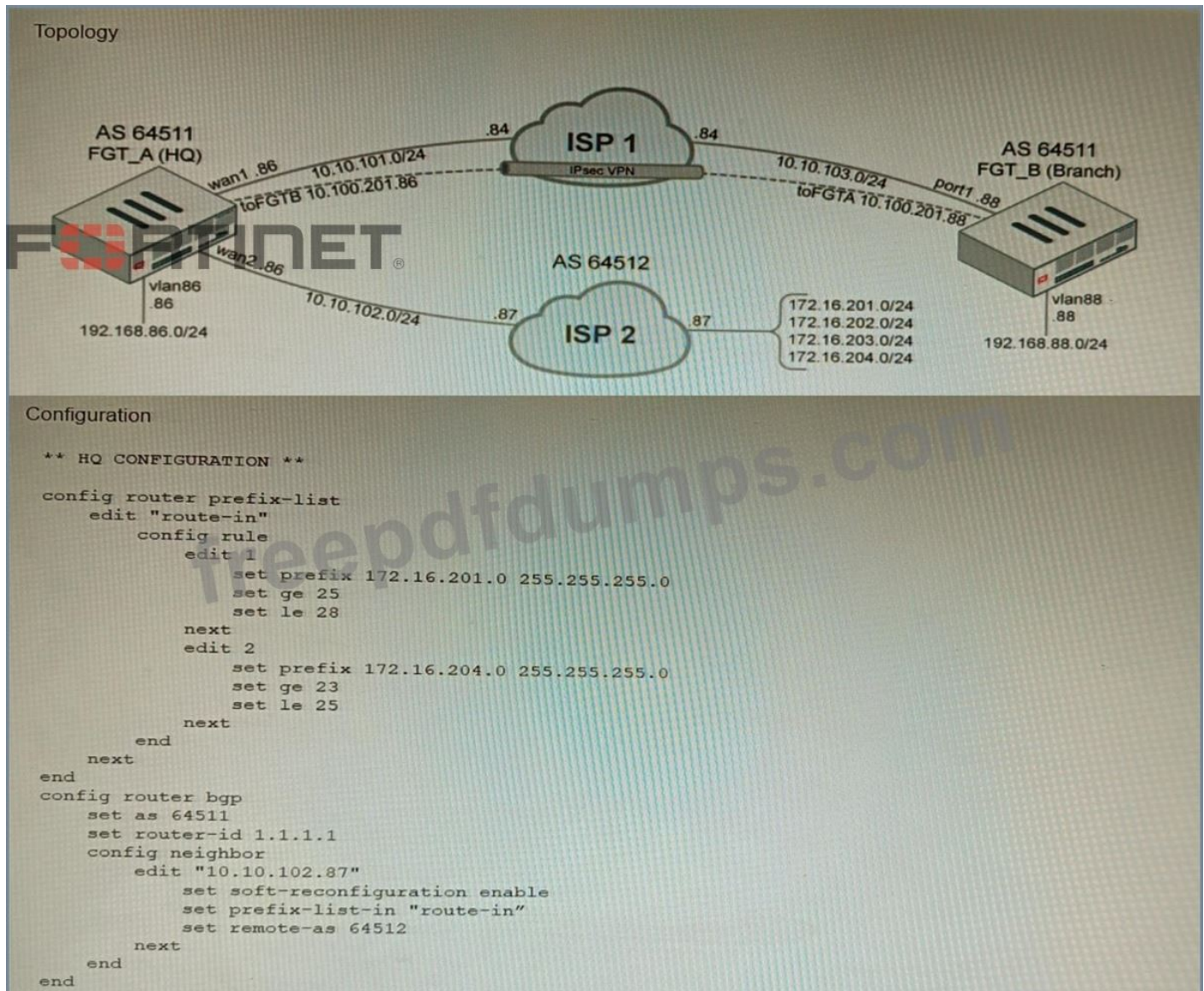
FortiGate 6000F Front Panel Interfaces:

<https://docs.fortinet.com/document/fortigate-6000/hardware/fortigate-6000f-system-guide/827055/front-panel-interfaces>

<https://docs.fortinet.com/document/fortigate-6000/7.0.12/fortigate-6000-handbook/633498/interface-groups-and-changing-data-interface-speeds>

### NEW QUESTION: 41

Refer to the exhibits.



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. 172.620.64.27
- D. 172.16.204.64/27

**Answer: A,D (LEAVE A REPLY)**

The prefix list in the exhibit is configured to match prefixes that are either in the 172.16.204.0/24 subnet or in the 172.62.0.0/16 subnet. The routes that match these prefixes will be active in the routing table on the HQ firewall.

The routes that match the following prefixes will not be active in the routing table:

- \* 172.16.201.96/29
- \* 172.62.0.64/27

These routes do not match the criteria set by the prefix list.

References:

Prefix lists | FortiGate / FortiOS 7.4.0 - Fortinet Document Library

Configuring BGP | FortiGate / FortiOS 7.4.0 - Fortinet Document Library

### NEW QUESTION: 42

Refer to the exhibit.



The exhibit shows the topology a customer wants to implement using a flexible authentication scheme. Users connecting from trusted remote locations are authenticated using only their username/password when connecting to the SSLVPN FortiGate in the data center.

When connecting from the Untrusted Clients, users must authenticate using 2-factor authentication.

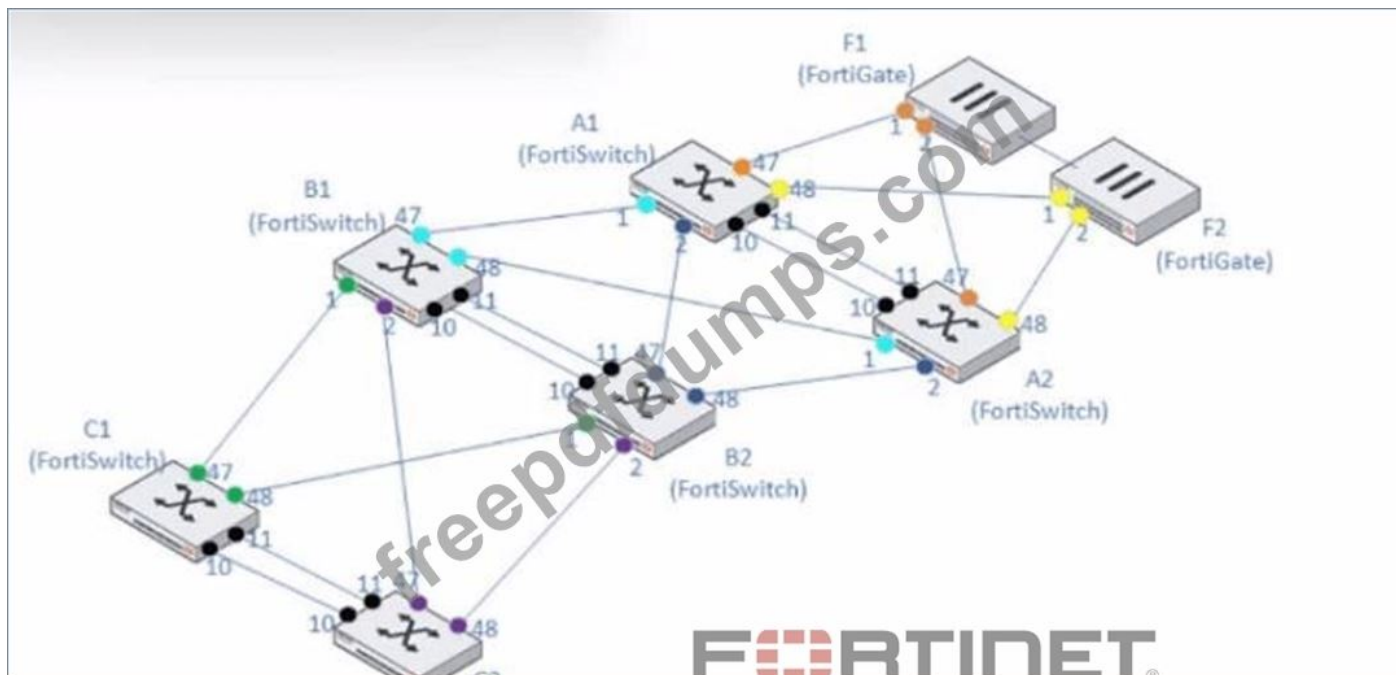
In this scenario, which RADIUS attribute can be used as a RADIUS policy selector on the FortiAuthenticator to accomplish this goal?

- A. Tunnel-Client-Auth-Id
- B. Login-IP-Host
- C. Framed-IP-Address
- D. Calling-Station-Id

**Answer: A** ([LEAVE A REPLY](#))

### NEW QUESTION: 43

Refer to the exhibit.



A customer needs to create a multi-tier MCLAG set up with the topology as shown in the exhibit.

A1/A2

B1/B2

C1/C2

Which command snippet should be applied to it, to allow active/active links in this topology?

```
A1 # config switch auto-isl-port-group
A1 (auto-isl-port-g~o) # edit aggregate-port10-11
A1 (aggregate-port10-11) # set members port10 port11
A1 (aggregate-port10-11) # next
A1 (auto-isl-port-g~o) # end

A2 # config switch auto-isl-port-group
A2 (auto-isl-port-g~o) # edit aggregate-port10-11
A2 (aggregate-port10-11) # set members port10 port11
A2 (aggregate-port10-11) # next
```

A.

B.

```

○A1 # config switch auto-is1-port-group
 A1 (auto-is1-port-g~o) # edit aggregate-port1
 A1 (aggregate-port1) # set members port1
 A1 (aggregate-port1) # next
 A1 (auto-is1-port-g~o) # end

 A1 # config switch auto-is1-port-group
 A1 (auto-is1-port-g~o) # edit aggregate-port2
 A1 (aggregate-port2) # set members port2
 A1 (aggregate-port2) # next
 A1 (auto-is1-port-g~o) # end

```

```

A1 # config switch auto-is1-port-group
A1 (auto-is1-port-g~o) # edit aggregate-port1
A1 (aggregate-port1) # set members port1
A1 (aggregate-port1) # next
A1 (auto-is1-port-g~o) # end

A1 # config switch auto-is1-port-group
A1 (auto-is1-port-g~o) # edit aggregate-port2
A1 (aggregate-port2) # set members port2
A1 (aggregate-port2) # next
A1 (auto-is1-port-g~o) # end

```

C.

```

A1 # config switch auto-is1-port-group
A1 (auto-is1-port-g~o) # edit aggregate-port10
A1 (aggregate-port10) # set members port10
A1 (aggregate-port10) # next
A1 (auto-is1-port-g~o) # end

A1 # config switch auto-is1-port-group
A1 (auto-is1-port-g~o) # edit aggregate-port11
A1 (aggregate-port11) # set members port11
A1 (aggregate-port11) # next
A1 (auto-is1-port-g~o) # end

```

D.

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 44**

You are creating the CLI script to be used on a new SD-WAN deployment. You will have branches with a different number of internet connections and want to be sure there is no need to change the Performance SLA configuration in case more connections are added to the branch.

The current configuration is:

```
config health-check
 edit "Default_AWS"
 set server "aws.amazon.com"
 set protocol http
 set interval 1000
 set probe-timeout 1000
 set recoverytime 10
 config sla
 edit 1
 set latency-threshold 250
 set jitter-threshold 50
 set packetloss-threshold 5
 next
 end
 next
end
```

Which configuration do you use for the Performance SLA members?

- A. set members any
- B. set members 0
- C. current configuration already fulfills the requirement
- D. set members all

Answer: B ([LEAVE A REPLY](#))

References:

Performance SLA | FortiGate / FortiOS 7.4.0

### NEW QUESTION: 45

Refer to the exhibit.

```
FGT # get router info bgp network 10.10.10.0
Paths: (2 available, no best path)
Local
10.20.1.4 (inaccessible) from 10.21.16.15 (10.21.116.20)
Local
10.20.1.4 (inaccessible) from 10.21.16.16 (10.21.116.20)

FGT # get router info routing-table details 10.20.1.4
Routing entry for 10.20.1.0/28
Known via "bgp", distance 200, metric 0, best
Last update 07w2d18h ago
* 10.21.116.28 (recursive via 10.21.161.21)

FGT # get router info routing-table details 10.10.10.0
% Network not in table
```

A customer reports that they are not able to reach subnet 10.10.10.0/24 from their FortiGate device.

Based on the exhibit, what should you do to correct the situation?

- A. Enable next-hop-self feature
- B. Enable recursive resolution for BGP routes
- C. Enable additional-path feature
- D. Enable iBGP multipath

**Answer: A** ([LEAVE A REPLY](#))

### NEW QUESTION: 46

Refer to the exhibits.

Topology

Configuration

```

DC:
config vpn ipsec phase1-interface
 edit "advpn1"
 set type dynamic
 set interface "port1"
 set ike-version 2
 set peertype any
 set net-device disable
 set add-route disable
 set dpd on-idle
 set suite-b suite-b-gcm-128
 set auto-discovery-sender enable
 set psksecret fortinet
 next
 edit "advpn2"
 set type dynamic
 set interface "port1"
 set ike-version 2
 set peertype any
 set net-device disable
 set add-route disable
 set dpd on-idle
 set suite-b suite-b-gcm-128
 set auto-discovery-sender enable
 set psksecret fortinet
 next
end

Spokes:
config vpn ipsec phase1-interface
 edit "advpn1"
 set interface "port1"
 set ike-version 2
 set peertype any
 set net-device enable
 set add-route disable
 set dpd on-idle
 set suite-b suite-b-gcm-128
 set idle-timeout enable
 set idle-timeoutinterval 5
 set auto-discovery-receiver enable
 set remote-gw 198.18.101.100
 set psksecret fortinet
 next
 edit "advpn2"
 set interface "port2"
 set ike-version 2
 set peertype any
 set net-device enable
 set add-route disable
 set dpd on-idle
 set suite-b suite-b-gcm-128
 set idle-timeout enable
 set idle-timeoutinterval 5
 set auto-discovery-receiver enable
 set remote-gw 198.18.101.100
 set psksecret fortinet
 next

```

The exhibits show a diagram of a requested topology and the base IPsec configuration.

A customer asks you to configure ADVPN via two internet underlays. The requirement is that you use one interface with a single IP address on DC FortiGate.

In this scenario, which feature should be implemented to achieve this requirement?

- A. Use network-overlay id
- B. Change advpn2 to IKEv1

C. Use local-id

D. Use peer-id

**Answer:** ([SHOW ANSWER](#))

A is correct because using network-overlay id allows you to configure multiple ADVPN tunnels on a single interface with a single IP address on the DC FortiGate. This is explained in the FortiGate Administration Guide under ADVPN > Configuring ADVPN > Configuring ADVPN on the hub.

References: <https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn>

<https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn/978794/configuring-advpn>

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Use-case-of-Network-Ids-with-ADVPN-shortcut>

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Use-case-of-Network-Ids-with-ADVPN-shortcut>

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Use-case-of-Network-Ids-with-ADVPN-shortcut>

[/ta-p/241025](https://community.fortinet.com/t5/FortiGate/Technical-Tip-Use-case-of-Network-Ids-with-ADVPN-shortcut)

**Valid NSE8\_812 Dumps** shared by Actual4test.com for Helping Passing NSE8\_812 Exam!

Actual4test.com now offer the **newest NSE8\_812 exam dumps**, the Actual4test.com

NSE8\_812 exam **questions have been updated** and **answers have been corrected** get the

**newest** Actual4test.com NSE8\_812 dumps with Test Engine here:

[https://www.actual4test.com/NSE8\\_812\\_examcollection.html](https://www.actual4test.com/NSE8_812_examcollection.html) (107 Q&As Dumps, **30%OFF**

**Special Discount: Freepdfdumps)**

#### NEW QUESTION: 47

A retail customer with a FortiADC HA cluster load balancing five web servers in L7 Full NAT mode is receiving reports of users not able to access their website during a sale event. But for clients that were able to connect, the website works fine.

CPU usage on the FortiADC and the web servers is low, application and database servers are still able to handle more traffic, and the bandwidth utilization is under 30%.

Which two options can resolve this situation? (Choose two.)

A. Add more web servers to the real server pool

B. Add a connection-pool to the FortiADC virtual server

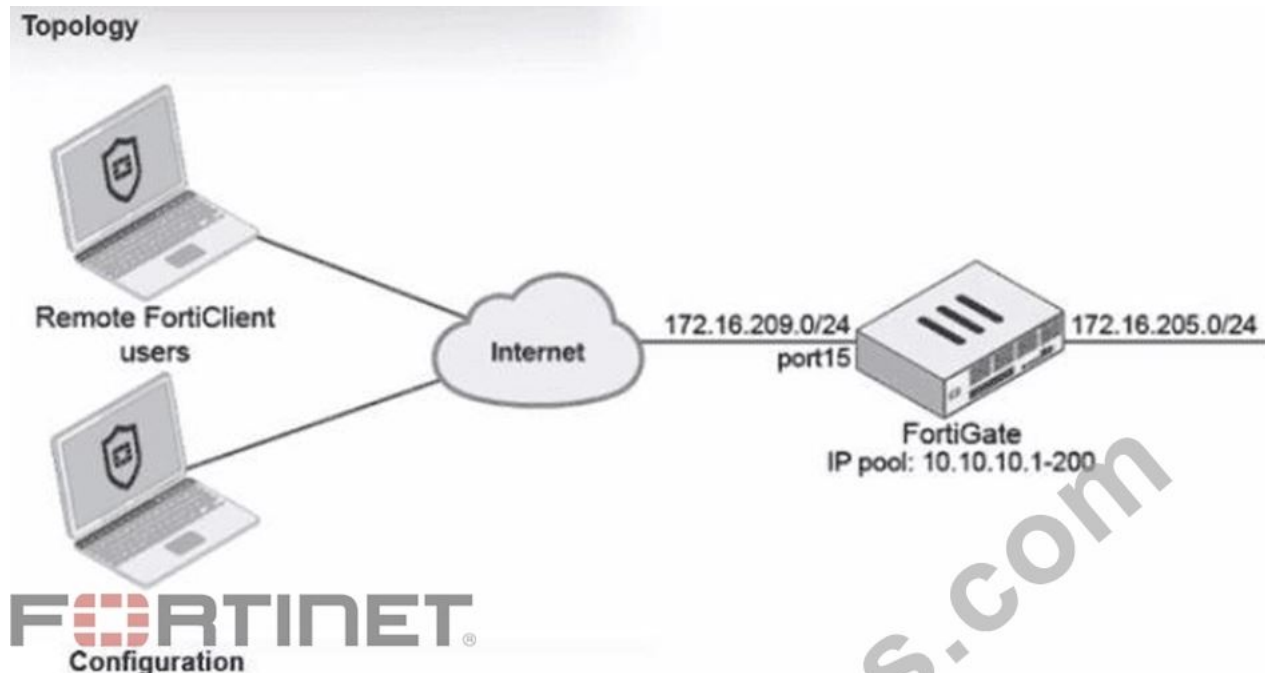
C. Disable SSL between the FortiADC and the web servers

D. Change the persistence rule to LB\_PERSIS\_SSL\_SESSJD.

**Answer:** B,D ([LEAVE A REPLY](#))

#### NEW QUESTION: 48

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



```
config vpn ipsec phase1-interface
 edit "vpn_endpts"
 set type dynamic
 set interface "port15"
 set mode aggressive
 set peertype any
 set net-device disable
 set mode-cfg enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set dpd on-idle
 set dhgrp 5
 set xauthtype auto
 set authusrgrp "vpngroup"
 set assign-ip-from name
 set ipv4-netmask 255.255.255.0
 set dns-mode auto
 set ipv4-split-include "172.16.205.0"
 set ipv4-name "client_range"
 set save-password enable
 set psksecret "nse8exam"
 set dpd-retryinterval 60
 next
end

config system link-monitor
 edit "1"
 set srcintf "vpn_endpts"
 set server-type dynamic
 next
end
```

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.

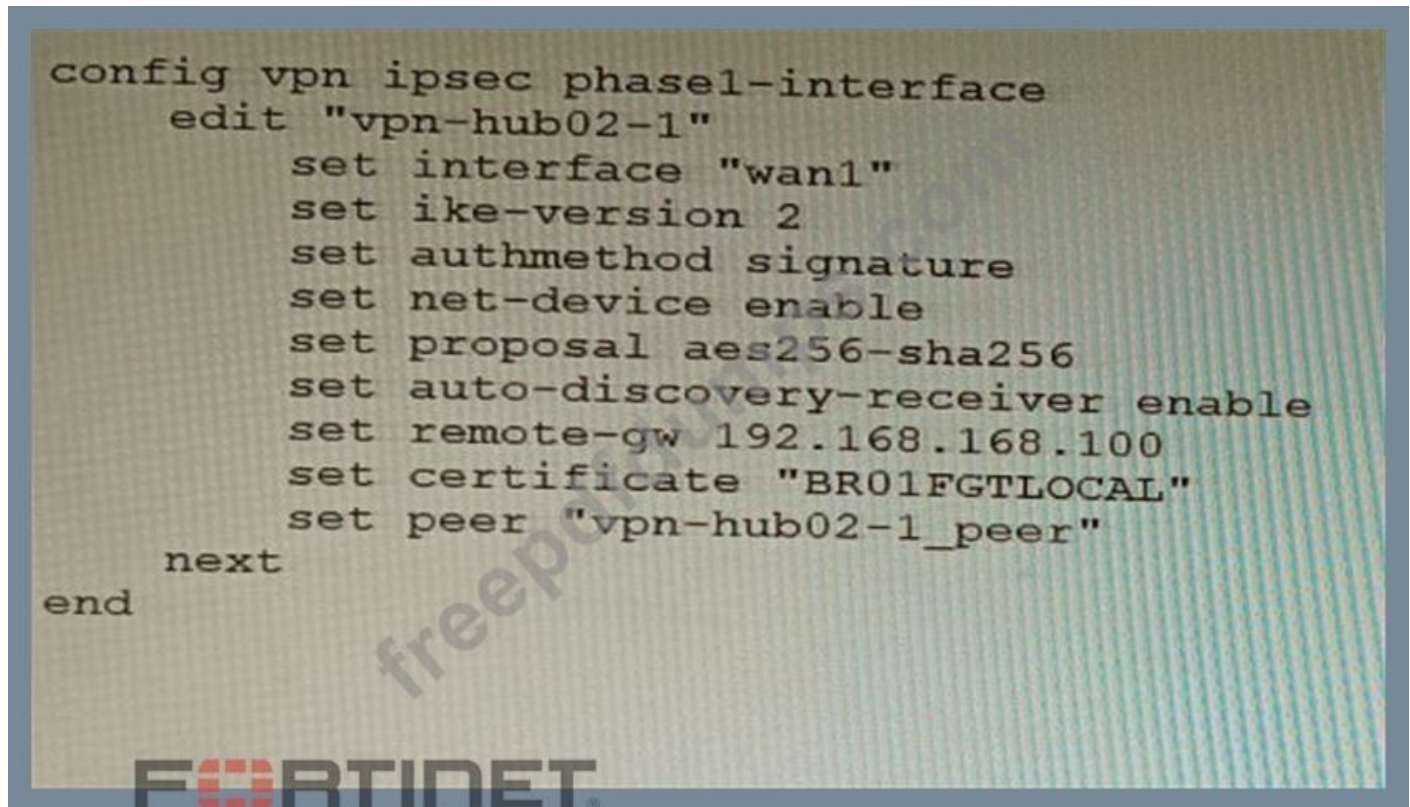
What is wrong with the configuration?

- A. It is necessary to use the IKEv2 protocol in this situation.
- B. IPsec Phase1 Interface has to be configured in IPsec main mode.
- C. The admin needs to disable the mode-cfg setting.
- D. SLA link monitoring does not work with the net-device setting.

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 49

Refer to the exhibit.



```
config vpn ipsec phase1-interface
 edit "vpn-hub02-1"
 set interface "wan1"
 set ike-version 2
 set authmethod signature
 set net-device enable
 set proposal aes256-sha256
 set auto-discovery-receiver enable
 set remote-gw 192.168.168.100
 set certificate "BR01FGTLOCAL"
 set peer "vpn-hub02-1_peer"
 next
end
```

The image shows a screenshot of a FortiGate device's command-line interface. The configuration is for a VPN interface named 'vpn-hub02-1'. The commands shown are: 'config vpn ipsec phase1-interface', 'edit "vpn-hub02-1"', 'set interface "wan1"', 'set ike-version 2', 'set authmethod signature', 'set net-device enable', 'set proposal aes256-sha256', 'set auto-discovery-receiver enable', 'set remote-gw 192.168.168.100', 'set certificate "BR01FGTLOCAL"', 'set peer "vpn-hub02-1\_peer"', 'next', and 'end'. A 'freepdf' watermark is visible across the center of the screenshot.

To facilitate a large-scale deployment of SD-WAN/ADVPN with FortiGate devices, you are tasked with configuring the FortiGate devices to support injecting of IKE routes on the ADVPN shortcut tunnels.

Which three commands must be added or changed to the FortiGate spoke config vpn ipsec phase1-interface options referenced in the exhibit for the VPN interface to enable this capability? (Choose three.)

- A. set net-device disable
- B. set mode-cfg enable
- C. set ike-version 1
- D. set add-route enable
- E. set mode-cfg-allow-client-selector enable

Answer: B,D,E ([LEAVE A REPLY](#))

\* B must be set to enable mode-cfg, which is required for injecting IKE routes on the ADVPN shortcut tunnels.

\* D must be set to enable add-route, which is the command that actually injects the IKE routes.

\* E must be set to enable mode-cfg-allow-client-selector, which allows custom phase 2 selectors

to be configured.

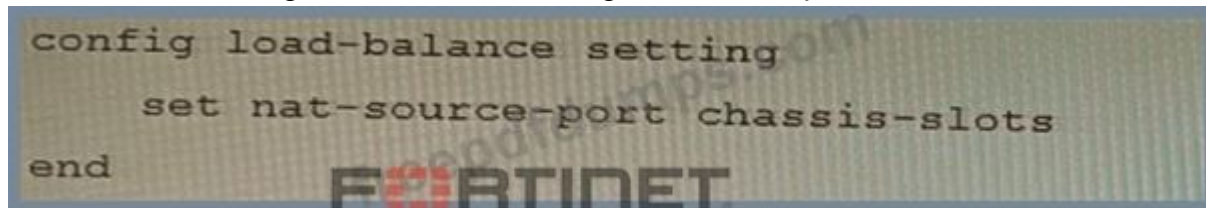
The other options are incorrect. Option A is incorrect because net-device disable is not required for injecting IKE routes on the ADVPN shortcut tunnels. Option C is incorrect because IKE version 1 is not supported for ADVPN.

References:

Phase 2 selectors and ADVPN shortcut tunnels | FortiGate / FortiOS 7.2.0 Configuring SD-WAN/ADVPN with FortiGate | FortiGate / FortiOS 7.2.0

### NEW QUESTION: 50

Review the following FortiGate-6000 configuration excerpt:



```
config load-balance setting
 set nat-source-port chassis-slots
end
```

Based on the configuration, which statement is correct regarding SNAT source port partitioning behavior?

- A. It dynamically distributes SNAT source ports to operating FPCs or FPMs.
- B. It is the default SNAT configuration and preserves active sessions when an FPC or FPM goes down.
- C. It statically distributes SNAT source ports to operating FPCs or FPMs
- D. It equally distributes SNAT source ports across chassis slots.

**Answer: C** ([LEAVE A REPLY](#))

<https://docs.fortinet.com/document/fortigate/7.4.1/fortigate-6000-administration-guide/81276/controlling-snat-port-partitioning-behavior>

"chassis-slots this option statically allocates SNAT source ports to all FPCs that are enabled when you enter the command. If you disable an FPC from the CLI, the SNAT source ports assigned to that FPC will not be re-allocated to the remaining FPCs. All FPCs that are still operating will maintain the same SNAT source port allocation and active sessions being processed by the still operating FPCs will not be affected."

### NEW QUESTION: 51

Refer to the exhibit.

```

FGT_3 # show router ospf
config router ospf
 set router-id 10.10.10.3
 config area
 edit 0.0.0.0
 next
 end
 config ospf-interface
 edit "port2"
 set interface "port2"
 set network-type point-to-point
 next
 end
 config network
 edit 1
 set prefix 10.10.10.0 255.255.255.0
 next
 end
end

```

You are operating an internal network with multiple OSPF routers on the same LAN segment. FGT\_3 needs to be added to the OSPF network and has the configuration shown in the exhibit. FGT\_3 is not establishing any OSPF connection. What needs to be changed to the configuration to make sure FGT\_3 will establish OSPF neighbors without affecting the DR/BDR election?

A.

```

config router ospf
 config ospf-interface
 edit "port2"
 set priority 255
 set network-type point-to-multipoint
 next
 end
end

```

```

config router ospf
 config ospf-interface
 edit "port2"
 set priority 0
 set network-type broadcast
 next
 end
end

```

B.



```

config router ospf
 config ospf-interface
 edit "port2"
 set priority 255
 set network-type broadcast
 next
 end
end

```

C.

```

config router ospf
 config ospf-interface
 edit "port2"
 set priority 0
 set network-type point-to-multipoint
 next
 end

```

D.

**Answer: (SHOW ANSWER)**

The OSPF configuration shown in the exhibit is using the default priority value of 1 for the interface port1.

This means that FGT\_3 will participate in the DR/BDR election process with the other OSPF routers on the same LAN segment. However, this is not desirable because FGT\_3 is a new device that needs to be added to the OSPF network without affecting the existing DR/BDR election. Therefore, to make sure FGT\_3 will establish OSPF neighbors without affecting the DR/BDR election, the priority value of the interface port1 should be changed to 0. This will prevent FGT\_3 from becoming a DR or BDR and allow it to form OSPF adjacencies with the current DR and BDR. Option B shows the correct configuration that changes the priority value to 0. Option A is incorrect because it does not change the priority value. Option C is incorrect because it changes the network type to point-to-point, which is not suitable for a LAN segment with multiple OSPF routers. Option D is incorrect because it changes the area ID to 0.0.0.1, which does not match the area ID of the other OSPF routers on the same LAN segment. References: <https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/358640/basic-ospf-example>

**Valid NSE8\_812 Dumps** shared by Actual4test.com for Helping Passing NSE8\_812 Exam!  
Actual4test.com now offer the **newest NSE8\_812 exam dumps**, the Actual4test.com

NSE8\_812 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NSE8\_812 dumps with Test Engine here:

[https://www.actual4test.com/NSE8\\_812\\_examcollection.html](https://www.actual4test.com/NSE8_812_examcollection.html) (107 Q&As Dumps, **30%OFF**

**Special Discount: Freepdfdumps)**