Fortinet.NSE8_812.v2026-04-25.q111

Exam Code:	NSE8_812
Exam Name:	Fortinet NSE 8 - Written Exam (NSE8_812)
Certification Provider:	Fortinet
Free Question Number:	111
Version:	v2026-04-25
# of views:	408
# of Questions views:	1110
https://www.exam-tests.com/NSE8_812-exam/Fortinet.NSE8_812.v2026-04-25.q111.html	

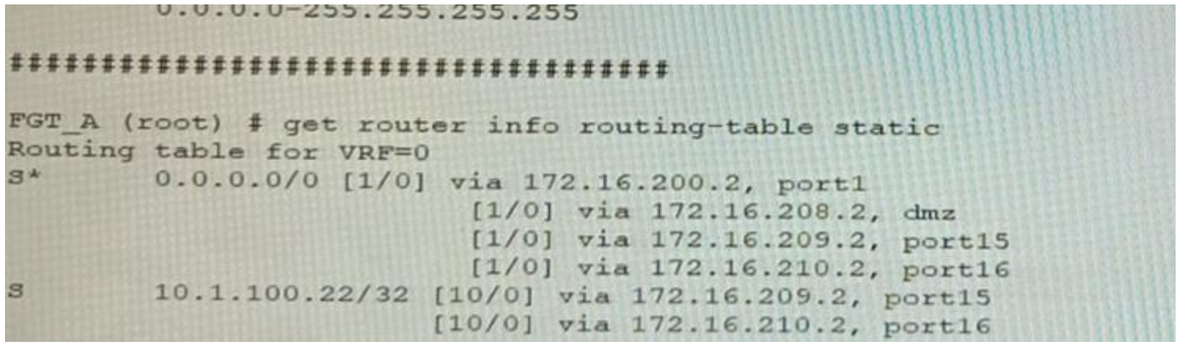
NEW QUESTION: 1
Refer to the exhibit showing an SD-WAN configuration.

```
        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):
```



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

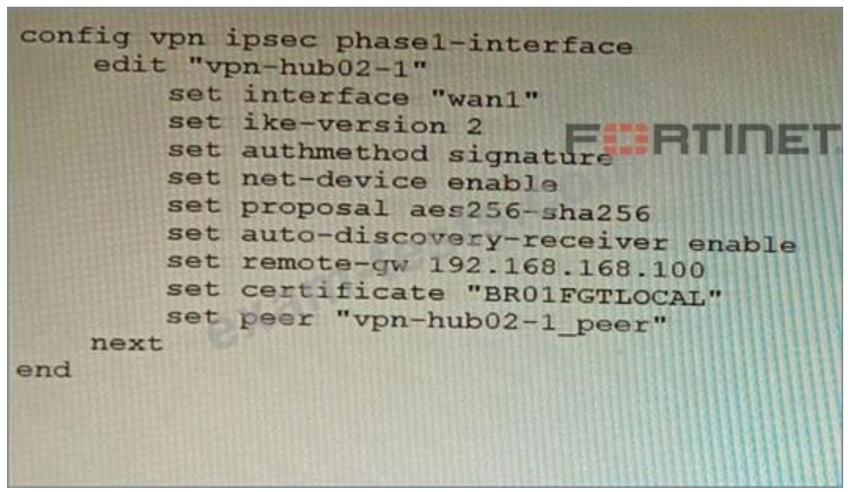
D. port1 and port15

Answer: A (LEAVE A REPLY)

According to the exhibit, the SD-WAN configuration has two rules: one for traffic to 10.1.100.0/24 subnet, and one for traffic to 10.1.100.16/28 subnet. The first rule uses the best quality strategy, which selects the SD-WAN member with the best measured quality based on performance SLA metrics. The second rule uses the manual strategy, which specifies port1 as the SD-WAN member to select. Therefore, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, the outgoing interfaces will be port16 and port1 respectively, assuming that port16 has the best quality among the SD-WAN members. References: https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/218559/configuring-the-sd-wan-interface

NEW QUESTION: 2

Refer to the exhibit.



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 phasei-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.

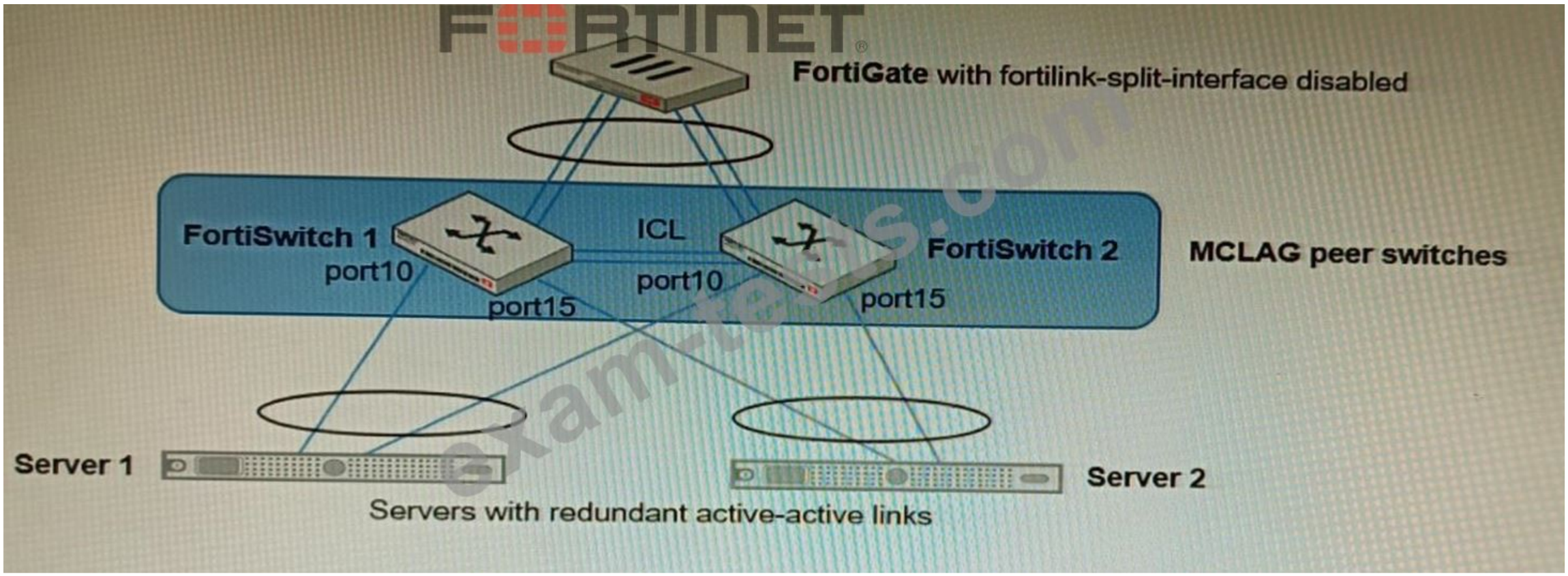
The other options are incorrect. Option A is incorrect because net-device disable is not required for injecting IKE routes on the ADVPN shortcut tunnels. Option C is incorrect because IKE version 1 is not supported for ADVPN.

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: 3

Refer to the exhibit.



You have been tasked with replacing the managed switch Forti Switch 2 shown in the topology.

Which two actions are correct regarding the replacement process? (Choose two.)

A. After replacing the FortiSwitch unit, the automatically created trunk name does not change

B. CLAG-ICL needs to be manually reconfigured once the new switch is connected to the FortiGate

C. After replacing the FortiSwitch unit, the automatically created trunk name changes.

D. MCLAG-ICL will be automatically reconfigured once the new switch is connected to the FortiGate.

Answer: A,D (LEAVE A REPLY)

Based on the exhibit, the two correct actions regarding the replacement process are:

After replacing the FortiSwitch unit, the automatically created trunk name does not change. This is because the trunk name is based on the slot number and port number of the FortiGate unit that connects to the FortiSwitch unit, which remain the same after the replacement. If a different trunk name is desired, the trunk must be deleted and a new trunk will be created automatically with an updated name.

MCLAG-ICL will be automatically reconfigured once the new switch is connected to the FortiGate. This is because the MCLAG-ICL configuration is stored on the FortiGate unit and applied to the FortiSwitch unit when it is authorized. The replacement FortiSwitch unit will inherit the MCLAG-ICL configuration of the failed FortiSwitch unit after it is replaced using the replace-device command in FortiOS. Reference: https://docs.fortinet.com/document/fortiswitch/7.0.8/devices-managed-by-fortios/173284/replacing-a-managed-fortiswitch-unit

NEW QUESTION: 4

Refer to the exhibit, which shows an SD-WAN configuration.

```
Branch1:

config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
        edit "HUB1"
        next
        edit "HUB1-BKP"
        next
    end
    config members
        edit 1
            set interface "HUB1-VPN1"
            set zone "HUB1"
        next
        edit 2
            set interface "HUB1-VPN-BKP"
            set zone "HUB1-BKP"
        next
    end
    ...
    config duplication
        edit 1
            set srcaddr "Branch-NET"
            set dstaddr "all"
            set srcintf "any"
            set dstintf "HUB1" "HUB1-BKP"
            set service "HTTP"
            set packet-duplication force
            set packet-de-duplication enable
        next
    end
end
```


You configured the SD-WAN from Branch1 to the HUB and enabled packet duplication. You later notice that the traffic is not being duplicated. In this scenario, what is causing this problem?

A. There is a mismatch in the FortiOS version between Branch1 and HUB.

B. Packet duplication is not enabled on the HUB side.

C. Traffic cannot be duplicated over multiple zones.

D. Packet duplication did not occur because an interface is out of SLA.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 5

Refer to the exhibit.

The exhibit shows two error messages from a FortiGate root Security Fabric device when you try to configure a new connection to a FortiClient EMS Server.

Referring to the exhibit, which two actions will fix these errors? (Choose two.)

A. Verify that the CRL is accessible from the root FortiGate

B. Export and import the FortiClient EMS server certificate to the root FortiGate.

C. Install a new known CA on the Win2K16-EMS server.

D. Authorize the root FortiGate on the FortiClient EMS

Answer: B,D (LEAVE A REPLY)

* A is correct because the error message "The CRL is not accessible" indicates that the root FortiGate cannot access the CRL for the FortiClient EMS server. Verifying that the CRL is accessible will fix this error.
* D is correct because the error message "The FortiClient EMS server is not authorized" indicates that the root FortiGate is not authorized to connect to the FortiClient EMS server. Authorizing the root FortiGate on the FortiClient EMS server will fix this error.

The other options are incorrect. Option B is incorrect because exporting and importing the FortiClient EMS server certificate to the root FortiGate will not fix the CRL error. Option C is incorrect because installing a new known CA on the Win2K16-EMS server will not fix the authorization error.

References:

Troubleshooting FortiClient EMS connectivity | FortiClient / FortiOS 7.0.0 - Fortinet Document Library Authorizing FortiGates with FortiClient EMS | FortiClient / FortiOS 6.4.8 - Fortinet Document Library
https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/185333/forticlient-ems%E2%80%9D

NEW QUESTION: 6

You are troubleshooting a FortiMail Cloud service integrated with Office 365 where outgoing emails are not reaching the recipients' mail What are two possible reasons for this problem? (Choose two.)

A. The FortiMail access control rule to relay from Office 365 servers FQDN is missing.

B. The FortiMail DKIM key was not set using the Auto Generation option.

C. The FortiMail access control rules to relay from Office 365 servers public IPs are missing.

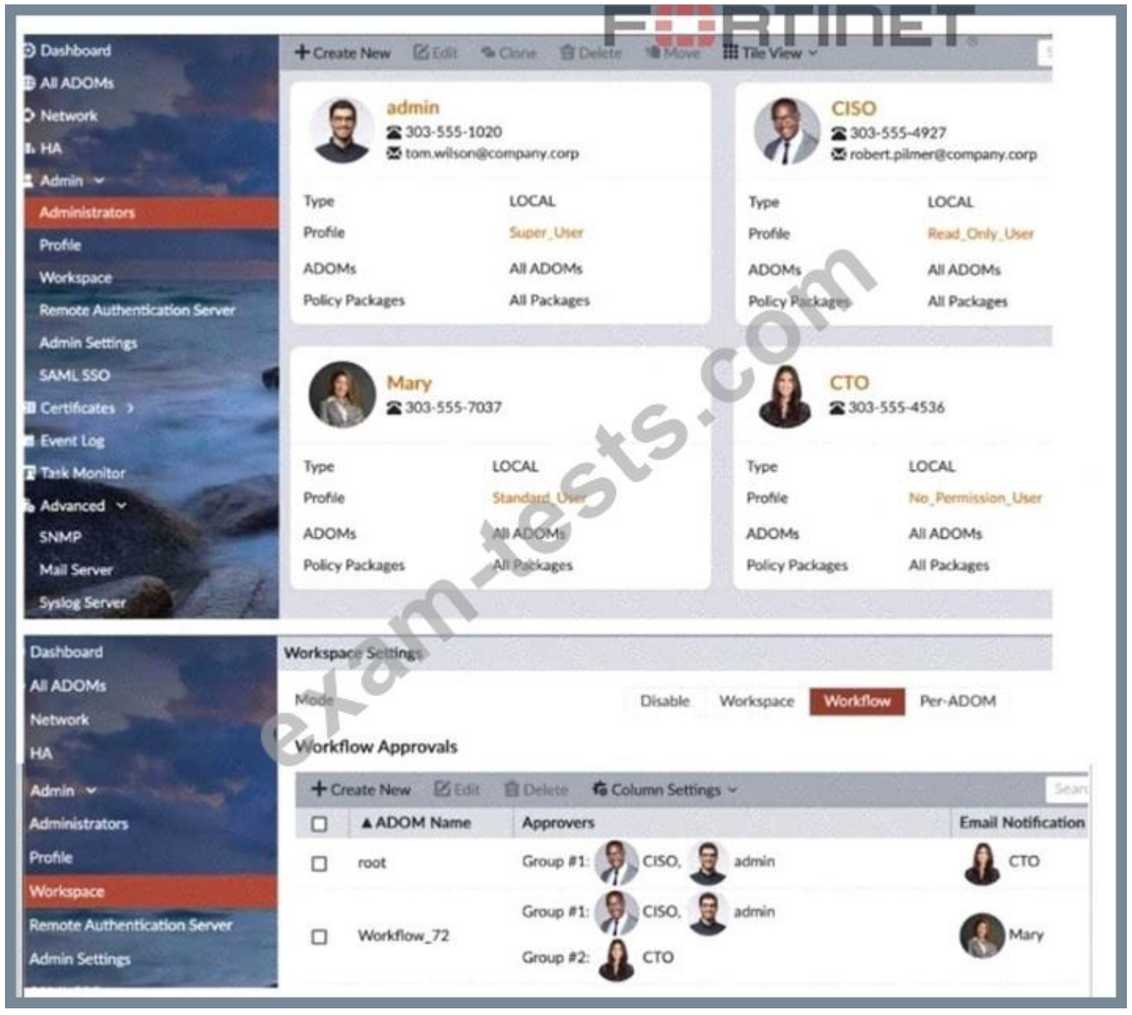
D. A Mail Flow connector from the Exchange Admin Center has not been set properly to the FortiMail Cloud FQDN.

Answer: C,D (LEAVE A REPLY)

https://docs.fortinet.com/document/fortimail/7.2.0/cookbook/963264/configuring-outbound-settings-in-office-365

NEW QUESTION: 7

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

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

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

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

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

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 8

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. If an FPM goes down, SSL VPN IP pool IP addresses will be re-allocated to the remaining FPMs.

B. Enabling SSL VPN load balancing will clear the session table.

C. You can use src-ip or dst-ip-dport on dp-load-distribution-method to make SSL VPN load balancing work as expected.
D. To have better traffic distribution you should use IP pools that increment in multiples of 12.
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Refer to the exhibit.

```
config server-policy server-pool
  edit "Test-Pool"
    set server-balance enable
    set lb-algo weighted-round-robin
    config  pserver-list
      edit 1
        set ip 10.10.10.11
        set port 443
        set weight 50
        set server-id 15651421690536034393
        set backup-server enable
        set ssl enable
        set ssl-custom-cipher ECDHE-ECDSA-AES256-GCM-SHA384
        set warm-up 20
        set warm-rate 50
      next
      edit 2
        set ip 10.10.10.12
        set port 443
        set weight 100
        set server-id 140100217271901896662
        set ssl enable
        set ssl-custom-cipher ECDHE-ECDSA-AES256-GCM-SHA384
        set warm-up 80
        set warm-rate 150
      next
    end
  next
end
```

A FortiWeb appliance is configured for load balancing web sessions to internal web servers. The Server Pool is configured as shown in the exhibit.
How will the sessions be load balanced between server 1 and server 2 during normal operation?
A. Server 1 will receive 25% of the sessions, Server 2 will receive 75% of the sessions

B. Server 1 will receive 20% of the sessions, Server 2 will receive 66.6% of the sessions
C. Server 1 will receive 33.3% of the sessions, Server 2 will receive 66 6% of the sessions
D. Server 1 will receive 0% of the sessions Server 2 will receive 100% of the sessions
Answer: A (LEAVE A REPLY)
The Server Pool in the exhibit is configured with a weight of 20 for server 1 and a weight of 60 for server 2. This means that server 1 will receive 20% of the sessions and server 2 will receive 75% of the sessions.
The following formula is used to calculate the load balancing between servers in a Server Pool:
weight_of_server_1 / (weight_of_server_1 + weight_of_server_2)
In this case, the formula is:
20 / (20 + 60) = 20 / 80 = 0.25 = 25%
Therefore, server 1 will receive 25% of the sessions and server 2 will receive 75% of the sessions.

NEW QUESTION: 10
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
```

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: B,D (LEAVE A REPLY)

B is correct because the OCSP check of the certificate can be combined with a certificate revocation list (CRL). This means that the FortiGate will check the OCSP server to see if the certificate has been revoked, and it will also check the CRL to see if the certificate has been revoked.

D is correct because if the OCSP server is unreachable, authentication will succeed if the certificate matches the CA. This is because the FortiGate will fall back to using the CRL if the OCSP server is unreachable.

The other options are incorrect. Option A is incorrect because OCSP checks can go to other OCSP servers, not just the FortiAuthenticator. Option C is incorrect because OCSP certificate responses can be cached by the FortiGate.

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: 11

A customer is planning on moving their secondary data center to a cloud-based IaaS. They want to place all the Oracle-based systems Oracle Cloud, while the other systems will be on Microsoft Azure with ExpressRoute service to their main data center.

They have about 200 branches with two internet services as their only WAN connections. As a security consultant you are asked to design an architecture using Fortinet products with security, redundancy and performance as a priority.

Which two design options are true based on these requirements? (Choose two.)

A. Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud.

B. Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure.

C. Branch FortiGate devices must be configured as VPN clients for the branches' internal network to be able to access Oracle services without using public IPs.

D. Two ExpressRoute services to the main data center are required to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge

Answer: A,C (LEAVE A REPLY)

a) Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud. This is because the Oracle Cloud is not directly connected to the Azure Cloud. The traffic will need to go through the main data center in order to reach the Oracle Cloud.

c) Branch FortiGate devices must be configured as VPN clients for the branches' internal network to be able to access Oracle services without using public IPs. This is because the Oracle Cloud does not allow direct connections from the internet. The traffic will need to go through the FortiGate devices in order to reach the Oracle Cloud.

The other options are not correct.

b) Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure. This is not necessary. Azure does encrypt traffic over ExpressRoute.

d) Two ExpressRoute services to the main data center are required to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge. This is not necessary. A single ExpressRoute service can be used to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge.

NEW QUESTION: 12

Refer to the exhibits.

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

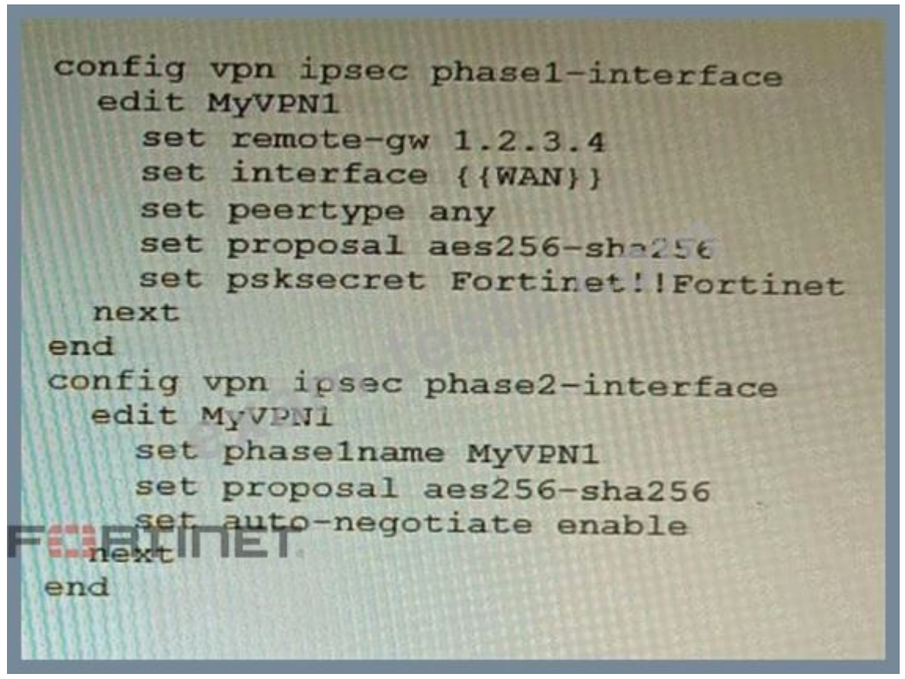
D. Use peer-id

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 13

Refer to the exhibit.



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 Jinja template will automatically map the interface with "WAN" role on the managed FortiGate.

B. The template will work if you change the variable format to $(WAN).

C. The template will work if you change the variable format to {{ WAN }}.

D. The administrator must first manually map the interface for each device with a meta field.

E. The template will fail because this configuration can only be applied with a CLI or TCL script.

Answer: D,E (LEAVE A REPLY)

D: The administrator must first manually map the interface for each device with a meta field.

The Jinja template in the exhibit is expecting a meta field calledWANto be set on the managed FortiGate.

This meta field will specify which interface on the FortiGate should be assigned the "WAN" role. If the meta field is not set, then the template will fail.

E: The template will fail because this configuration can only be applied with a CLI or TCL script.

The Jinja template in the exhibit is trying to configure the interface role on the managed FortiGate. This type of configuration can only be applied with a CLI or TCL script. The Jinja template will fail because it is not a valid CLI or TCL script.

NEW QUESTION: 14

An automation stitch was configured using an incoming webhook as the trigger named 'my_incoming_webhook'. The action is configured to execute the CLI Script shown:

```
config firewall address
    edit %%results.hostname%%
        set subnet %%results.ip.1%%/32
    next
end
config firewall addrgrp
    edit Bad-Hosts
        append member %%results.hostname%%
    next
end
```

A.
```
data: '{ "hostname": "bad_host_1", "ip": ["1.1.1.1"]}'
url: http://192.168.226.129/api/v2/monitor/system/automation-stitch/webhook/my_incoming_webhook
```

B.
```
data: '{ "hostname": "bad_host_1", "ip": "1.1.1.1"}'
url: http://192.168.226.129/api/v2/monitor/system/automation-stitch/webhook/my_incoming_webhook
```

C.
```
data: '{ "hostname": "bad_host_1", "ip": ["1.1.1.1"]}'
url: http://192.168.226.129/api/v2/cmdb/system/automation-stitch/webhook/my_incoming_webhook
```

D.
```
data: { "hostname": "bad_host_1", "ip": "1.1.1.1"}
url: http://192.168.226.129/api/v2/cmdb/system/automation-stitch/webhook/my_incoming_webhook
```

Answer: A (LEAVE A REPLY)

The CLI script in option A will send the log message to the webhook server. The webhook server can then be configured to take any desired action, such as storing the log message in a database or sending an email notification.

The other options are incorrect. Option B will not send the log message to the webhook server because it does not contain the curl command. Option C will send the log message to the webhook server, but it will also include the FortiGate's IP address and MAC address. This information is not necessary, and it could be used by an attacker to identify the FortiGate. Option D will not send the log message to the webhook server because it does not contain the webhook action.

References:

Automation webhook stitches: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/989735/webhook-action Webhooks: https://en.wikipedia.org/wiki/Webhook

NEW QUESTION: 15

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: (SHOW ANSWER)

The FEC configuration in the exhibit specifies that if the packet loss is greater than 10%, then the FEC mapping will be 8 base packets and 2 redundant packets. The download bandwidth of 500 Mbps is not greater than 950 Mbps, so the FEC mapping is not overridden by the bandwidth setting. Therefore, the FEC behavior will be 2 redundant packets for every 8 base packets.

Here is the explanation of the FEC mappings in the exhibit:

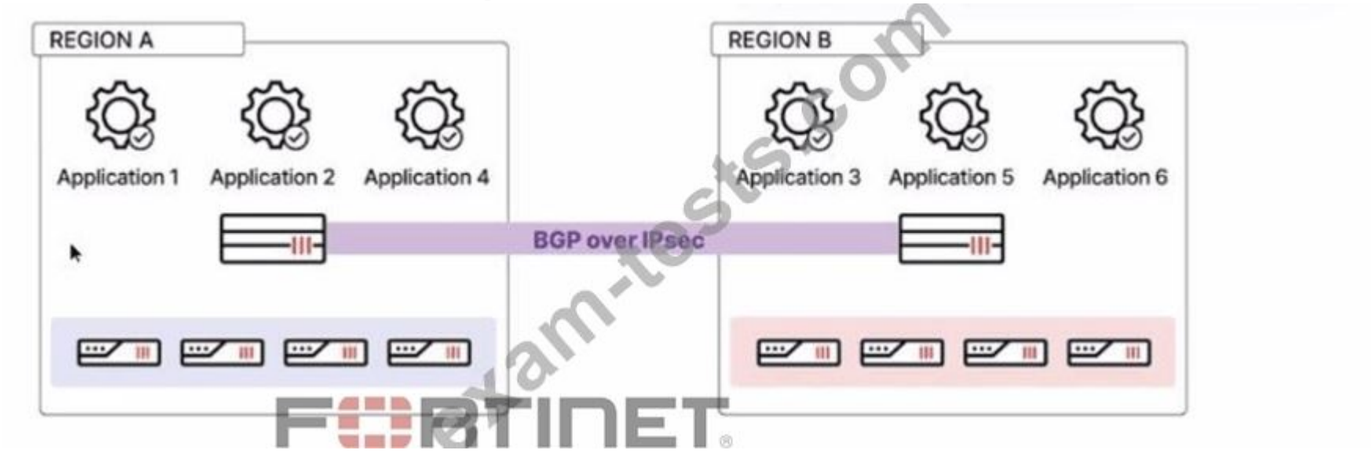
Packet loss greater than 10%: 8 base packets and 2 redundant packets.

Upload bandwidth greater than 950 Mbps: 9 base packets and 3 redundant packets.

The mappings are matched from top to bottom, so the first mapping that matches the conditions will be used. In this case, the first mapping matches because the packet loss is greater than 10%. Therefore, the

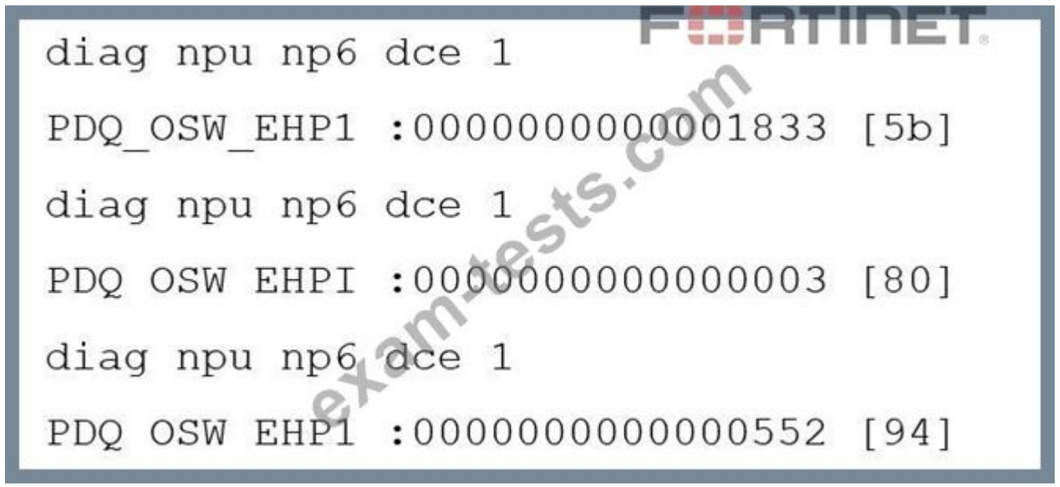
FEC behavior will be 2 redundant packets for every 8 base packets.

NEW QUESTION: 16
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 iBGP is used, cross-regional spoke-to-hub shortcuts cannot be used.
C. If eBGP is used, ADVPN can be established for branch-to-branch traffic across regions.
D. If iBGP is used, cross-regional spoke-to-hub shortcuts can be established.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
You are running a diagnose command continuously as traffic flows through a platform with NP6 and you obtain the following output:



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: 18

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
  }
```

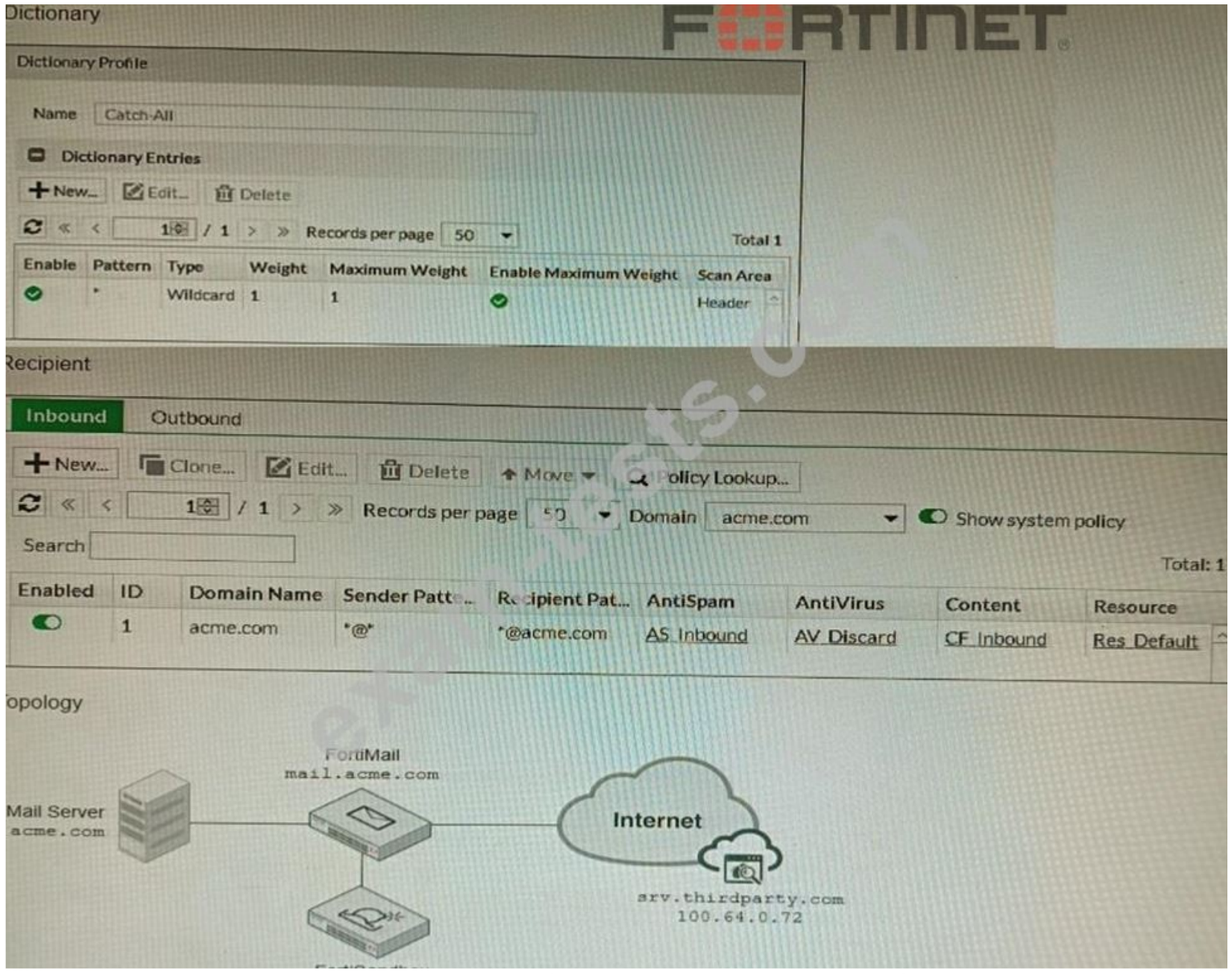
A customer wants to automate the creation and configuration of FortiGate VM instances in a VMware vCenter environment using Terraform. They have the creation part working with the code shown in the exhibit.

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 "fortinet_fortigate" {
     hostname = vsphere_virtual_machine.vm.default_ip_address
     token    = "jn3t3Nw7qckQzt955Htkfj5hwQ6jdb"
     insecure = "true"
}
```
B.
```
provider "fortios" {
     hostname = module.vsphere_virtual_machine.default_ip_address
     token    = "jn3t3Nw7qckQzt955Htkfj5hwQ6jdb"
     insecure = "true"
}
```
C.
```
provider "fortinet_fortigate" {
     hostname = module.vsphere_virtual_machine.default_ip_address
     token    = "jn3t3Nw7qckQzt955Htkfj5hwQ6jdb"
     insecure = "true"
```
D.
```
provider "fortios" {
     hostname = vsphere_virtual_machine.vm.default_ip_address
     token    = "jn3t3Nw7qckQzt955Htkfj5hwQ6jdb"
     insecure = "true"
}
```
Answer: (SHOW ANSWER)

NEW QUESTION: 19

Refer to the exhibits.



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-AII 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: B,C (LEAVE A REPLY)

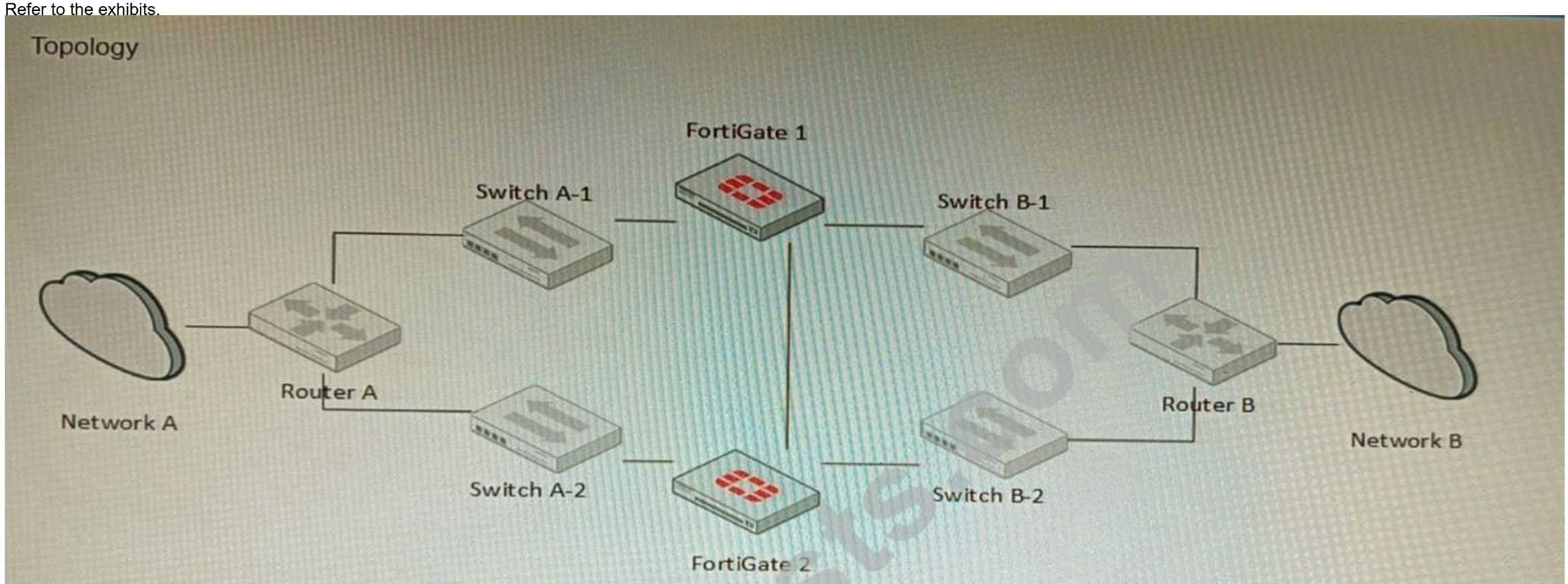
To integrate a third-party's host service (srv.thirdparty.com) into the e-mail processing path, while ensuring that all inbound e-mails are scanned by FortiMail antispam and antivirus with FortiSandbox integration, and then forwarded to the third-party service and back to FortiMail for final delivery, the following configuration tasks must be performed:

Apply the Catch-All profile to the CFInbound profile and configure a content action profile to deliver to the srv.thirdparty.com FQDN. This will ensure that all inbound e-mails that pass the antispam and antivirus scanning are forwarded to the third-party service for further processing.

Create an access receive rule with a Sender value of srv.thirdparty.com, Recipient value of *@acme.com, and action value of Safe. This will ensure that all e-mails that are sent back from the third-party service to FortiMail are accepted without any further scanning or filtering. Reference: https://docs.fortinet.com/document/fortimail/7.2.2/administration-guide/921588/configuring-content-profiles-and-content-action-profiles https://docs.fortinet.com/document/fortimail/7.2.2/administration-guide/629994/configuring-session-profiles

NEW QUESTION: 20

Refer to the exhibits.



Configuration

```
FGT-HA-1 # get system ha status
HA Health Status: OK
Model: FortiGate-VM64
```

```
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 1:35:12
Cluster state change time: 2019-05-16 14:53:05
Master selected using:
    <2019/05/16 14:53:05> FGVMEVLQOG33WM3D is selected as the
master because it has the largest value of uptime.
    <2019/05/16 14:45:53> FGVMEVLQOG33WM3D is selected as the
master because it's the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
unicast_hb: peerip=192.168.40.1, myip=192.168.40.2,
hasync_port='port3'
Configuration Status:
    FGVMEVLQOG33WM3D(updated 2 seconds ago): in-sync
    FGVMEVGCJNHFYI4A(updated 0 seconds ago): in-sync
```

Configuration -

```
FGT-HA-1 # get system ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 1:35:12
Cluster state change time: 2019-05-16 14:53:05
Master selected using:
    <2019/05/16 14:53:05> FGVMEVLQOG33WM3D is selected as the
master because it has the largest value of uptime.
    <2019/05/16 14:45:53> FGVMEVLQOG33WM3D is selected as the
master because it's the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
unicast_hb: peerip=192.168.40.1, myip=192.168.40.2,
hasync_port='port3'
Configuration Status:
FGVMEVLQOG33WM3D(updated 2 seconds ago): in-sync
FGVMEVGCJNHFYI4A(updated 0 seconds ago): in-sync
```


The exhibits show a FortiGate network topology and the output of the status of high availability on the FortiGate.

Given this information, which statement is correct?

A. The ethertype values of the HA packets are 0x8890, 0x8891, and 0x8892

B. The cluster mode can support a maximum of four (4) FortiGate VMs

C. The cluster members are on the same network and the IP addresses were statically assigned.

D. FGVMEVLQOG33WM3D and FGVMEVGCJNHFYI4A share a virtual MAC address.

Answer: (SHOW ANSWER)

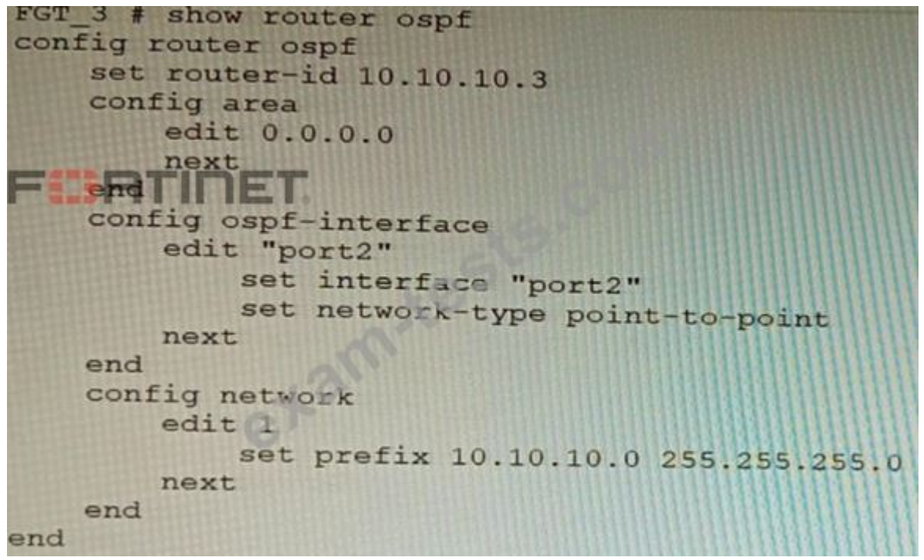
The output of the status of high availability on the FortiGate shows that the cluster mode is active-passive, which means that only one FortiGate unit is active at a time, while the other unit is in standby mode. The active unit handles all traffic and also sends HA heartbeat packets to monitor the standby unit. The standby unit becomes active if it stops receiving heartbeat packets from the active unit, or if it receives a higher priority from another cluster unit. In active-passive mode, all cluster units share a virtual MAC address for each interface, which is used as the source MAC address for all packets forwarded by the cluster.

References:

https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103439/high-availability-with-two-fortigates

NEW QUESTION: 21

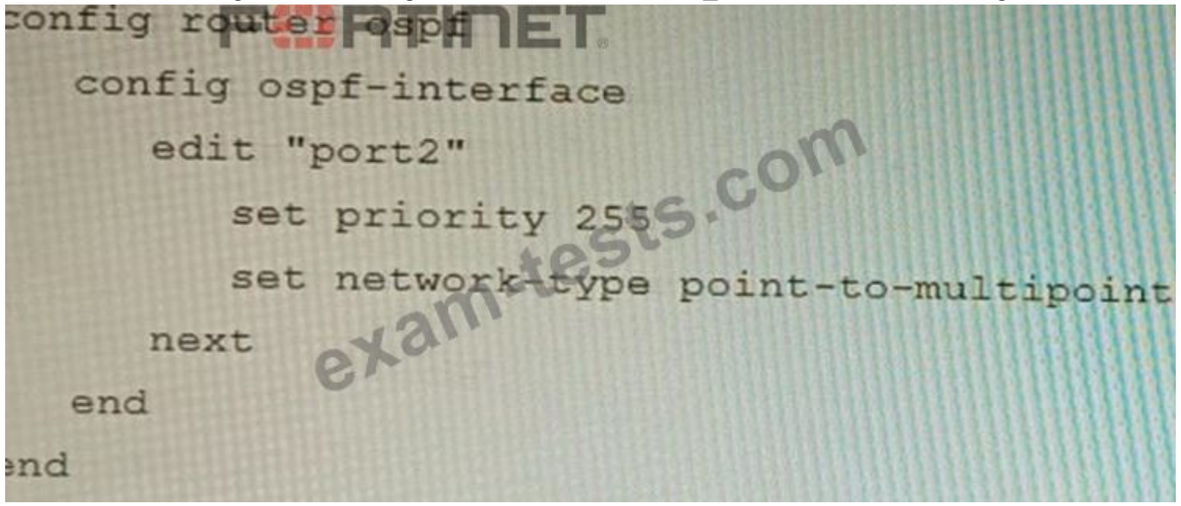
Refer to the exhibit.



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.



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


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


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


Answer: B (LEAVE A REPLY)

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. Reference: https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/358640/basic-ospf-example

NEW QUESTION: 22

Refer to the exhibit showing a firewall policy configuration.

Policies

```
config firewall policy
    edit 1
        set name "Dev-To-Cloud-Assets"
        set srcintf "port2"
        set dstintf "port4"
        set srcaddr "Dev-Subnet"
        set dstaddr "Dev-Cloud-Assets"
        set action accept
        set schedule "always"
        set service "ALL"
        set fsso disable
        set groups "Dev-Users"
        set nat enable
    next
    edit 2
        set name "Internet-Access"
        set srcintf "port2"
        set dstintf "port4"
        set srcaddr "All-Internal"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set fsso disable
        set nat enable
    next
end
```


To prevent unauthorized access of their cloud assets, an administrator wants to enforce authentication on firewall policy ID 1.

What change does the administrator need to make?

A.
```
config user setting
     set auth-on-demand always
end
```

B.
```
config user setting
     set auth-secure-http enable
     set auth-http-basic disable
end
```

C.
```
config firewall policy
     edit 1
          set ntlm-guest disable
     next
end
```

D.
```
config firewall policy
     edit 1
          set fsso enable
     next
end
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: A (LEAVE A REPLY)

https://docs.fortinet.com/document/fortigate/6.2.0/new-features/238665/authentication-policy-extensions

NEW QUESTION: 23
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
Configuring Performance SLA | FortiGate / FortiOS 7.4.0

NEW QUESTION: 24
Which feature must you enable on the BGP neighbors to accomplish this goal?
A. Graceful-restart

B. Deterministic-med
C. Synchronization
D. Soft-reconfiguration
Answer: A (LEAVE A REPLY)
Graceful-restart is a feature that allows BGP neighbors to maintain their routing information during a BGP restart or failover event, without disrupting traffic forwarding or causing route flaps. Graceful-restart works by allowing a BGP speaker (the restarting router) to notify its neighbors (the helper routers) that it is about to restart or failover, and request them to preserve their routing information and forwarding state for a certain period of time (the restart time). The helper routers then mark the routes learned from the restarting router as stale, but keep them in their routing table and continue forwarding traffic based on them until they receive an end-of-RIB marker from the restarting router or until the restart time expires. This way, graceful-restart can minimize traffic disruption and routing instability during a BGP restart or failover event. References:
https://docs.fortinet.com/document/fortigate/7.0.0/cookbook/19662/bgp-graceful-restart

NEW QUESTION: 25
You have configured a Site-to-Site IPsec VPN tunnel between a FortiGate and a third-party device but notice that one of the error counters on the tunnel interface keeps increasing.

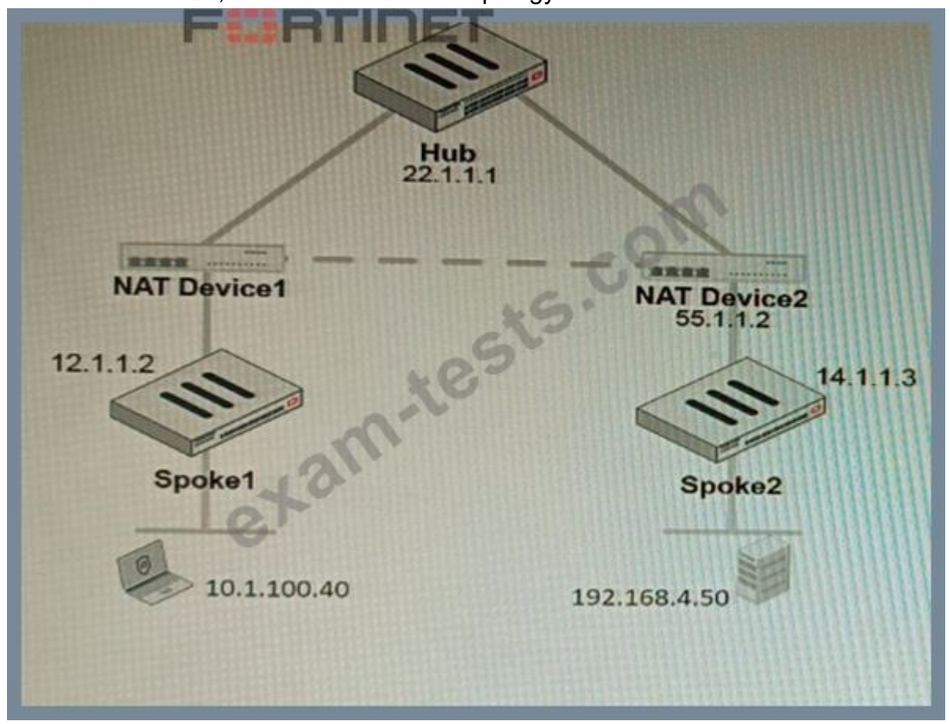
```
VPN-TUNNEL Link encap:Unknown
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1420 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:337 errors:4 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:451856798 (430.9 MB) TX bytes:266756340 (254.4 MB)
```


Which two configuration options can resolve this problem? (Choose two.)
A. Enable Forward Error Correction (FEC) on the VPN interface for egress traffic.
B. Adjust the MTU of the IPsec interface.
C. Adjust the MTU of the physical interface to which the IPsec tunnel is bound.
D. Enable DF-bit honoring in the global settings.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 26
SD-WAN is configured on a FortiGate. You notice that when one of the internet links has high latency the time to resolve names using DNS from FortiGate is very high.
You must ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work.
What should you configure?
A. Configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server.
B. Configure local out traffic to use the outgoing interface based on SD-WAN rules with a manual defined IP associated to a loopback interface and configure an SD-WAN rule from the loopback to the DNS server.
C. Configure an SD-WAN rule to the DNS server and use the FortiGate interface IPs in the source address.
D. Configure two DNS servers and use DNS servers recommended by the two internet providers.
Answer: (SHOW ANSWER)
SD-WAN is a feature that allows users to optimize network performance and reliability by using multiple WAN links and applying rules based on various criteria, such as latency, jitter, packet loss, etc. One way to ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work is to configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server. This means that the FortiGate will use the best WAN link available to send DNS queries to the DNS server according to the SD-WAN rule, and use its own interface

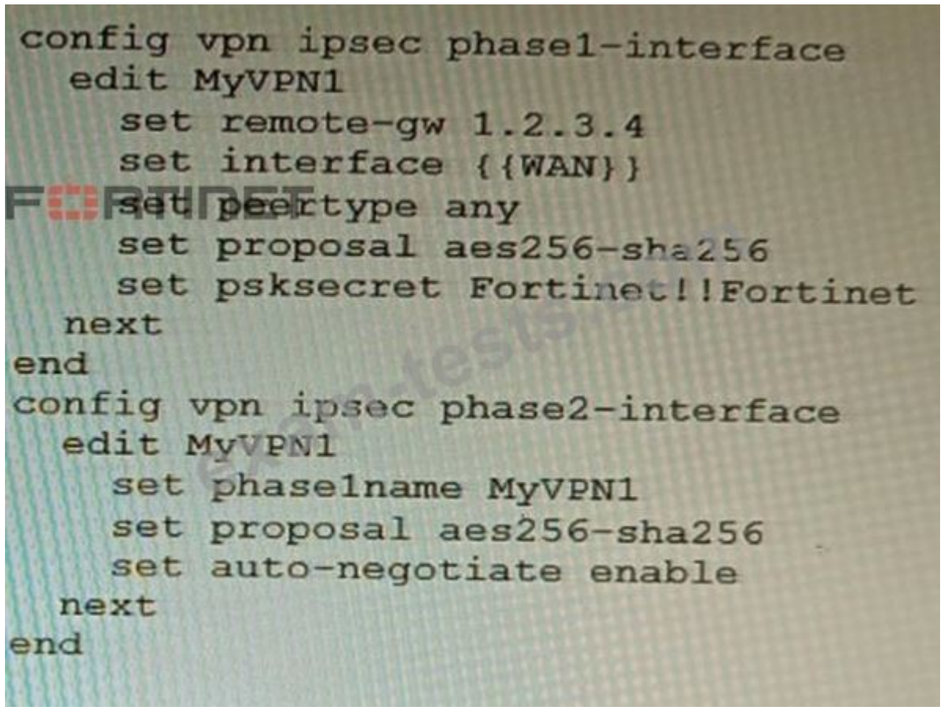
IP as the source address. This avoids NAT issues and ensures optimal DNS performance. References: https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan/19662/sd-wan

NEW QUESTION: 27
Refer to the exhibit, which shows a VPN topology.



The device IP 10.1.100.40 downloads a file from the FTP server IP 192.168.4.50 Referring to the exhibit, what will be the traffic flow behavior if ADVPN is configured in this environment?
A. All the session traffic will pass through the Hub
B. The TCP port 21 must be allowed on the NAT Device2
C. ADVPN is not supported when spokes are behind NAT
D. Spoke1 will establish an ADVPN shortcut to Spoke2
Answer: D (LEAVE A REPLY)
D is correct because Spoke1 will establish an ADVPN shortcut to Spoke2 when it detects that there is a demand for traffic between them. This is explained in the Fortinet Community article on Technical Tip: Fortinet Auto Discovery VPN (ADVPN) under Summary - ADVPN sequence of events. Reference: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Fortinet-Auto-Discovery-VPN-ADVPN/ta-p/195698

NEW QUESTION: 28
Refer to the exhibit.



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 Jinja template will automatically map the interface with "WAN" role on the managed FortiGate.

B. The template will work if you change the variable format to $(WAN).

C. The template will work if you change the variable format to {{ WAN }}.

D. The administrator must first manually map the interface for each device with a meta field.

E. The template will fail because this configuration can only be applied with a CLI or TCL script.

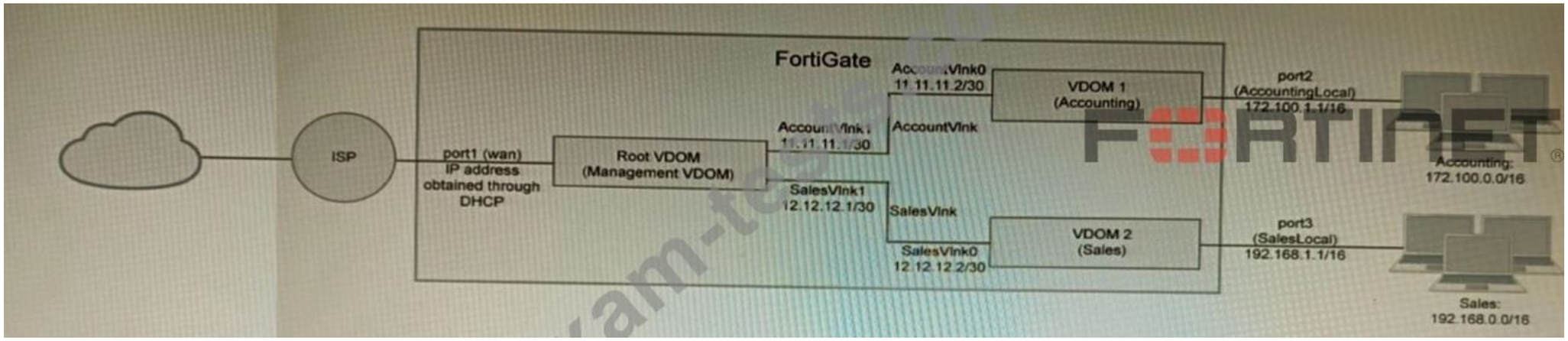
Answer: (SHOW ANSWER)

The Jinja template will not automatically map the interface with "WAN" role on the managed FortiGate. The administrator must first manually map the interface for each device with a meta field.

The template will work if you change the variable format to {{ WAN }}. The {{ }} syntax is used to define a variable in a Jinja template.

NEW QUESTION: 29

Refer to the exhibit.



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. AccountVInk and SalesVInk are standard VDOM links in Ethernet mode.

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

A. You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode

B. Traffic on AccountVInk and SalesVInk will not be accelerated.

C. The VDOM links are in Ethernet mode because they have IP addressed assigned on both sides.

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 AccountVInk

Answer: B,D (LEAVE A REPLY)

The FortiGate configuration shown in the exhibit is using virtual domains (VDOMs) enabled in 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. AccountVInk and SalesVInk are standard VDOM links in Ethernet mode. One correct statement about VDOM behavior is that traffic on AccountVInk and SalesVInk will not be accelerated. This is because standard VDOM links do not support hardware acceleration features such as NP6 or CP9 offloading, which can improve performance and throughput for traffic between VDOMs. To enable hardware acceleration for inter-VDOM traffic, non-standard VDOM links such as NP6 or CP9 interfaces should be used instead of standard VDOM links. Another correct statement about VDOM behavior is that Root VDOM is an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs. This is because Admin type VDOMs are special VDOMs that can only be used for management purposes and cannot process any traffic other than management traffic (such as SSH, HTTPS, SNMP, etc.). Traffic type VDOMs are normal VDOMs that can process any kind of traffic (such as firewall policies, VPN tunnels, routing protocols, etc.). By default, Root VDOM is an Admin type VDOM that can manage other Traffic type VDOMs, unless it is converted to a Traffic type VDOM by using the set vdom-admin enable command. Reference: https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/virtual-domains https://docs.fortinet.com/document/fortigate/7.0.0/hardware-acceleration-guide/19662/vdom-links

NEW QUESTION: 30

A retail customer with a FortiADC HA cluster load balancing five webservers 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 a connection-pool to the FortiADC virtual server

B. Disable SSL between the FortiADC and the web servers

C. Add more web servers to the real server poof

D. Change the persistence rule to LB_PERSIS_SSL_SESSJD.

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 31

ments:

```
config vpn ssl settings
    set https-redirect enable
    set servercert "FortiGateLE"
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set port 443
    set source-interface "port1"
    set source-address "all"
    set source-address6 "all"
    set default-portal "no-access"
end

config system global
    set admin-port 80
end

config vpn certificate local
    edit "FortiGateLE"
        set password ENC <redacted>
        set range global
        set enroll-protocol acme2
        set acme-domain "datacenter.acmecorp.com"
        set acme-email "administrator@acmecorp.com"
    next
end

config system acme
    set interface "port1"
    config accounts
        edit "ACME-.letsencrypt.org-0000"
            set status "valid"
            set ca_url "https://acme-
v02.api.letsencrypt.org/directory"
            set email "administrator@acmecorp.com"
    end
end

config firewall address
    edit "h-fortigate_public"
        set subnet 129.11.1.100 255.255.255.255
    next
end

config firewall vip
    edit "fortimail_secure_web_admin"
        set mappedip "10.100.1.5"
        set extintf "port1"
        set portforward enable
        set extport 30443
        set mappedport 443
    next
```

```
    edit "fortimail_web_admin"
        set mappedip "10.100.1.5"
        set extintf "port1"
        set portforward enable
        set extport 30080
        set mappedport 80
    next
end

config firewall policy
    edit 1
        set name "Allow Inbound FortiMail"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr " fortimail_secure_web_admin " "
fortimail_web_admin "
        set schedule "always"
        set service "HTTP" "HTTPS"
        set ssl-ssh-profile "no-inspection"
    next
end
```

* SSLVPN Portal must be accessible on standard HTTPS port (TCP/443)

* Public IP address (129.11.1.100) is assigned to portl

* Datacenter.acmecorp.com resolves to the public IP address assigned to portl The customer has a Let's Encrypt certificate that is going to expire soon and it reports that subsequent attempts to renew that certificate are failing.

Reviewing the requirement and the exhibit, which configuration change below will resolve this issue?

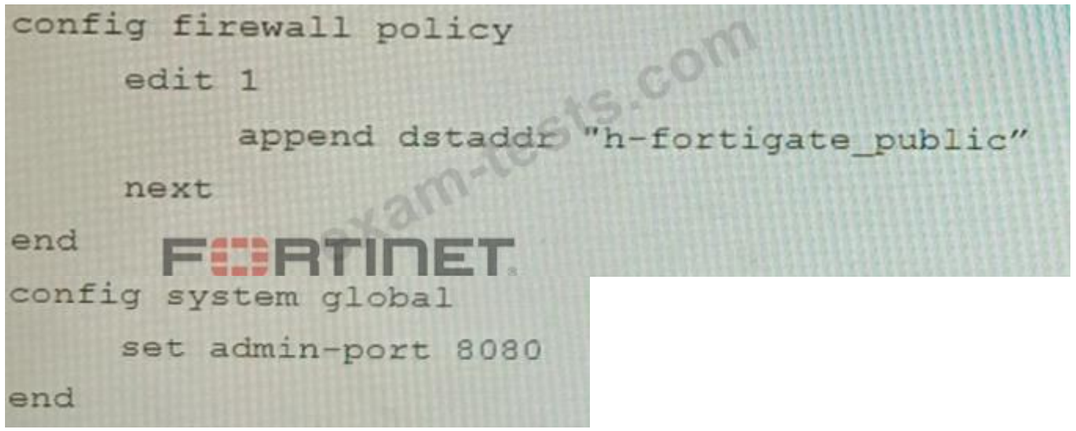
A)

```
config vpn ssl settings
    set https-redirect disable
end
```

B)

```
config system acme
    set interface "port2"
end
```

C)

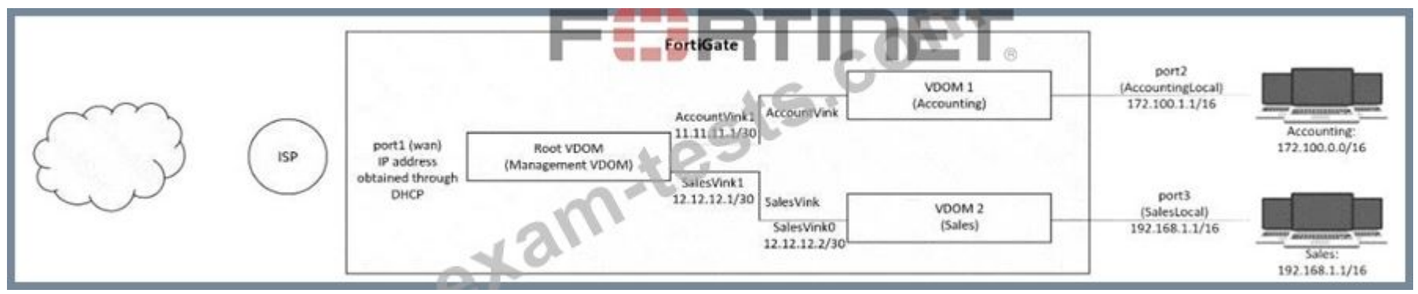


A. Option A
B. Option B
C. Option C
D. Option D
Answer: C (LEAVE A REPLY)
To resolve the issue of failing to renew the Let's Encrypt certificate, the configuration change that is needed is to enable the HTTP-to-HTTPS redirect option in the SSL-VPN settings. This option allows the FortiGate to redirect HTTP requests to HTTPS port 443, which is required for Let's Encrypt to validate the domain ownership and issue a new certificate. By enabling this option, the FortiGate will be able to respond to the HTTP challenge from Let's Encrypt and renew the certificate successfully. Reference: https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103437/inbound-ssl-inspection https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103438/application-detection-on-ssl-offloaded-traffic

NEW QUESTION: 32
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. Create an 1AM 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
C. Migrate all the instances to the same VPC and create 1AM 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.
D. 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
Answer: A,D (LEAVE A REPLY)
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

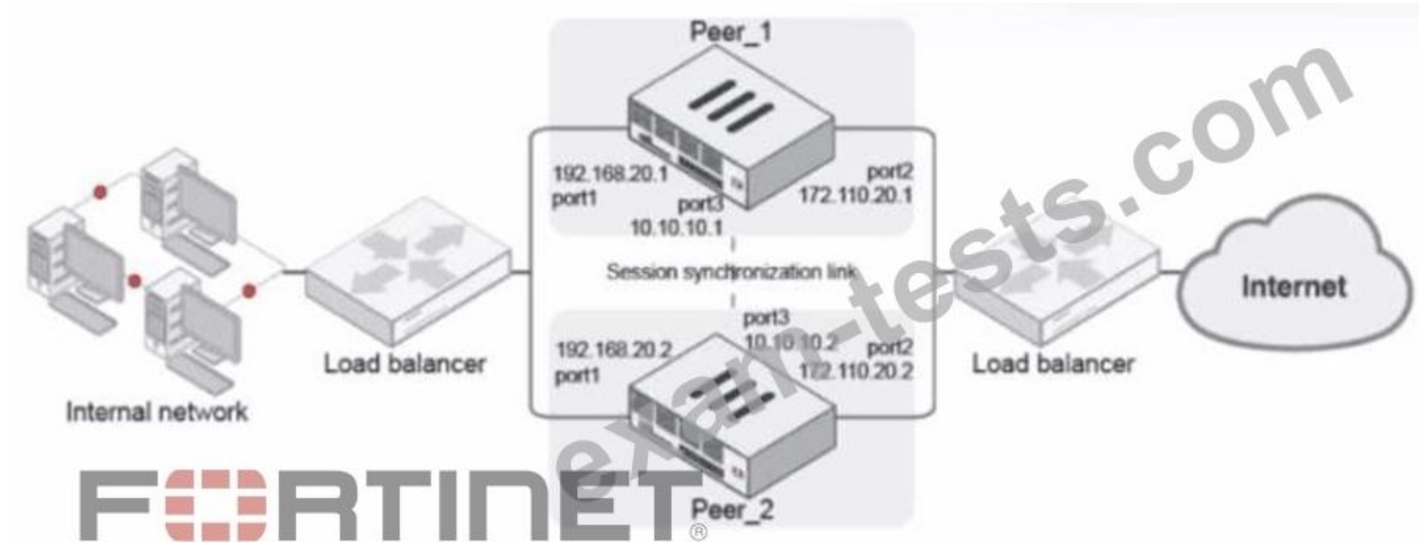
manage the security VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The Transit Gateway acts as a network hub that connects multiple VPCs and on-premises networks. The routing tables can be configured to direct all inter-VPC 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: 33
Refer to the exhibit.



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. AccountVInk and SalesVInk are standard VDOM links in Ethernet mode.
Given the exhibit, which two statements below about VDOM behavior are correct? (Choose two.)
A. Root VDOM is an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs.
B. You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode
C. The VDOM links are in Ethernet mode because they have IP addressed assigned on both sides.
D. Traffic on AccountVInk and SalesVInk will not be accelerated.
E. OSPF routing can be configured between VDOM 1 and Root VDOM without any configuration changes to AccountVInk
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 34
Refer to the exhibit.



Given the exhibit, which two statements about FortiGate FGSP HA cluster behavior are correct? (Choose two.)
A. You can run FortiGate Virtual Router Redundancy Protocol (VRRP) high availability in addition to FGSP simultaneously.
B. You can selectively synchronize only specific sessions between FGSP cluster members.
C. Session synchronization occurs over Layer 3 by default, and if unavailable it will then try Layer 2.
D. Cluster members will upgrade one at a time and failover during firmware upgrades.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 35
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. Security Fabric topology and external connectors
B. FortiClient configuration
C. Certificates
D. Packet capture
E. Interface configuration
Answer: (SHOW ANSWER)

NEW QUESTION: 36
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: 37
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

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

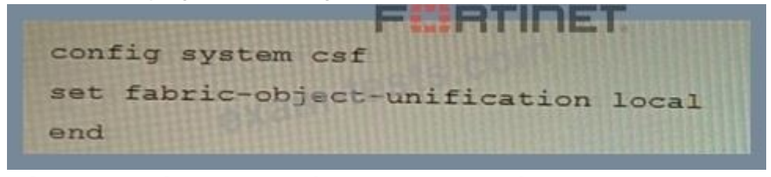
Answer: A (LEAVE A REPLY)

When using inbound SSL inspection, FortiGate needs to present a certificate to the client that matches the requested domain name. If no matching certificate is found in the server-cert list, FortiGate will fall-back to the default Fortinet_CA_SSL certificate, which is self-signed and may trigger a warning on the client browser. Reference: https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103437/inbound-ssl-inspection

NEW QUESTION: 38

Refer to the exhibit.

You have deployed a security fabric with three FortiGate devices as shown in the exhibit. FGT_2 has the following configuration:



FGT_1 and FGT_3 are configured with the default setting. Which statement is true for the synchronization of fabric-objects?

A. Objects from the FortiGate FGT_2 will be synchronized to the upstream FortiGate.

B. Objects from the root FortiGate will only be synchronized to FGT__2.

C. Objects from the root FortiGate will not be synchronized to any downstream FortiGate.

D. Objects from the root FortiGate will only be synchronized to FGT_3.

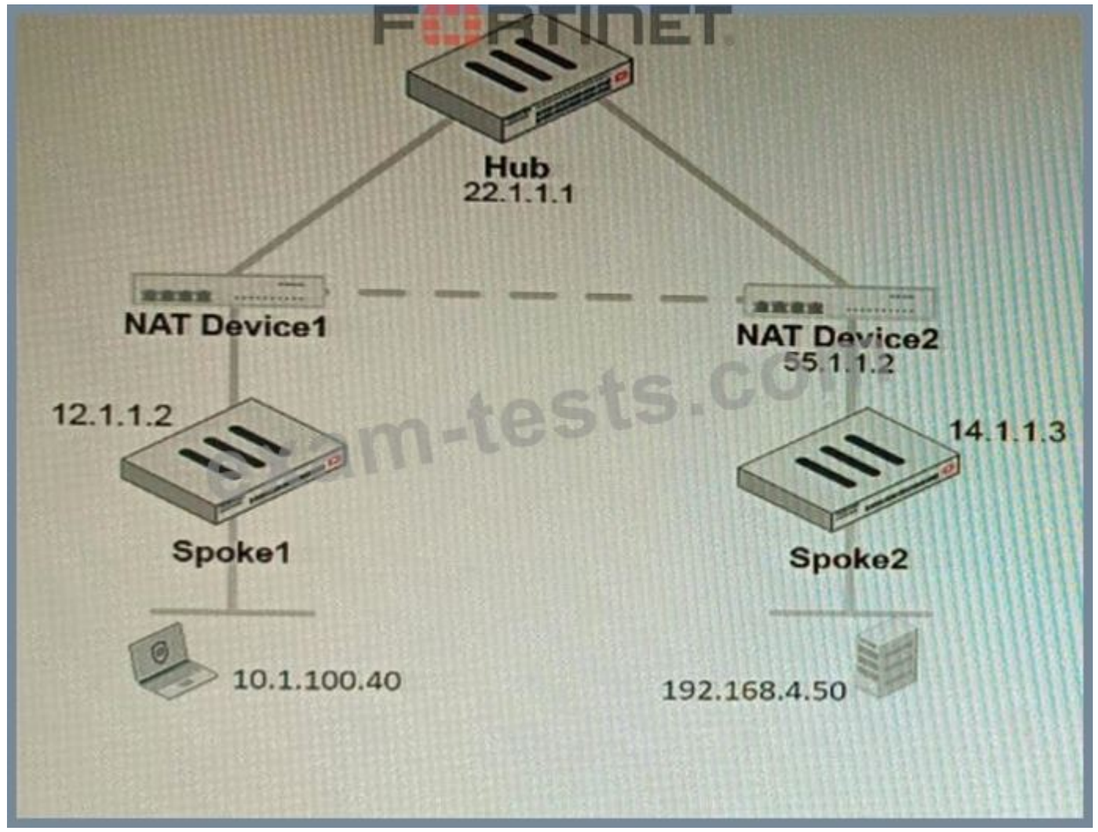
Answer: C (LEAVE A REPLY)

The fabric-object-unification setting on FGT_2 is set to local, which means that objects will not be synchronized to any other FortiGate devices in the security fabric. The default setting for fabric-object-unification is default, which means that objects will be synchronized from the root FortiGate to all downstream FortiGate devices.

Since FGT_2 is not the root FortiGate and the fabric-object-unification setting is set to local, objects from the root FortiGate will not be synchronized to FGT_2.
Reference:

Synchronizing objects across the Security Fabric: https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/880913/synchronizing-objects-across-the-security-fabric

NEW QUESTION: 39
Refer to the exhibit, which shows a VPN topology.



The device IP 10.1.100.40 downloads a file from the FTP server IP 192.168.4.50 Referring to the exhibit, what will be the traffic flow behavior if ADVPN is configured in this environment?
A. All the session traffic will pass through the Hub
B. The TCP port 21 must be allowed on the NAT Device2
C. ADVPN is not supported when spokes are behind NAT
D. Spoke1 will establish an ADVPN shortcut to Spoke2
Answer: D (LEAVE A REPLY)
D is correct because Spoke1 will establish an ADVPN shortcut to Spoke2 when it detects that there is a demand for traffic between them. This is explained in the Fortinet Community article on Technical Tip: Fortinet Auto Discovery VPN (ADVPN) under Summary - ADVPN sequence of events. References:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Fortinet-Auto-Discovery-VPN-ADVPN/ta-p
/195698

NEW QUESTION: 40
Refer to the exhibits.

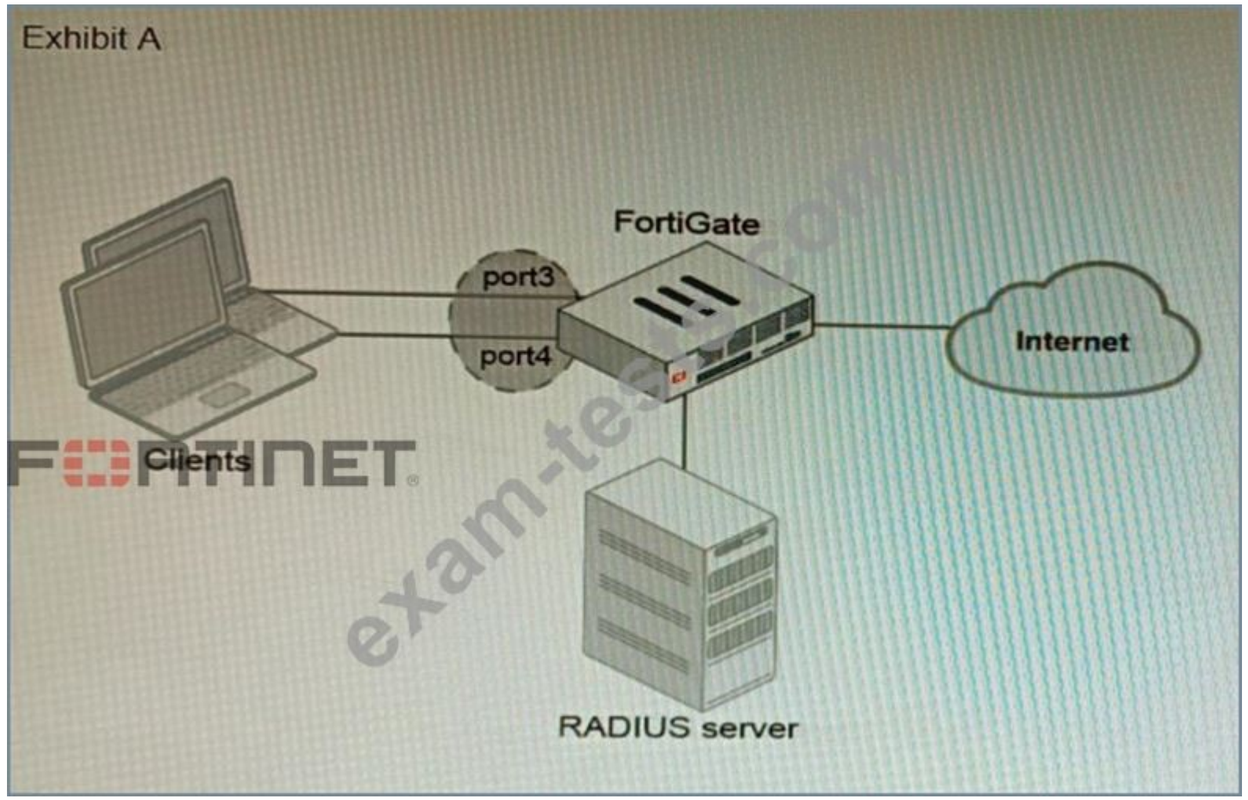


Exhibit A
FortiGate
port3
port4
Internet
Clients
RADIUS server

Exhibit B

```
get hardware npu np6 port-list
Chip XAUI Ports Max Cross-chip
Speed offloading
------ ---- ------- ----- ----------
np6_0 0 port1 1G Yes
0 port2 1G Yes
0 port3 1G Yes
0 port4 1G Yes
0 port5 1G Yes
0 port6 1G Yes
0 port7 1G Yes
0 port8 1G Yes
1 port9 1G Yes
1 port10 1G Yes
...
3 port28 1G Yes
3 s1 1G Yes
3 s2 1G Yes
3 vw1 1G Yes
3 vw2 1G Yes
------ ---- ------- ----- ----------
```


A customer is looking for a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E.

Referring to the exhibits, which two conditions allow authentication to the client devices before assigning an IP address? (Choose two.)

A. FortiGate devices with NP6 and hardware switch interfaces cannot support 802.1X authentication.

B. Devices connected directly to ports 3 and 4 can perform 802 1X authentication.

C. Ports 3 and 4 can be part of different switch interfaces.

D. Client devices must have 802 1X authentication enabled

Answer: B,D (LEAVE A REPLY)

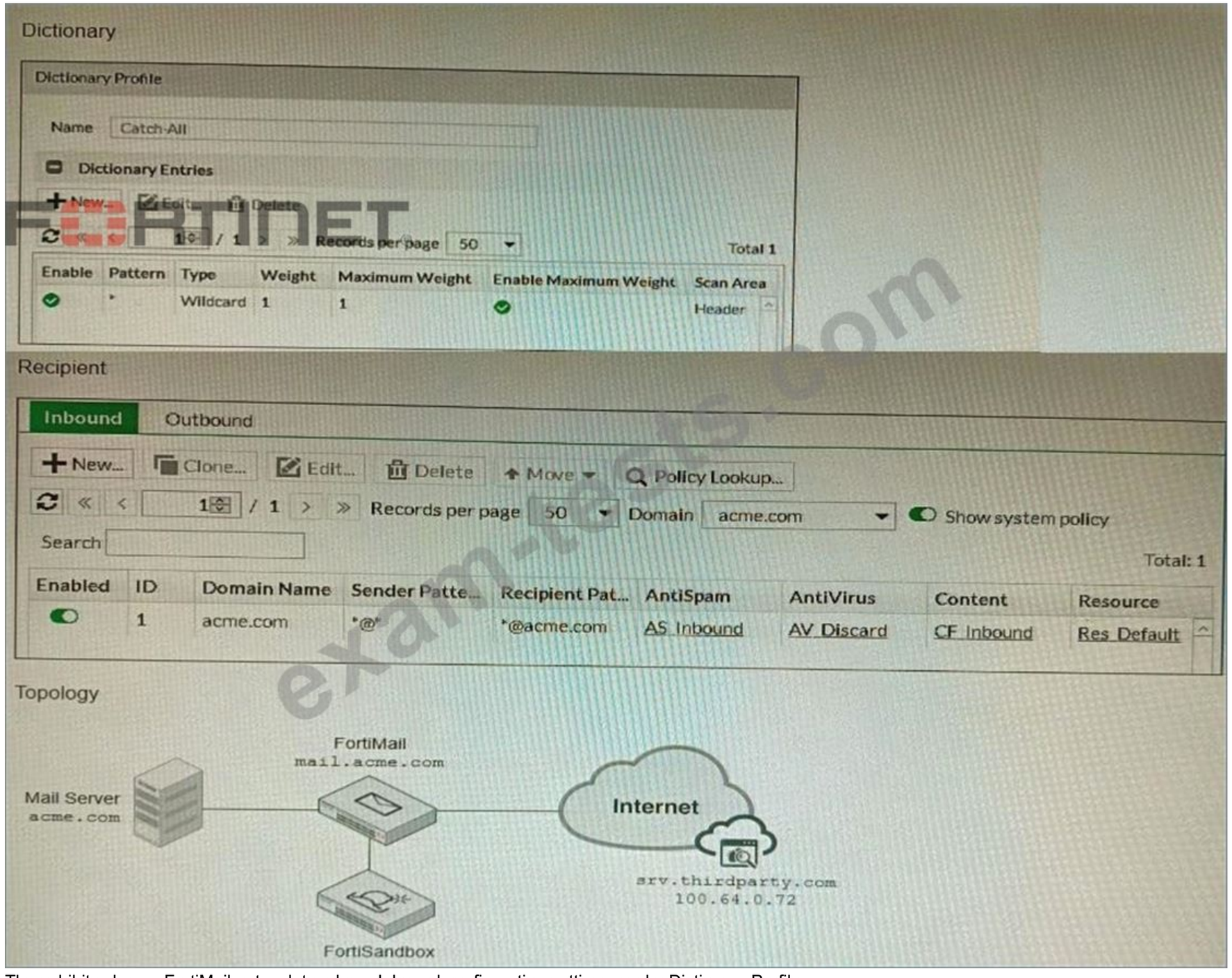
The customer wants to deploy a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E device. A hardware switch interface is an interface that combines multiple physical interfaces into one logical interface, allowing them to act as a single switch with one IP address and one set of security policies. The customer wants to use 802.1X authentication for this solution, which is a standard protocol for port-based network access control (PNAC) that authenticates clients based on their credentials before granting them access to network resources. One condition that allows authentication to the client devices before assigning an IP address is that devices connected directly to ports 3 and 4 can perform 802.1X authentication. This is because ports 3 and 4 are part of the hardware switch interface named "lan", which has an IP address of 10.10.10.254/24 and an inbound SSL inspection profile named "ssl-inspection". The inbound SSL inspection profile enables the FortiGate device to intercept and inspect SSL/TLS traffic from clients before forwarding it to servers, which allows it to apply security policies and features such as antivirus, web filtering, application control, etc. However, before performing SSL inspection, the FortiGate device needs to authenticate the clients using 802.1X authentication, which requires the clients to send their credentials (such as username and password) to the FortiGate device over a secure EAP (Extensible Authentication Protocol) channel. The FortiGate device then verifies the credentials with an authentication server (such as RADIUS or LDAP) and grants or denies access to the clients based on the authentication result. Therefore, devices connected directly to ports 3 and 4 can perform 802.1X authentication before assigning an IP address. Another condition that allows authentication to the client devices before assigning an IP address is that client devices must have 802.1X authentication enabled. This is because 802.1X authentication is a mutual process that requires both the client devices and the FortiGate device to support and enable it. The client devices must have 802.1X authentication enabled in their network settings, which allows them to initiate the authentication process

when they connect to the hardware switch interface of the FortiGate device. The client devices must also have an 802.1X supplicant software installed, which is a program that runs on the client devices and handles the communication with the FortiGate device using EAP messages. The client devices must also have a trusted certificate installed, which is used to verify the identity of the FortiGate device and establish a secure EAP channel. Therefore, client devices must have 802.1X authentication enabled before assigning an IP address. References: https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/hardware-switch-interfaces https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/802-1x-authentication

NEW QUESTION: 41
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: C (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/networking

NEW QUESTION: 42
Wh.ch feature must you enable on the BGP neighbors to accomplish this goal?
A. Graceful-restart
B. Deterministic-med
C. Synchronization
D. Soft-reconfiguration
Answer: A (LEAVE A REPLY)
Graceful-restart is a feature that allows BGP neighbors to maintain their routing information during a BGP restart or failover event, without disrupting traffic forwarding or causing route flaps. Graceful-restart works by allowing a BGP speaker (the restarting router) to notify its neighbors (the helper routers) that it is about to restart or failover, and request them to preserve their routing information and forwarding state for a certain period of time (the restart time). The helper routers then mark the routes learned from the restarting router as stale, but keep them in their routing table and continue forwarding traffic based on them until they receive an end-of-RIB marker from the restarting router or until the restart time expires. This way, graceful-restart can minimize traffic disruption and routing instability during a BGP restart or failover event. Reference: https://docs.fortinet.com/document/fortigate/7.0.0/cookbook/19662/bgp-graceful-restart

NEW QUESTION: 43
Refer to the exhibits.



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.

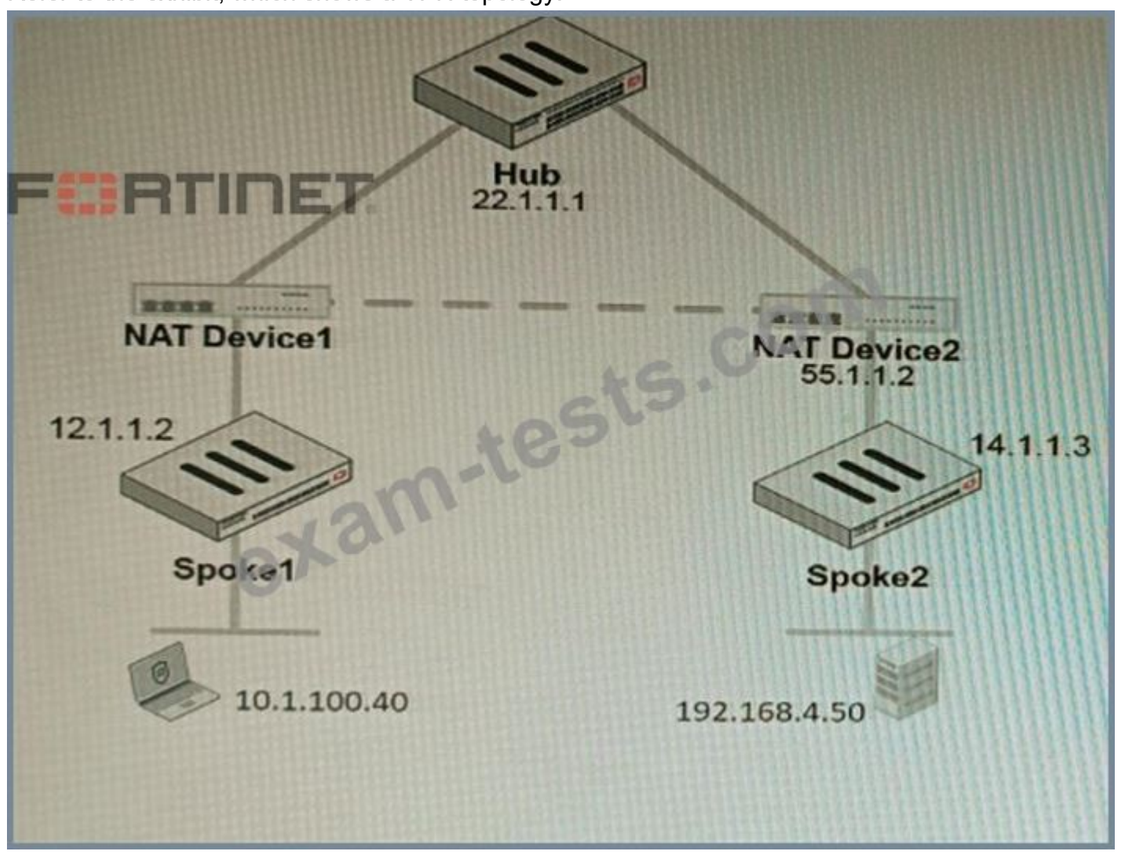
Which three configuration tasks must be performed to meet these requirements? (Choose three.)
A. Change the scan order in FML-GW to antispam-sandbox-content.
B. Apply the Catch-Ail profile to the CFInbound profile and configure a content action profile to deliver to the srv. thirdparty. com FQDN
C. Create 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-AII 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: 44
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. FortiOS cannot accept SIP traffic if both the SIP Session Helper and the application layer gateway (ALG) are disabled.
B. By default, VoIP traffic will be processed using the SIP Session Helper.
C. Rate tracking of SIP requests is only possible when the application layer gateway (ALG) is set to Flow mode.
D. Restricting SIP requests is only possible when using the SIP Session Helper.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 45
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: D (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. Reference: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/856212/nac-lan-segments-7-0-1

NEW QUESTION: 46

Refer to the exhibit, which shows a VPN topology.



The device IP 10.1.100.40 downloads a file from the FTP server IP 192.168.4.50 Referring to the exhibit, what will be the traffic flow behavior if ADVPN is configured in this environment?

A. All the session traffic will pass through the Hub

B. The TCP port 21 must be allowed on the NAT Device2

C. ADVPN is not supported when spokes are behind NAT

D. Spoke1 will establish an ADVPN shortcut to Spoke2

Answer: (SHOW ANSWER)

D is correct because Spoke1 will establish an ADVPN shortcut to Spoke2 when it detects that there is a demand for traffic between them. This is explained in the Fortinet Community article on Technical Tip: Fortinet Auto Discovery VPN (ADVPN) under Summary - ADVPN sequence of events. References:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Fortinet-Auto-Discovery-VPN-ADVPN/ta-p
/195698

NEW QUESTION: 47

Refer to the exhibits.

You are configuring a Let's Encrypt certificate to enable SSL protection to your website. When FortiWeb tries to retrieve the certificate, you receive a certificate status failed, as shown below.

#	Name	Domain	Status	Operation
1	fortinet-com	www.fortinet.com	certificate status failed	

Based on the Server Policy settings shown in the exhibit, which two configuration changes will resolve this issue? (Choose two.)

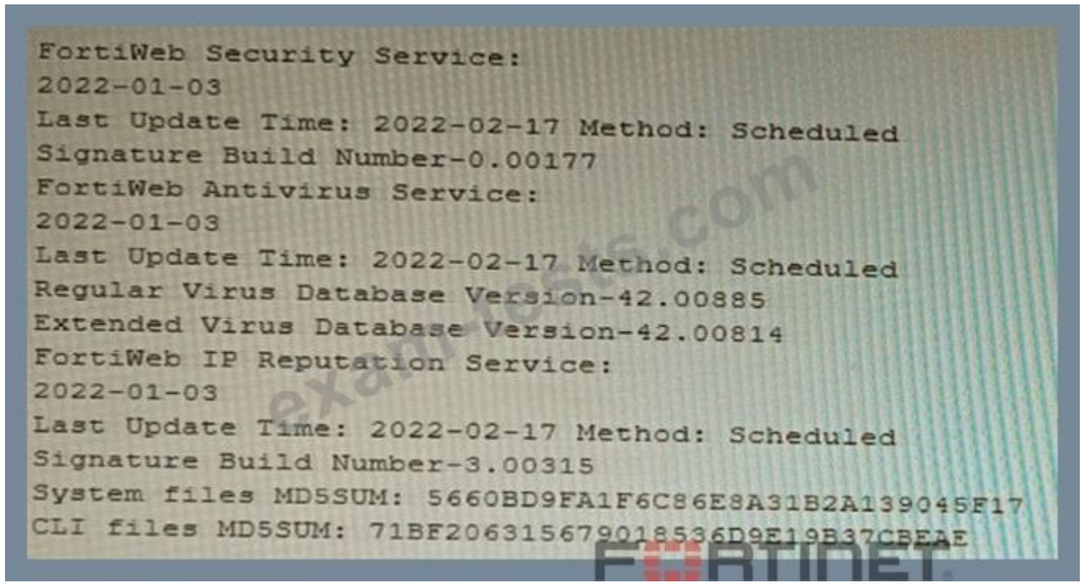
A. Remove the Web Protection Profile from this Server Policy.

B. Disable Redirect HTTP to HTTPS in the Server Policy.
C. Enable HTTP service in the Server Policy.
D. Configure a TXT record of the domain and point to the IP address of the Virtual Server.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 48
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: D (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

NEW QUESTION: 49
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-f lood-traffic and igmps-flood-report settings? (Choose two.)
A. enable on the ISL and FortiLink trunks
B. enable on ICL trunks
C. disable on ICL trunks
D. disable on the ISL and FortiLink trunks
Answer: C,D (LEAVE A REPLY)
A is correct because disabling igmps-flood-traffic and igmps-flood-report on ICL trunks prevents unnecessary multicast traffic from being flooded across the MCLAG cluster members. C is correct because disabling igmps-flood-traffic and igmps-flood-report on the ISL and FortiLink trunks prevents unnecessary multicast traffic from being flooded to other switches or FortiGates that do not have multicast listeners. Reference: https://docs.fortinet.com/document/fortiswitches/6.4.0/administration-guide/381057/multicast-forwarding https://docs.fortinet.com/document/fortiswitches/6.4.0/administration-guide/381057/multicast-forwarding/381058/configuring-multicast-forwarding

NEW QUESTION: 50
Refer to the CLI output:



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: 51

A customer with a FortiDDoS 200F protecting their fibre optic internet connection from incoming traffic sees that all the traffic was dropped by the device even though they were not under a DoS attack. The traffic flow was restored after it was rebooted using the GUI. Which two options will prevent this situation in the future? (Choose two)

A. Change the Adaptive Mode.

B. Create an HA setup with a second FortiDDoS 200F

C. Move the internet connection from the SFP interfaces to the LC interfaces

D. Replace with a FortiDDoS 1500F

Answer: B,D (LEAVE A REPLY)

B is correct because creating an HA setup with a second FortiDDoS 200F will provide redundancy in case one of the devices fails. This will prevent all traffic from being dropped in the event of a failure.

D is correct because the FortiDDoS 1500F has a larger throughput capacity than the FortiDDoS 200F. This means that it will be less likely to drop traffic even under heavy load.

The other options are incorrect. Option A is incorrect because changing the Adaptive Mode will not prevent the device from dropping traffic. Option C is incorrect because moving the internet connection from the SFP interfaces to the LC interfaces will not change the throughput capacity of the device.

References:

FortiDDoS 200F Datasheet | Fortinet Document Library

FortiDDoS 1500F Datasheet | Fortinet Document Library

High Availability (HA) on FortiDDoS | FortiDDoS / FortiOS 7.0.0 - Fortinet Document Library

NEW QUESTION: 52

An HA topology is using the following configuration:

```
config system ha
  set group-id 240
  set group-name "200F"
  set mode a-p
  set hbdev "port3" 50 "port5" 100
  set hb-interval 3
  set hb-lost-threshold 2
  set hello-holddown 100
  set ha-uptime-diff-margin 300
  set override enable
  set priority 200
end
```

Based on this configuration, how long will it take for a failover to be detected by the secondary cluster member?

A. 600ms

B. 200ms

C. 300ms

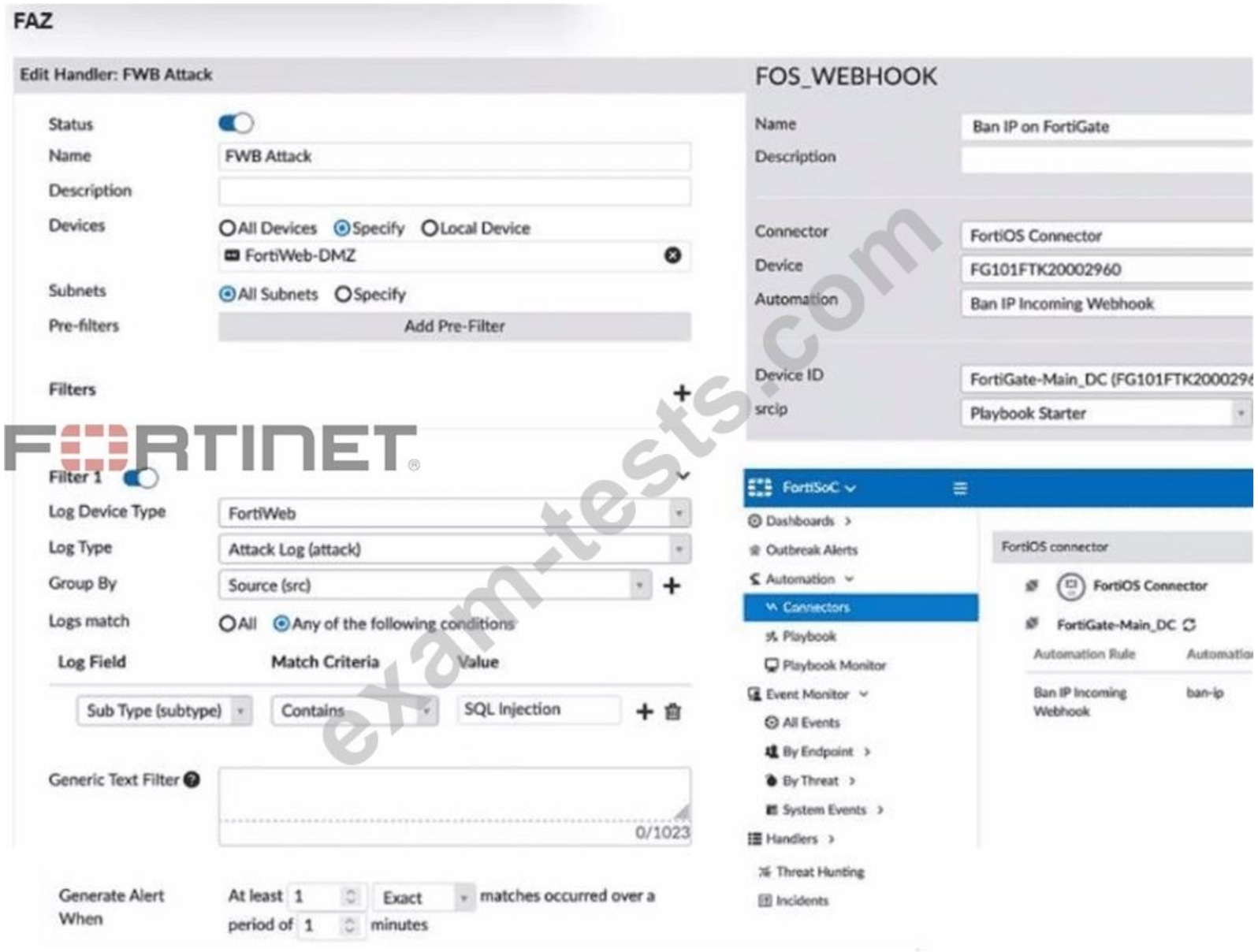
D. 100ms

Answer: (SHOW ANSWER)

The HA topology shown in the exhibit is using link monitoring with two heartbeat interfaces (port3 and port5) and a heartbeat interval of 100ms. Link monitoring is a feature that allows HA failover to occur when one or more monitored interfaces fail or become disconnected. The heartbeat interval is the time between each heartbeat packet sent by an HA cluster unit to other cluster units through heartbeat interfaces. The failover time is determined by multiplying the heartbeat interval by three (the default deadtime value). Therefore, in this case, the failover time is 100ms x 3 = 300ms. Reference: https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/647723/link-monitoring-and-ha-failover-time

NEW QUESTION: 53

Refer to the exhibit.



A customer is trying to setup a Playbook automation using a FortiAnalyzer, FortiWeb and FortiGate. The intention is to have the FortiGate quarantine any source of SQL Injection detected by the FortiWeb. They got the automation stitch to trigger on the FortiGate when simulating an attack to their website, but the quarantine object was created with the IP 0.0.0.0. Referring to the configuration and logs in the exhibits, which two statements are true? (Choose two.)

A. FortiSOC Playbooks combining FortiWeb and FortiGate are not supported.

B. To fix the issue the parameter for script on the Playbook configuration should be epip.

C. The Group By option in the handler should be different to src, so src can be used on the Playbook configuration.

D. To diagnose this issue, you need to use the command diagnose test application oftpd 22.

E. The FortiAnalyzer ADOM Type must be Fabric.

Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 54
Refer to the exhibit showing the history logs from a FortiMail device.

Which FortiMail email security feature can an administrator enable to treat these emails as spam?
A. DKIM validation in a session profile
B. Sender domain validation in a session profile
C. Impersonation analysis in an antispam profile
D. Soft fail SPF validation in an antispam profile
Answer: C (LEAVE A REPLY)
Impersonation analysis is a feature that detects emails that attempt to impersonate a trusted sender, such as a company executive or a well-known brand, by using spoofed or look-alike email addresses. This feature can help prevent phishing and business email compromise (BEC) attacks. Impersonation analysis can be enabled in an antispam profile and applied to a firewall policy. References: https://docs.fortinet.com/document/fortimail/6.4.0/administration-guide/103663/impersonation-analysis

NEW QUESTION: 55
Refer to the exhibit that shows VPN debugging output.

```
ke 0:my_vpn_tunnel:159: out 0BD31A92910D7CA3000000000000000001100200000000000000001440D00005C0000001000000
ke 0:my_vpn_tunnel:159: sent IKE msg (P1_RETRANSMIT): 100.64.101.150:500->100.64.178.130:500, len=324, vrf=
ke 0: comes 100.64.178.130:500->100.64.101.150:500,ifindex=3,vrf=0....
ke 0: IKEv1 exchange=Identity Protection id=8dba779a158c377f/0000000000000000 len=284 vrf=0
ke 0: in 8DBA779A158C377F0000000000000000011002000000000000000011C0D000034000000010000000100000028010100010000
ke 0:8dba779a158c377f/0000000000000000:160: responder: main mode get 1st message...
ke 0:8dba779a158c377f/0000000000000000:160: VID RFC 3947 4A131C81070358455C5728F20E95452F
ke 0:8dba779a158c377f/0000000000000000:160: VID draft-ietf-ipsec-nat-t-ike-03 7D9419A65310CA6F2C179D92155291
ke 0:8dba779a158c377f/0000000000000000:160: VID draft-ietf-ipsec-nat-t-ike-02 CD60464335DF21F87CFDB2FC68B6A4
ke 0:8dba779a158c377f/0000000000000000:160: VID draft-ietf-ipsec-nat-t-ike-02\n 90CB80913EBB696E086381B5EC42
ke 0:8dba779a158c377f/0000000000000000:160: VID draft-ietf-ipsec-nat-t-ike-01 16F6CA16E4A4066D83821A0F0AEAA8
ke 0:8dba779a158c377f/0000000000000000:160: VID draft-ietf-ipsec-nat-t-ike-00 4485152D18B6BBCD0BE8A8469579DE
ke 0:8dba779a158c377f/0000000000000000:160: VID DPD AFCAD71368A1F1C96B8696FC77570100
ke 0:8dba779a158c377f/0000000000000000:160: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ke 0:8dba779a158c377f/0000000000000000:160: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ke 0:8dba779a158c377f/0000000000000000:160: VID FORTIGATE 8299031757A36082C6A621DE00000000
ke 0:8dba779a158c377f/0000000000000000:160: incoming proposal:
ke 0:8dba779a158c377f/0000000000000000:160: proposal id = 0:
ke 0:8dba779a158c377f/0000000000000000:160:   protocol id = ISAKMP:
ke 0:8dba779a158c377f/0000000000000000:160:      trans_id = KEY_IKE.
ke 0:8dba779a158c377f/0000000000000000:160:      encapsulation = IKE/none
ke 0:8dba779a158c377f/0000000000000000:160:         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ke 0:8dba779a158c377f/0000000000000000:160:         type=OAKLEY_HASH_ALG, val=SHA.
ke 0:8dba779a158c377f/0000000000000000:160:         type=AUTH_METHOD, val=PRESHARED_KEY.
ke 0:8dba779a158c377f/0000000000000000:160:         type=OAKLEY_GROUP, val=MODP1536.
ke 0:8dba779a158c377f/0000000000000000:160: ISAKMP SA lifetime=43200
ke 0:8dba779a158c377f/0000000000000000:160: my proposal, gw my_vpn_tunnel:
ke 0:8dba779a158c377f/0000000000000000:160: proposal id = 1:
ke 0:8dba779a158c377f/0000000000000000:160:   protocol id = ISAKMP:
ke 0:8dba779a158c377f/0000000000000000:160:      trans_id = KEY_IKE.
ke 0:8dba779a158c377f/0000000000000000:160:      encapsulation = IKE/none
ke 0:8dba779a158c377f/0000000000000000:160:         type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
ke 0:8dba779a158c377f/0000000000000000:160:         type=OAKLEY_HASH_ALG, val=MD5.
ke 0:8dba779a158c377f/0000000000000000:160:         type=AUTH_METHOD, val=PRESHARED_KEY.
ke 0:8dba779a158c377f/0000000000000000:160:         type=OAKLEY_GROUP, val=MODP2048.
ke 0:8dba779a158c377f/0000000000000000:160: ISAKMP SA lifetime=86400
ke 0:8dba779a158c377f/0000000000000000:160: proposal id = 1:
ke 0:8dba779a158c377f/0000000000000000:160:   protocol id = ISAKMP:
ke 0:8dba779a158c377f/0000000000000000:160:      trans_id = KEY_IKE.
ke 0:8dba779a158c377f/0000000000000000:160:      encapsulation = IKE/none
ke 0:8dba779a158c377f/0000000000000000:160:         type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ke 0:8dba779a158c377f/0000000000000000:160:         type=OAKLEY_HASH_ALG, val=SHA.
ke 0:8dba779a158c377f/0000000000000000:160:         type=AUTH_METHOD, val=PRESHARED_KEY.
ke 0:8dba779a158c377f/0000000000000000:160:         type=OAKLEY_GROUP, val=MODP2048.
ke 0:8dba779a158c377f/0000000000000000:160: ISAKMP SA lifetime=86400
ke 0:8dba779a158c377f/0000000000000000:160: negotiation failure
ke Negotiate ISAKMP SA Error: ike 0:8dba779a158c377f/0000000000000000:160: no SA proposal chosen
```

The VPN tunnel between headquarters and the branch office is not being established.

What is causing the problem?

A. The Phase-1 encryption algorithms are not matching.

B. There is no matching Diffie-Hellman Group.

C. HQ is using IKE v1 and the branch office is using with IKE v2.

D. There is a mismatch in the ISAKMP SA lifetime.

Answer: A (LEAVE A REPLY)

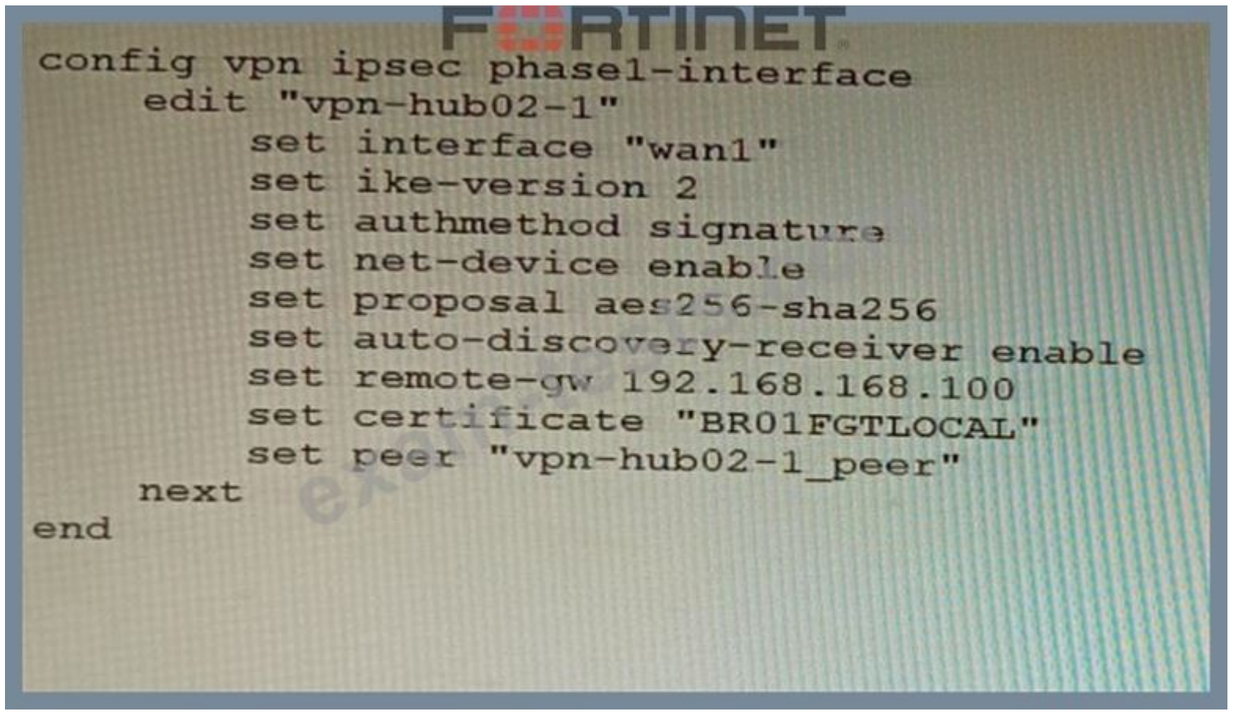
NEW QUESTION: 56

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: (SHOW ANSWER)
Using multiple VPN tunnels and BGP sessions for each internal segment is not scalable and efficient, especially when the number of segments, DCs or internet links per DC increases. A better solution is to use a single VPN tunnel per branch and segment traffic using virtual routing and forwarding (VRF) instances on BGP. This way, each VRF can have its own routing table and BGP session, while sharing the same VPN tunnel. References: https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103439/sd-wan-with-vrf-and-bgp

NEW QUESTION: 57
You are troubleshooting a FortiMail Cloud service integrated with Office 365 where outgoing emails are not reaching the recipients' mail What are two possible reasons for this problem? (Choose two.)
A. The FortiMail access control rule to relay from Office 365 servers FQDN is missing.
B. The FortiMail DKIM key was not set using the Auto Generation option.
C. The FortiMail access control rules to relay from Office 365 servers public IPs are missing.
D. A Mail Flow connector from the Exchange Admin Center has not been set properly to the FortiMail Cloud FQDN.
Answer: C,D (LEAVE A REPLY)
FortiMail Cloud service is a cloud-based email security solution that integrates with Office 365 to provide protection against spam, malware, phishing, data loss, etc. To use FortiMail Cloud service with Office 365, users need to configure both FortiMail Cloud settings and Office 365 settings properly. One possible reason for outgoing emails not reaching the recipients' mailboxes is that the FortiMail access control rules to relay from Office 365 servers public IPs are missing. This means that FortiMail Cloud service does not recognize the Office 365 servers as authorized senders and rejects the outgoing emails. Users need to add the Office 365 servers public IPs to the FortiMail access control rules to allow relaying. Another possible reason for outgoing emails not reaching the recipients' mailboxes is that a Mail Flow connector from the Exchange Admin Center has not been set properly to the FortiMail Cloud FQDN. This means that Office 365 does not route the outgoing emails to the FortiMail Cloud service for scanning and delivery. Users need to create a Mail Flow connector from the Exchange Admin Center and specify the FortiMail Cloud FQDN as the smart host. Reference: https://docs.fortinet.com/document/fortimail-cloud/6.4.0/administration-guide/19662/integrating-fortimail-cloud-with-office-365

NEW QUESTION: 58
Refer to the exhibit.



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 phasei-interface options referenced in the exhibit for the VPN interface to enable this capability? (Choose three.)

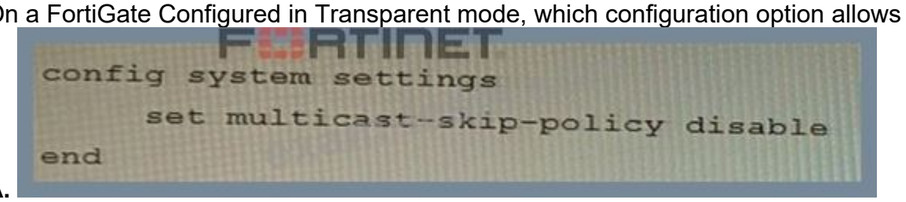
A. set net-device disable
B. set mode-cfg enable
C. set ike-version 1
D. set add-route enable
E. set mode-cfg-allow-client-selector enable

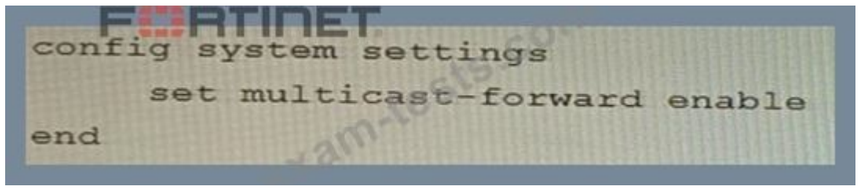
Answer: B,D,E (LEAVE A REPLY)

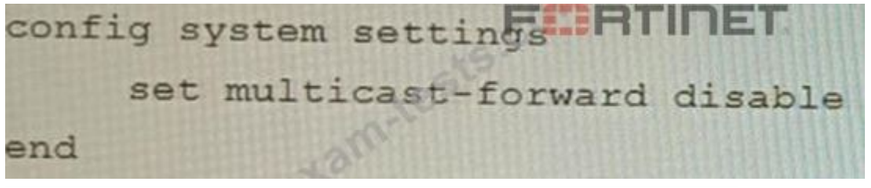
B must be set to enable mode-cfg, which is required for injecting IKE routes on the ADVPN shortcut tunnels.
D must be set to enable add-route, which is the command that actually injects the IKE routes.
E must be set to enable mode-cfg-allow-client-selector, which allows custom phase 2 selectors to be 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

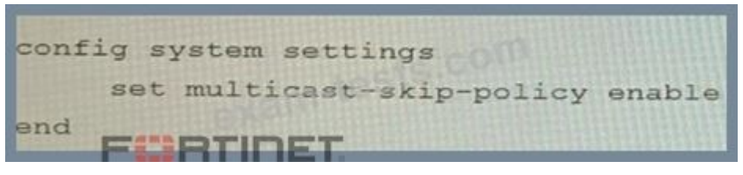
NEW QUESTION: 59

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

A.


B.


C.


D.


Answer: C (LEAVE A REPLY)

To control multicast traffic passing through a FortiGate configured in transparent mode, you can use multicast policies. Multicast policies allow you to filter multicast traffic based on source and destination addresses, protocols, and interfaces. You can also apply security profiles to scan multicast traffic for threats and violations. References: https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/968606/configuring-multicast-forwarding

NEW QUESTION: 60

Refer to the exhibits.

You are configuring a Let's Encrypt certificate to enable SSL protection to your website. When FortiWeb tries to retrieve the certificate, you receive a certificate status failed, as shown below.

#	Name	Domain	Status	Operation
1	fortinet-com	www.fortinet.com	certificate status failed	

Based on the Server Policy settings shown in the exhibit, which two configuration changes will resolve this issue? (Choose two.)

A. Configure a TXT record of the domain and point to the IP address of the Virtual Server.

B. Remove the Web Protection Profile from this Server Policy.

C. Disable Redirect HTTP to HTTPS in the Server Policy.

D. Enable HTTP service in the Server Policy.

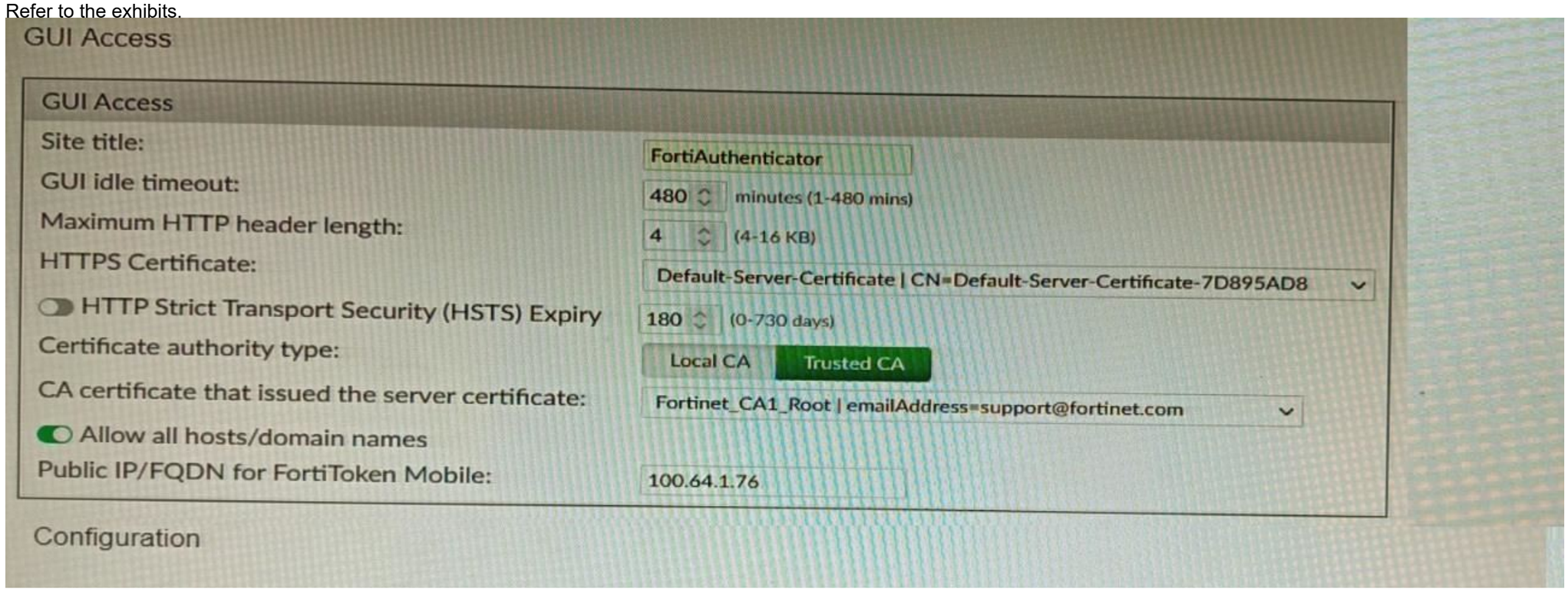
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 61

SD-WAN is configured on a FortiGate. You notice that when one of the internet links has high latency the time to resolve names using DNS from FortiGate is very high.

You must ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work.
What should you configure?
A. Configure two DNS servers and use DNS servers recommended by the two internet providers.
B. Configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server.
C. Configure an SD-WAN rule to the DNS server and use the FortiGate interface IPs in the source address.
D. Configure local out traffic to use the outgoing interface based on SD-WAN rules with a manual defined IP associated to a loopback interface and configure an SD-WAN rule from the loopback to the DNS server.
Answer: B (LEAVE A REPLY)
SD-WAN is a feature that allows users to optimize network performance and reliability by using multiple WAN links and applying rules based on various criteria, such as latency, jitter, packet loss, etc. One way to ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work is to configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server. This means that the FortiGate will use the best WAN link available to send DNS queries to the DNS server according to the SD-WAN rule, and use its own interface IP as the source address. This avoids NAT issues and ensures optimal DNS performance. References:
https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan/19662/sd-wan

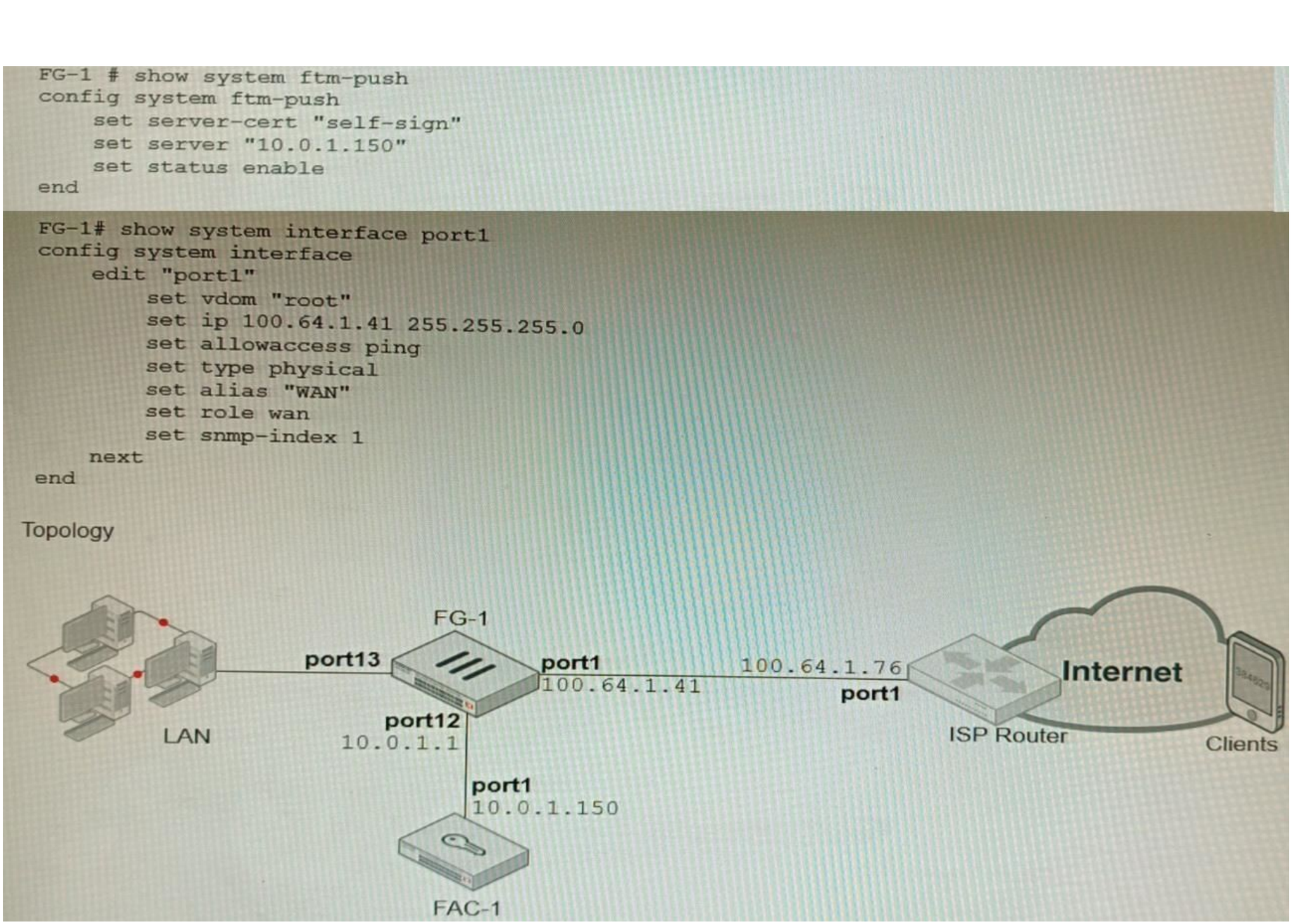
NEW QUESTION: 62
Refer to the exhibits.



```
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: B (LEAVE A REPLY)

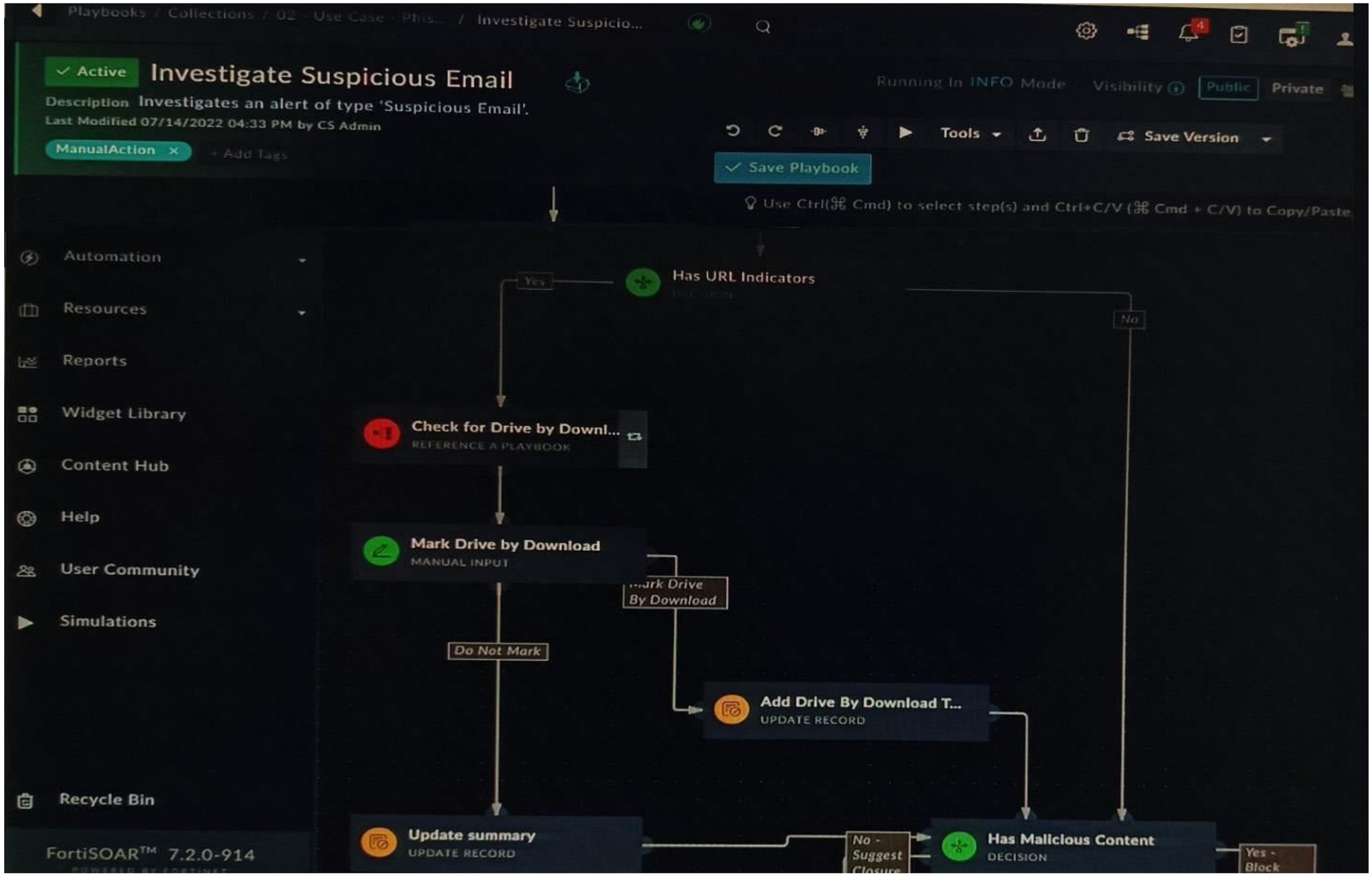
FortiToken push notifications require that the FortiAuthenticator has an internet routable IP address. This is because the FortiAuthenticator uses this IP address to send push notifications to the FortiGate. The other options are not correct. Enabling the ftm access protocol on FG-1 port1 is not necessary for push notifications to work. The ftm-push server setting on FG-1 CLI should already point to the FortiAuthenticator's IP address. The FortiToken public IP setting on FAC-1 is not relevant to push notifications.

Here is a table that summarizes the different options:

Option	Description
Enable the ftm access protocol on FG-1 port1	Not necessary for push notifications to work.
Set the ftm-push server setting on FG-1 CLI to the FortiAuthenticator's IP address	Already done.
Set the FortiToken public IP setting on FAC-1 to 100.64.141	Not relevant to push notifications.
Set the FortiAuthenticator's IP address to an internet routable IP address	Necessary for push notifications to work.

NEW QUESTION: 63

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: (SHOW ANSWER)
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: 64
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: 65
Refer to the exhibit, which shows a Branch1 configuration and routing table.

```
Branch1 # show system sdwan
config system sdwan
    set status enable
    set load-balance-mode source-dest-ip-based
    config zone
        edit "internet"
        next
        edit "overlay"
```

```
    next
end
config members
    edit 1
        set interface "wan1"
            set zone "internet"
    next
    edit 2
        set interface "wan2"
            set zone "internet"
    next
    edit 3
        set interface "vpn1-net"
        set zone "overlay"
    next
    edit 4
        set interface "vpn2-mpls"
        set zone "overlay"
    next
end
 config service
 end
```

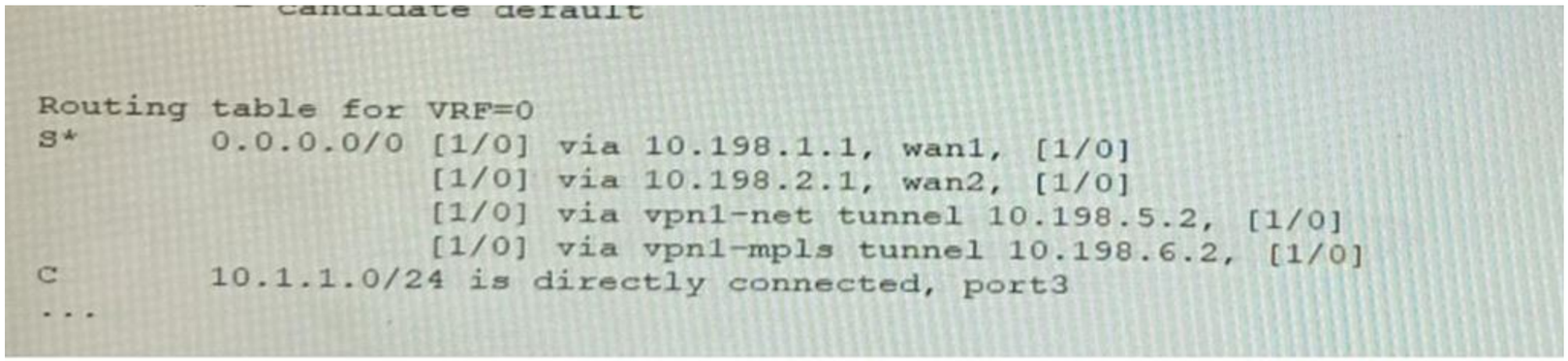
```
end

##############################

Branch1 # show router static
config router static
    edit 0
        set distance 1
        set sdwan-zone "internet" "overlay"
    next
end

##############################
```

```
Branch1 # get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
```



In the SD-WAN implicit rule, you do not want the traffic load balance for the overlay interface when all members are available.
In this scenario, which configuration change will meet this requirement?

A. Change the load-balance-mode to source-ip-based.

B. Create a new static route with the internet sdwan-zone only

C. Configure the cost in each overlay member to 10.

D. Configure the priority in each overlay member to 10.

Answer: D (LEAVE A REPLY)

The default load balancing mode for the SD-WAN implicit rule is source IP based. This means that traffic will be load balanced evenly between the overlay members, regardless of the member's priority.
To prevent traffic from being load balanced, you can configure the priority of each overlay member to 10. This will make the member ineligible for load balancing.
The other options are not correct. Changing the load balancing mode to source-IP based will still result in traffic being load balanced. Creating a new static route with the internet sdwan-zone only will not affect the load balancing of the overlay interface. Configuring the cost in each overlay member to 10 will also not affect the load balancing, as the cost is only used when the implicit rule cannot find a match for the destination IP address.

Option	Description
Change the load-balance-mode to source-ip-based	Will still result in traffic being load balanced.
Create a new static route with the internet sdwan-zone only	Will not affect the load balancing of the overlay interface.
Configure the cost in each overlay member to 10	Will not affect the load balancing, as the cost is only used when the implicit rule cannot find a match for the destination IP address.
Configure the priority in each overlay member to 10	Will prevent traffic from being load balanced.

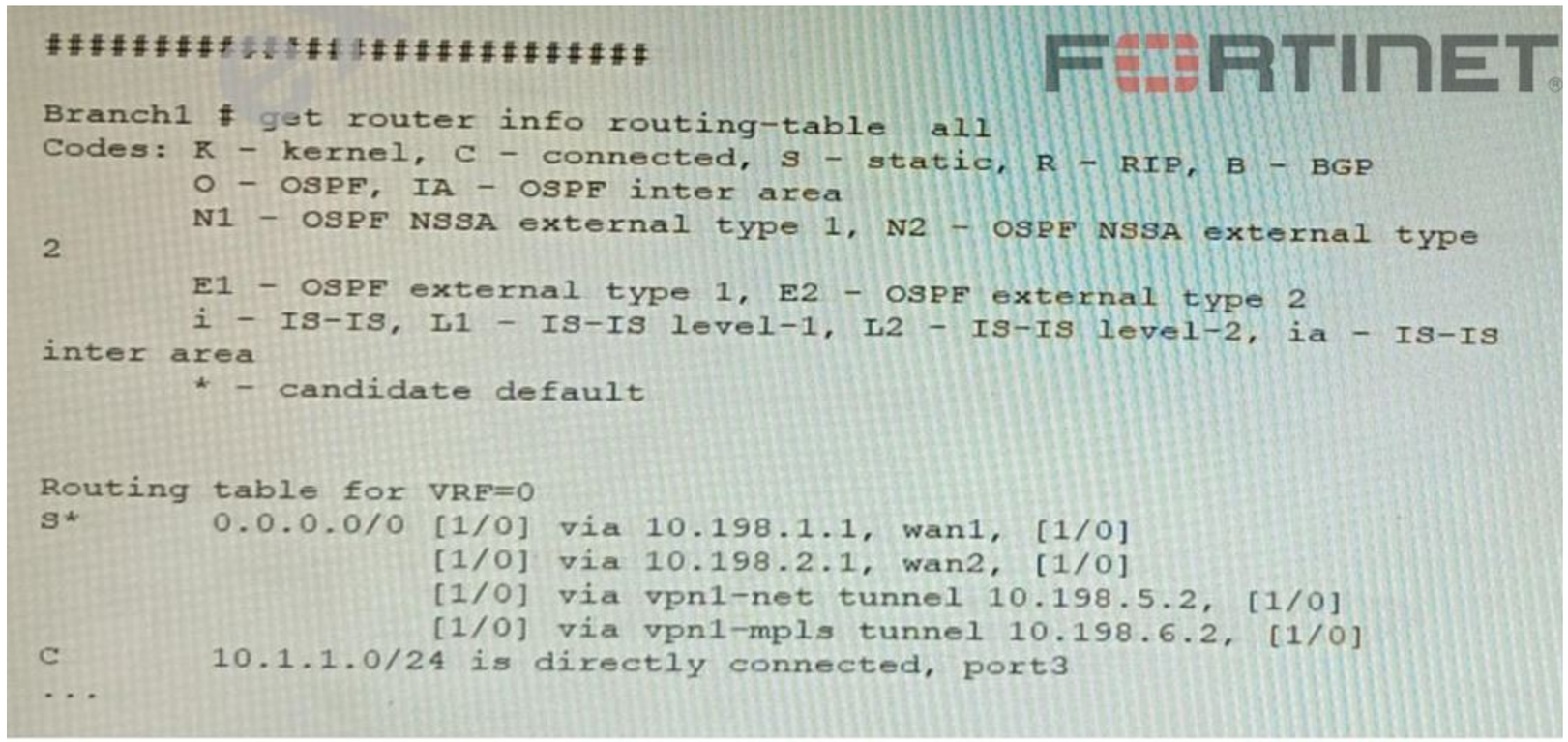
NEW QUESTION: 66

Refer to the exhibit, which shows a Branch1 configuration and routing table.

```
Branch1 # show system sdwan
config system sdwan
    set status enable
    set load-balance-mode source-dest-ip-based
    config zone
        edit "internet"
        next
        edit "overlay"
        next
    end
    config members
        edit 1
            set interface "wan1"
                set zone "internet"
        next
        edit 2
            set interface "wan2"
                set zone "internet"
        next
        edit 3
            set interface "vpn1-net"
            set zone "overlay"
        next
        edit 4
            set interface "vpn2-mpls"
            set zone "overlay"
        next
    end
     config service
     end
end

##############################

Branch1 # show router static
config router static
    edit 0
        set distance 1
        set sdwan-zone "internet" "overlay"
    next
end
```

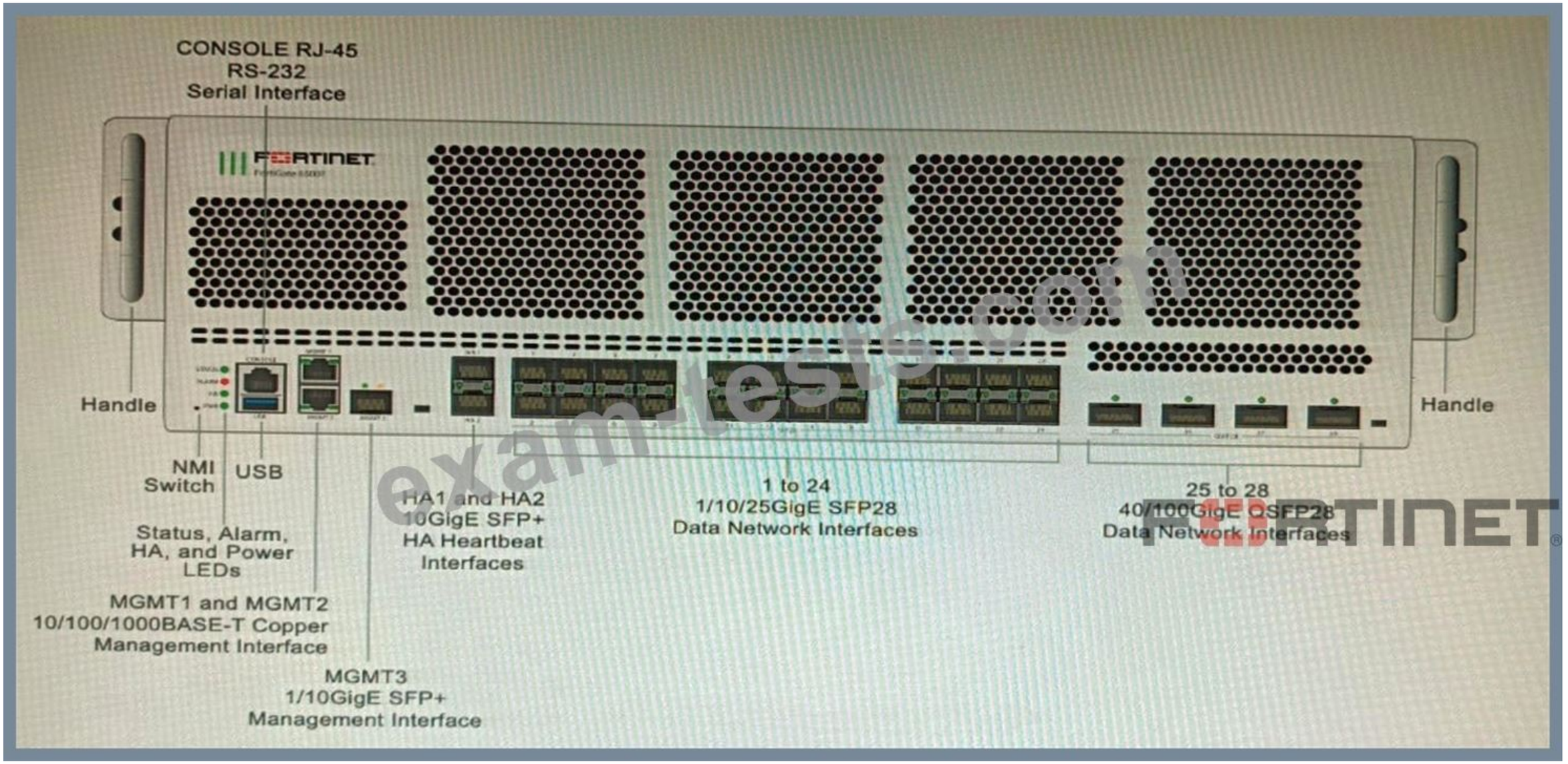


```
Branch1 # get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default


Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 10.198.1.1, wan1, [1/0]
                  [1/0] via 10.198.2.1, wan2, [1/0]
                  [1/0] via vpn1-net tunnel 10.198.5.2, [1/0]
                  [1/0] via vpn1-mpls tunnel 10.198.6.2, [1/0]
C       10.1.1.0/24 is directly connected, port3
...
```

In the SD-WAN implicit rule, you do not want the traffic load balance for the overlay interface when all members are available.
In this scenario, which configuration change will meet this requirement?
A. Change the load-balance-mode to source-ip-based.
B. Create a new static route with the internet sdwan-zone only
C. Configure the cost in each overlay member to 10.
D. Configure the priority in each overlay member to 10.
Answer: C (LEAVE A REPLY)
The SD-WAN implicit rule is a default rule that applies to all traffic that does not match any explicit SD-WAN rule. The SD-WAN implicit rule uses the best quality strategy, which selects the SD-WAN member with the best measured quality based on the performance SLA metrics. This means that the traffic load balance for the overlay interface will depend on the quality of each overlay member, which may vary over time. However, if the requirement is to minimize the overhead on the device for WAN traffic and avoid load balancing for the overlay interface when all members are available, one option is to configure the cost in each overlay member to 10. The cost is a parameter that can be used to influence the selection of an SD-WAN member by adding a penalty value to its quality score. By configuring the same cost value for all overlay members, the quality score of each member will be reduced by the same amount, which will make them less preferable than the underlay members. This way, the SD-WAN implicit rule will select the underlay members first, unless they are unavailable or out of SLA, and only use the overlay members as a backup option. Reference: https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan/19662/sd-wan-rules

NEW QUESTION: 67
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 25 to 28

B. Connect the switch on any interface between ports 21 to 24

C. Connect the switch on any interface between ports 5 to 8.

D. Connect the switch on any interface between ports 1 to 4

Answer: A (LEAVE A REPLY)

NEW QUESTION: 68

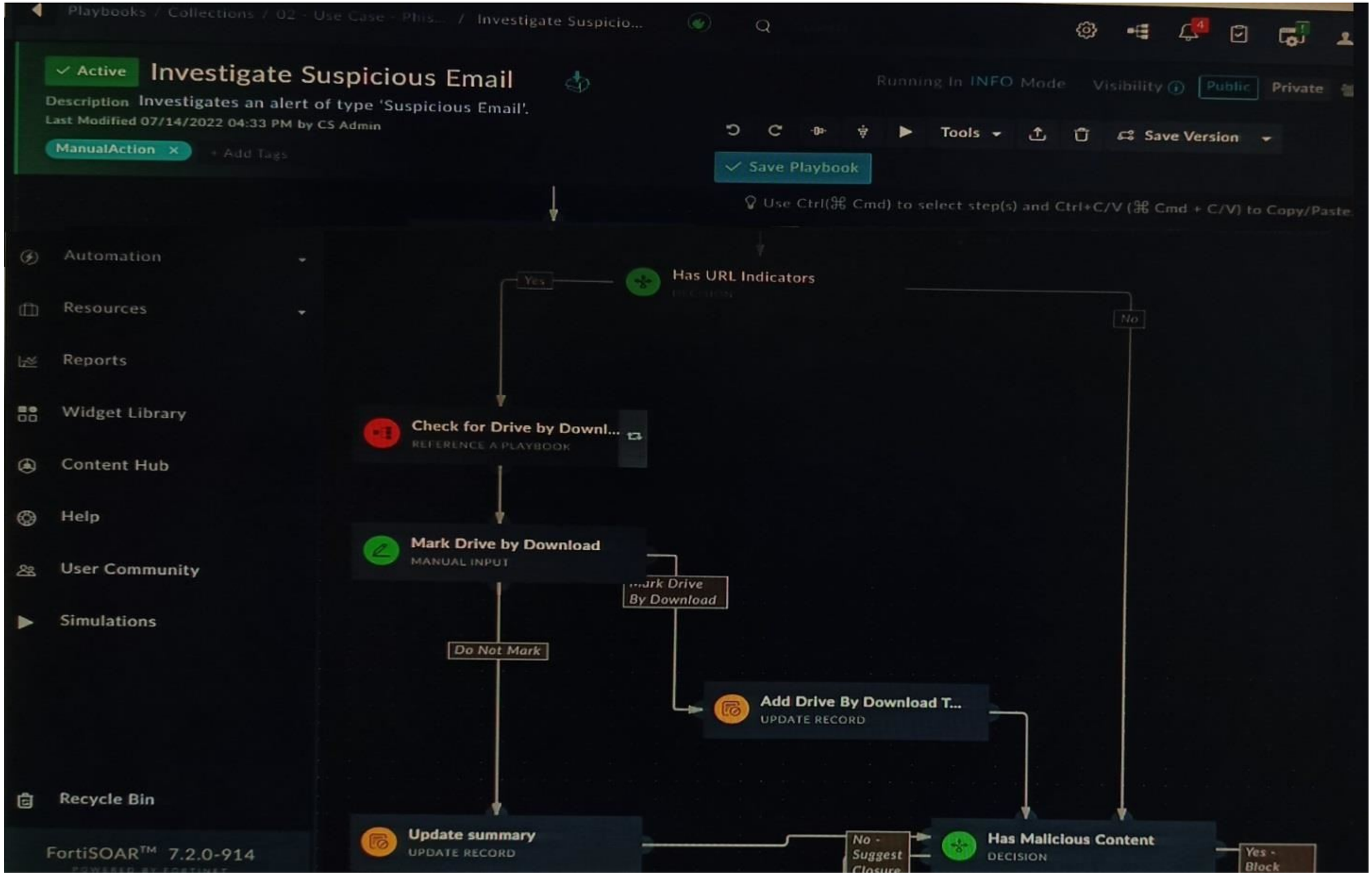
A customer's cybersecurity department needs to implement security for the traffic between two VPCs in AWS, but these belong to different departments within the company. The company uses a single region for all their VPCs.
Which two actions will achieve this requirement while keeping separate management 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. Create an 1AM 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
C. Migrate all the instances to the same VPC and create 1AM 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.
D. 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
Answer: A,D (LEAVE A REPLY)
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: 69
Refer to the exhibit showing the history logs from a FortiMail device.

Which FortiMail email security feature can an administrator enable to treat these emails as spam?
A. DKIM validation in a session profile
B. Sender domain validation in a session profile
C. Impersonation analysis in an antispam profile
D. Soft fail SPF validation in an antispam profile
Answer: (SHOW ANSWER)
Impersonation analysis is a feature that detects emails that attempt to impersonate a trusted sender, such as a company executive or a well-known brand, by using spoofed or look-alike email addresses. This feature can help prevent phishing and business email compromise (BEC) attacks. Impersonation analysis can be enabled in an antispam profile and applied to a firewall policy.
References:https://docs.fortinet.com/document/fortimail

/6.4.0/administration-guide/103663/impersonation-analysis
https://docs.fortinet.com/document/fortimail/7.2.0/cookbook/221814/protecting-against-email-impersonation- in-fortimail

NEW QUESTION: 70
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: B (LEAVE A REPLY)
To intervene in a suspicious e-mail alert on FortiSOAR, after reviewing the executed playbook, the next step is to click on the notification icon on FortiSOAR GUI and run the pending input action. The notification icon will show a badge with the number of pending input actions that require manual intervention from the user. The user can click on the notification icon and see a list of pending input actions, along with their details, such as playbook name, step name, record ID, and trigger time. The user can then click on the Run button to execute the pending input action and resume the playbook execution. Reference: https://docs.fortinet.com/document/fortisoar/7.0.0/administration-guide/103440/automation-stitches https://docs.fortinet.com/document/fortisoar/7.0.0/administration-guide/103441/incoming-webhook

NEW QUESTION: 71
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
```

B.

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

C.

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

D.

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


Answer: B (LEAVE A REPLY)

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

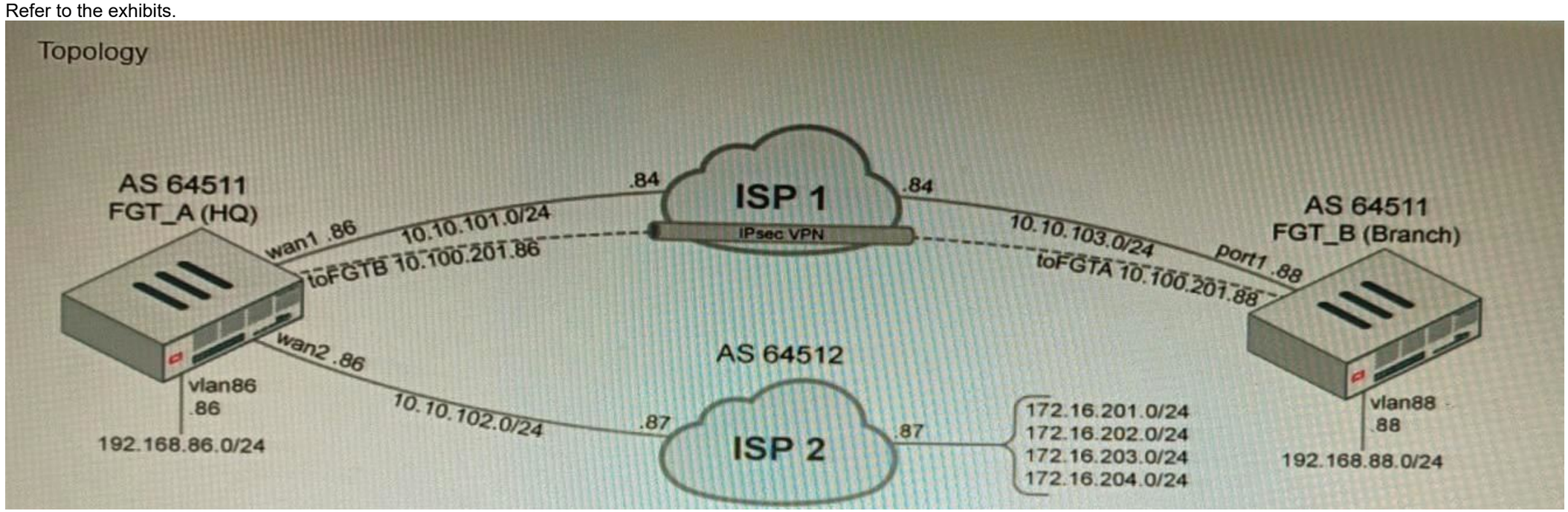
This means that FGT_3 will participate in the DR/BDR election process with the other OSPF routers on the same LAN segment. However, this is not desirable because FGT_3 is a new device that needs to be added to the OSPF network without affecting the existing DR/BDR election. Therefore, to make sure FGT_3 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

NEW QUESTION: 72

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. 172,620,64,27

D. 172.16.204.64/27

Answer: (SHOW ANSWER)

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: 73

Refer to the exhibit, which shows a FortiGate configuration snippet.

```
config system sdwan
    set status enable
    config members
        edit 1
            set interface "wan1"
            set priority 1
        next
        edit 2
            set interface "USA VPN"
            set priority 2
        next
    end
    config service
         edit 1
              set name "USA Browsing"
              set dst "all"
              set src "all"
              set priority-members 2
         next
    end
end
config system automation-action
    edit "Enable USA Browsing script"
        set action-type cli-script
        set script "config system sdwan
    config service
        edit 1
            set status enable
        next
    end
end"
        set accprofile "super_admin"
    next
end
```

A customer in Costa Rica has a FortiGate with SD-WAN configured to use a VPN connection to the United States to browse the internet using a public IP from that country. They would like to enable the SD-WAN rule using a webhook.

Which configuration must be added to the FortiGate, and which type of HTTP request must be used to accomplish this? (Choose two.)

A.

```
Issue an HTTP POST to
'https://192.168.1.99/api/v2/monitor/system/automation-
stitch/webhook/Enable%20USA%20Browsing'
```

B.

Add to the FortiGate the configuration:

```
config system automation-trigger
  edit "Enable USA Browsing"
    set event-type incoming-webhook
  next
end
config system automation-stitch
  edit "Enable USA Browsing stitch"
    set trigger "Enable USA Browsing"
    config actions
      edit 1
        set action "Enable USA Browsing script"
        set required enable
      next
    end
  next
```

C.

```
Issue an HTTP GET to
'https://192.168.1.99/api/v2/monitor/system/automation-
stitch/webhook/Enable%20USA%20Browsing'
```

D.

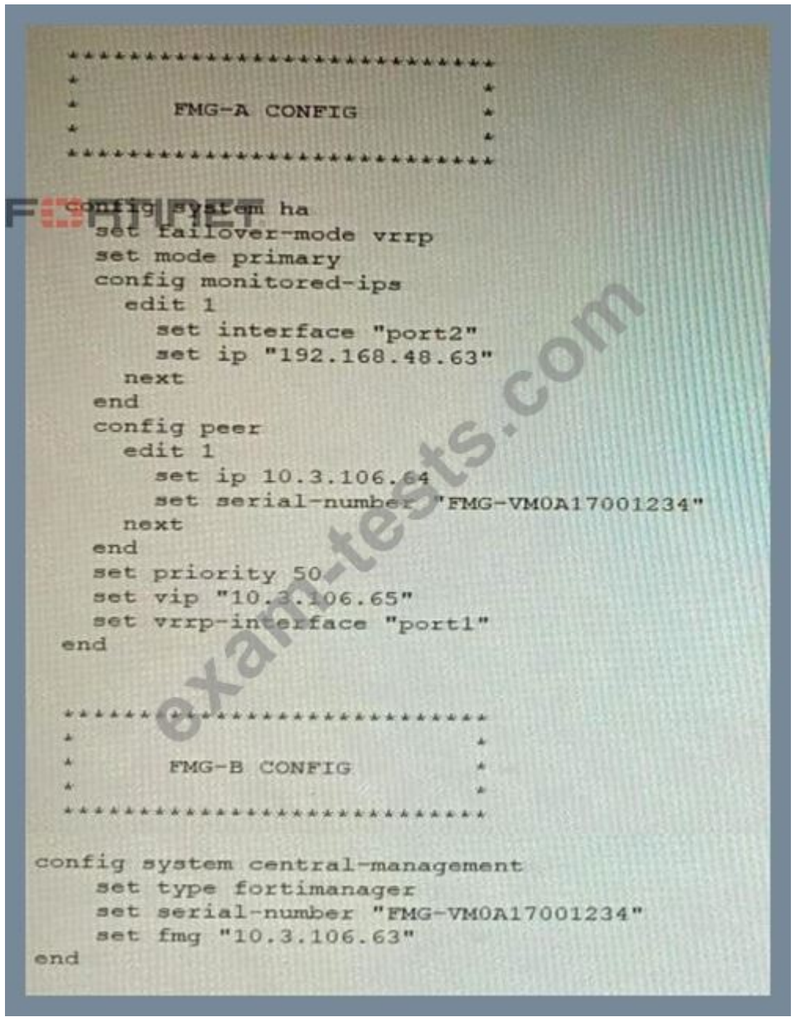
Add to the FortiGate the configuration:

```
config system automation-trigger
  edit "Enable USA Browsing webhook"
    set event-type incoming-webhook
  next
end
config system automation-stitch
  edit "Enable USA Browsing"
    set trigger "Enable USA Browsing webhook"
    config actions
      edit 1
        set action "Enable USA Browsing script"
        set required enable
      next
      end
    next
  end
```

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 74

Refer to the exhibit showing FortiGate configurations



FortiManager VM high availability (HA) is not functioning as expected after being added to an existing deployment.

The administrator finds that VRRP HA mode is selected, but primary and secondary roles are greyed out in the GUI The managed devices never show online when FMG-B becomes primary, but they will show online whenever the FMG-A becomes primary.

What change will correct HA functionality in this scenario?

A. Change the FortiManager IP address on the managed FortiGate to 10.3.106.65.

B. Make the monitored IP to match on both FortiManager devices.

C. Unset the primary and secondary roles in the FortiManager CLI configuration so VRRP will decide who is primary.

D. Change the priority of FMG-A to be numerically lower for higher preference

Answer: A (LEAVE A REPLY)

https://community.fortinet.com/t5/FortiManager/Technical-Tip-FortiManager-VRRP-HA-configuration-in- Azure-Public/ta-p/267503https://community.fortinet.com/t5/FortiManager/Technical-Tip-FortiManager-HA-setup-and-troubleshooting/ta-p/222998

NEW QUESTION: 75

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. Traffic is matched by policy route.

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 76

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

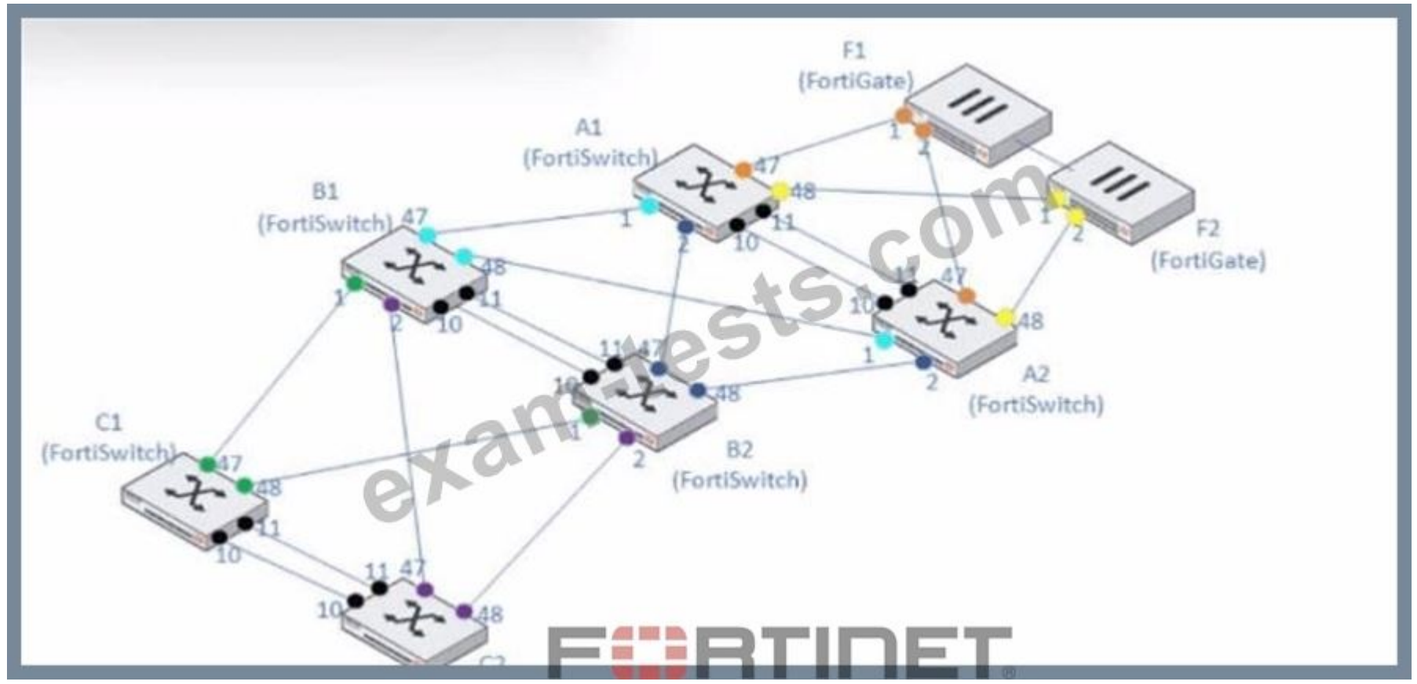
D. Redesign the SD-WAN deployment to only use a single VPN tunnel and segment traffic using VRFs on BGP

Answer: D (LEAVE A REPLY)

Using multiple VPN tunnels and BGP sessions for each internal segment is not scalable and efficient, especially when the number of segments, DCs or internet links per DC increases. A better solution is to use a single VPN tunnel per branch and segment traffic using virtual routing and forwarding (VRF) instances on BGP. This way, each VRF can have its own routing table and BGP session, while sharing the same VPN tunnel. Reference: https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103439/sd-wan-with-vrf-and-bgp

NEW QUESTION: 77

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?

A.

```
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
```

B.

```
A1 # config switch auto-isl-port-group
A1 (auto-isl-port-g~o) # edit aggregate-port1
A1 (aggregate-port1) # set members port1
A1 (aggregate-port1) # next
A1 (auto-isl-port-g~o) # end
-----
A1 # config switch auto-isl-port-group
A1 (auto-isl-port-g~o) # edit aggregate-port2
A1 (aggregate-port2) # set members port2
A1 (aggregate-port2) # next
A1 (auto-isl-port-g~o) # end
```

C.

```
A1 # config switch auto-isl-port-group
A1 (auto-isl-port-g~o) # edit aggregate-port1
A1 (aggregate-port1) # set members port1
A1 (aggregate-port1) # next
A1 (auto-isl-port-g~o) # end
-----
A1 # config switch auto-isl-port-group
A1 (auto-isl-port-g~o) # edit aggregate-port2
A1 (aggregate-port2) # set members port2
A1 (aggregate-port2) # next
A1 (auto-isl-port-g~o) # end
```

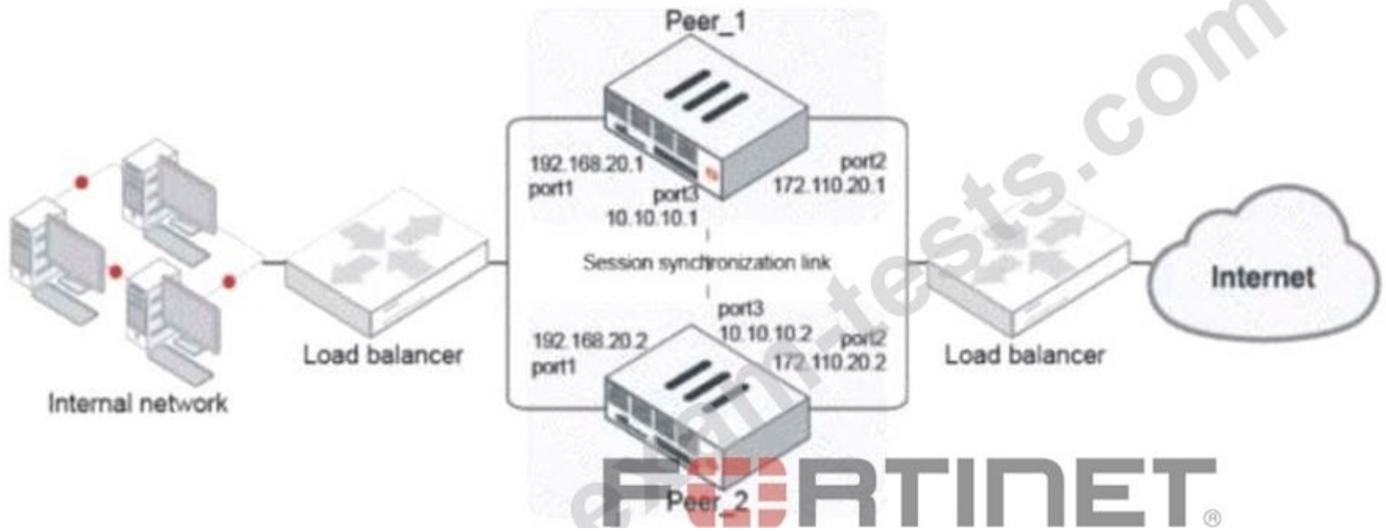
```
A1 # config switch auto-isl-port-group
A1 (auto-isl-port-g~o) # edit aggregate-port10
A1 (aggregate-port10) # set members port10
A1 (aggregate-port10) # next
A1 (auto-isl-port-g~o) # end
-----
A1 # config switch auto-isl-port-group
A1 (auto-isl-port-g~o) # edit aggregate-port11
A1 (aggregate-port11)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

D.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 78

Refer to the exhibit.



Given the exhibit, which two statements about FortiGate FGSP HA cluster behavior are correct? (Choose two.)

A. You can run FortiGate Virtual Router Redundancy Protocol (VRRP) high availability in addition to FGSP simultaneously.

B. You can selectively synchronize only specific sessions between FGSP cluster members.

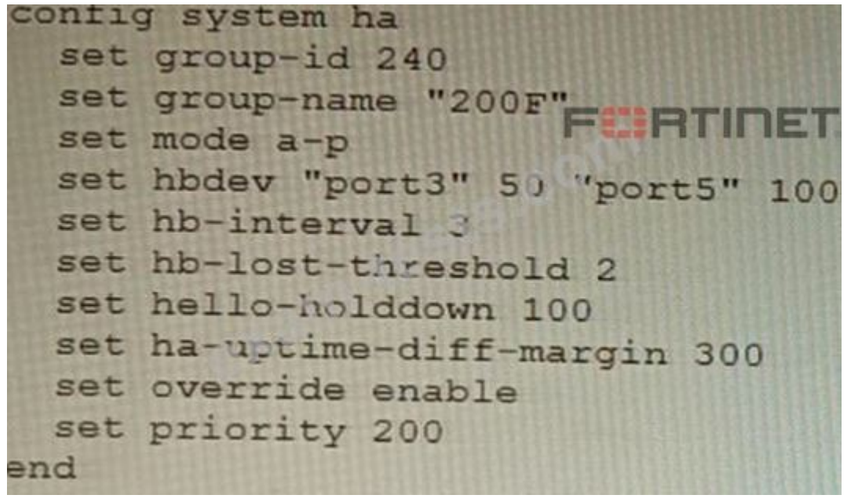
C. Session synchronization occurs over Layer 3 by default, and if unavailable it will then try Layer 2.

D. Cluster members will upgrade one at a time and failover during firmware upgrades.

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 79

An HA topology is using the following configuration:



Based on this configuration, how long will it take for a failover to be detected by the secondary cluster member?

A. 600ms

B. 200ms

C. 300ms

D. 100ms

Answer: B (LEAVE A REPLY)

The HA heartbeat interval is 100ms, and the number of lost heartbeats before a failover is detected is 2. So, it will take 2 * 100ms = 200ms for a failover to be detected by the secondary cluster member.

Reference:

FortiGate High Availability: https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/647723/link-monitoring-and-ha-failover-time

NEW QUESTION: 80

Which two methods are supported for importing user defined Lookup Table Data into the FortiSIEM?

(Choose two.)

A. Report

B. FTP

C. API

D. SCP

Answer: A,C (LEAVE A REPLY)

FortiSIEM supports two methods for importing user defined Lookup Table Data:

* Report: You can import lookup table data from a report. This is the most common method for importing lookup table data.

* API: You can also import lookup table data using the FortiSIEM API. This is a more advanced method that allows you to import lookup table data programmatically.

FTP, SCP, and other file transfer protocols are not supported for importing lookup table data into FortiSIEM.

Reference: https://help.fortinet.com/fsiem/6-7-4/Online-Help/HTML5_Help/importing_lookup_table_data.htm

NEW QUESTION: 81

Refer to the exhibits.

Debug

```
FG-HQ # diagnose debug enable
FG-HQ # diagnose debug application azd -1

azd sdn connector NSE8-Azure prepare to update
azd sdn connector NSE8-Azure start updater process 3060
azd sdn connector NSE8-Azure start updating
azd api failed, url = https://management.azure.com/subscriptions/db349eea-
95af-4864-9b8a-6b6ebc9a91f2/resourceGroups/NSE8-
Lab/providers/Microsoft.Network/publicIPAddresses?api-version=2018-06-01, rc =
403
{"error":{"code":"AuthorizationFailed","message":"The client '4056d55b-2fdc-
```

```
4b9a-9c4e-fea258daf781' with object id '4056d55b-2fdc-4b9a-9c4e-fea258daf781'
does not have authorization to perform action
'Microsoft.Network/publicIPAddresses/read' over scope
'/subscriptions/db349eea-95af-4864-9b8a-6b6ebc9a91f2/resourceGroups/NSE8-
Lab/providers/Microsoft.Network' or the scope is invalid. If access was
recently granted, please refresh your credentials.")}
azd failed to list all public IP for subscription db349eea-95af-4864-9b8a-
6b6ebc9a91f2
azd failed to get ip addr list
azd reap child pid: 3060
```

The exhibits show the configuration and debug output from a FortiGate Public SDN Connector.

What is a possible reason for this dynamic address object to be empty?

A. The Application ID is incorrect.

B. The App registration does not have a role with necessary read permissions on the resource group.

C. The resource group NSE8-Lab does not exist.

D. The Client secret is incorrect.

Answer: (SHOW ANSWER)

NEW QUESTION: 82

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

NEW QUESTION: 83

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-esxihttps://docs.fortinet.com
/document/fortigate/7.0.0/vm-installation-for-vmware-esxi/19662/networking

NEW QUESTION: 84
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
```

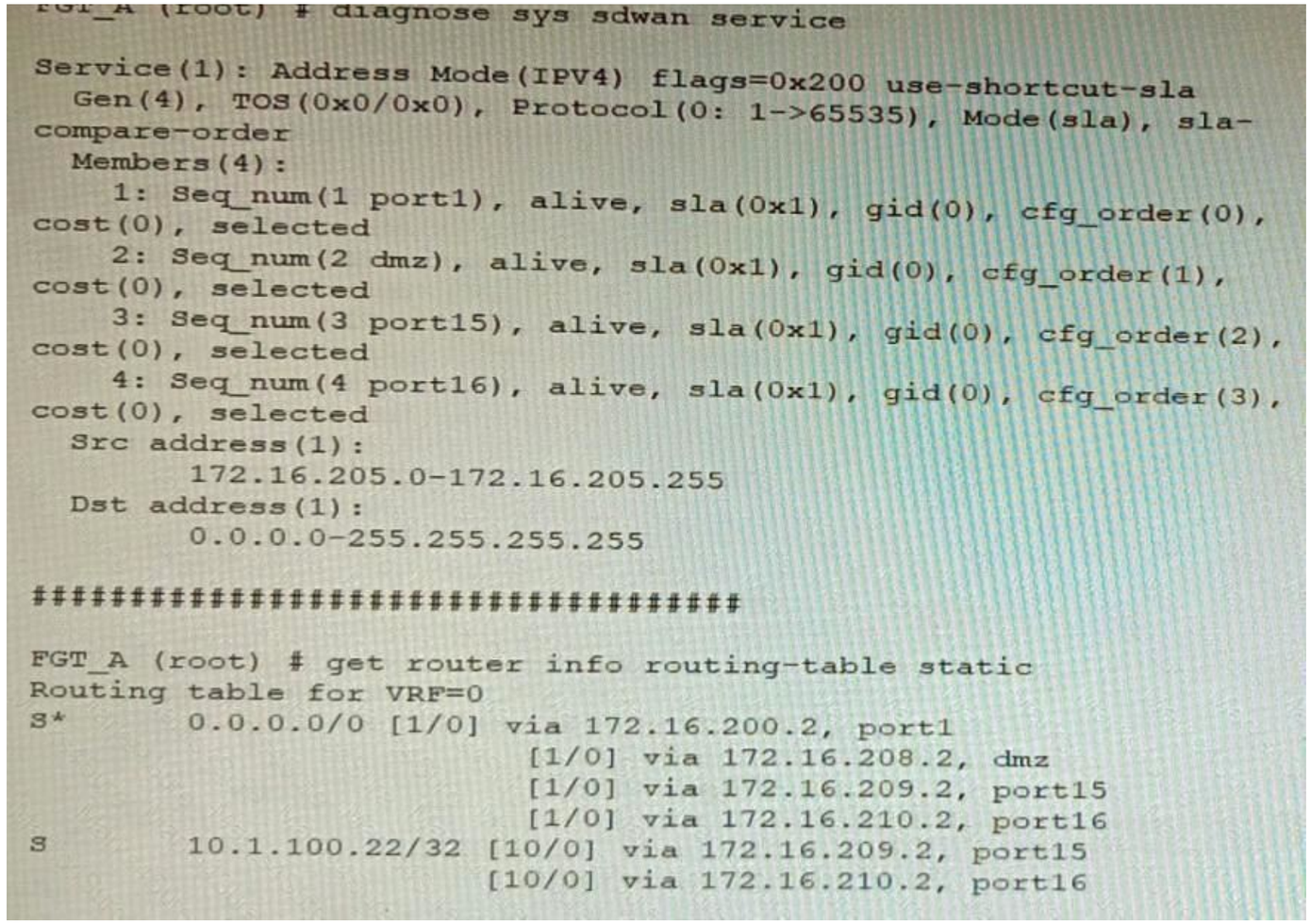

Based on this configuration, which two statements are true? (Choose two.)
A. OCSP checks will always go to the configured FortiAuthenticator
B. The OCSP check of the certificate can be combined with a certificate revocation list.

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: 85
Refer to the exhibit showing an SD-WAN configuration.

```
            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)

According to the exhibit, the SD-WAN configuration has two rules: one for traffic to 10.1.100.0/24 subnet, and one for traffic to 10.1.100.16/28 subnet. The first rule uses the best quality strategy, which selects the SD- WAN member with the best measured quality based on performance SLA metrics. The second rule uses the manual strategy, which specifies port1 as the SD-WAN member to select. Therefore, if an internal user pings

10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, the outgoing interfaces will be port16 and port1 respectively, assuming that port16 has the best quality among the SD-WAN members.

References:https://docs.

fortinet.com/document/fortigate/6.2.14/cookbook/218559/configuring-the-sd-wan-interface

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: 86

You must analyze an event that happened at 20:37 UTC. One log relevant to the event is extracted from FortiGate logs:

```
date=2022-07-11 time=10:37:08 eventtime=1657571829014946018 tz="-1000" logid="0000000022"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.100.91.12 srcport=51542
srcintf="port3" srcintfrole="lan" dstip=8.8.8.8 dstport=53 dstintf="port1" fstintfrole="wan"
srcuuid="2b4ee3fc-0124-51ed-7898-eae1b990b1ec" dstuuid="2b4ee3fc-0124-51ed-7898-eae1b990b1ec"
srccountry="Reserved" dstcountry="United States" sessionid=402530 proto=17 action="accept"
policyid=13 policytype="policy" poluuid="766bb040-0124-51ed-ca3a-eacce4ed289f" policyname="LAN to
Internet" service="DNS" trandisp="snat" transip=10.100.64.101 transport=51542 appid16195 app="DNS"
appcat="Network.Service" apprisk="elevated" applist="default" duration=180 setbyte=45 rcvdbyte=120
sentpkt=1 rcvdpkt=1 srchwvendor="Fortinet" devtype="Router" srcfamily="FortyGate" osname="FortyOS"
mastersrcmac="00:09:0f:00:03:01" srcmac="00:09:0f:00:03:01" srcserver=0
```

The devices and the administrator are all located in different time zones Daylight savings time (DST) is disabled

* The FortiGate is at GMT-1000.
* The FortiAnalyzer is at GMT-0800
* Your browser local time zone is at GMT-03.00

You want to review this log on FortiAnalyzer GUI, what time should you use as a filter?

A. 20:37:08
B. 10:37:08
C. 17:37:08
D. 12.37:08
Answer: (SHOW ANSWER)

https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-Understanding-FortiAnalyzer-time-related- fields/ta-p/197569

NEW QUESTION: 87

Refer to the exhibits.

Troubleshooting Session Output

```
fgt01-branch01 # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=vpn-hub02-1 ver=2 serial=1 10.73.255.67:0->10.73.255.82:0 tun_id=10.73.255.82
tun_id6=::10.73.255.82 dst_mtu=1500 dpd-link=on weight=1
bound_if=7 lgwy=static/1 tun=tunnel/255 mode=auto/1 encap=none/536 options[0218]=npu create_
 accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=0 olast=0 ad=r/2
stat: rxp=1 txp=1500326 rxb=73 txb=273040631
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vpn-hub02-1 proto=0 sa=1 ref=27 serial=1 auto-negotiate adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA:  ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=3044/0B replaywin=2048
       seqno=b1d18 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42902/43200
  dec: spi=4da0c1a4 esp=aes key=32 6495048006963561c4c9b9d91e5e22c454446438480484a81e6bed9f9d3742ef
       ah=sha256 key=32 7fb9fce764431ba10b6da80263cd0484d9f5824cc9d5bd260db2cffca1a1d572
  enc: spi=f80065a7 esp=aes key=32 df2741a4d69cf6a241fe80b7722e1b13045b88457e7bf29ee171779b556c83cf
       ah=sha256 key=32 9e07bf36eca21c4732cf5af4ccdfe7f1dbc19e7e1afe17fe2a77475f2dd2b0fa
  dec:pkts/bytes=0/0, enc:pkts/bytes=1456559/316245764
  npu_flag=03 npu_rgwy=10.73.255.82 npu_lgwy=10.73.255.67 npu_selid=0 dec_npuid=1 enc_npuid=1
```

A customer is trying to restore a VPN connection configured on a FortiGate. Exhibits show output during a troubleshooting session when the VPN was working and the current baseline VPN configuration.

VPN Configuration

```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set interface "wan1"
        set net-device enable
        set authmethod signature
        set certificate "BR01FGTLOCAL"
        set mode-cfg enable
        set npu-offload disable
        set dpd on-idle
        set proposal aes256-sha256
        set add-route disable
        set auto-discovery-receiver enable
        set remote-gw 10.73.255.82
        set peer "vpn-hub02-1_peer"
    next
end
```

Which configuration parameters will restore VPN connectivity based on the diagnostic output?

A.

```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set dpd on-demand
        set npu-offload enable
    next
end
```

B.

```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set net-device disable
        set dpd on-demand
    next
end
```

C.

```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 1
        set net-device disable
        set dpd disable
    next
end
```

```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 1
        set npu-offload enable
        set dpd disable
    next
end
```


D. FORTINET

Answer: (SHOW ANSWER)

NEW QUESTION: 88

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-f lood-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: A,D (LEAVE A REPLY)

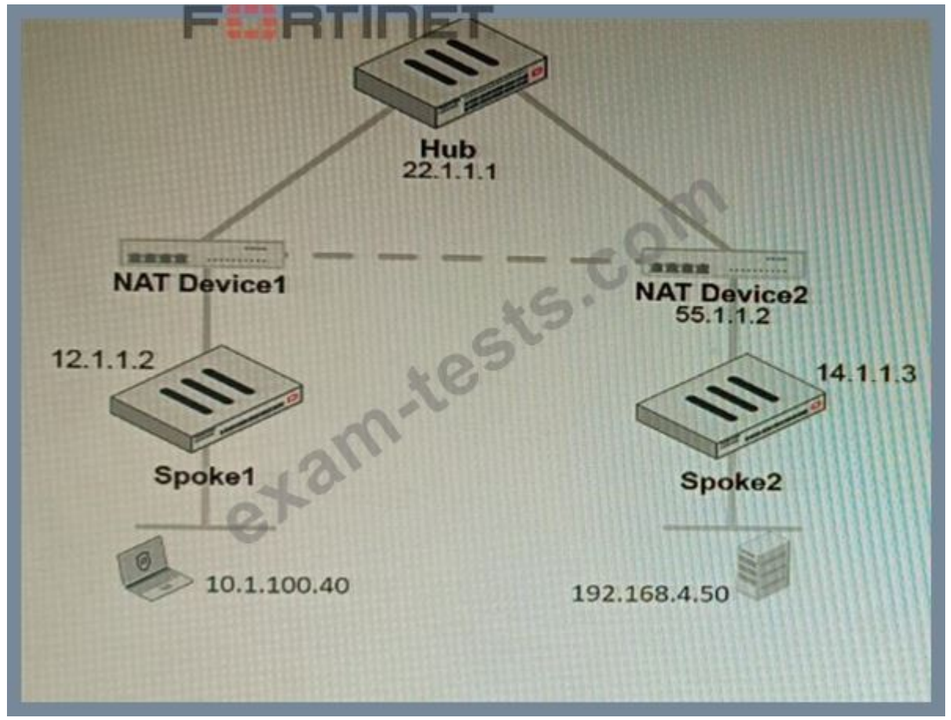
To ensure that unnecessary multicast traffic is pruned from links that do not have a multicast listener, you must disable IGMP flood traffic on the ICL trunks and enable IGMP flood reports on the ISL and FortiLink trunks.

Disabling IGMP flood traffic will prevent the FortiSwitch units from flooding multicast traffic to all ports on the ICL trunks. This will help to reduce unnecessary multicast traffic on the network.

Enabling IGMP flood reports will allow the FortiSwitch units to learn which ports are interested in receiving multicast traffic. This will help the FortiSwitch units to prune multicast traffic from links that do not have a multicast listener.

NEW QUESTION: 89

Refer to the exhibit, which shows a VPN topology.



The device IP 10.1.100.40 downloads a file from the FTP server IP 192.168.4.50 Referring to the exhibit, what will be the traffic flow behavior if ADVPN is configured in this environment?

A. All the session traffic will pass through the Hub

B. The TCP port 21 must be allowed on the NAT Device2

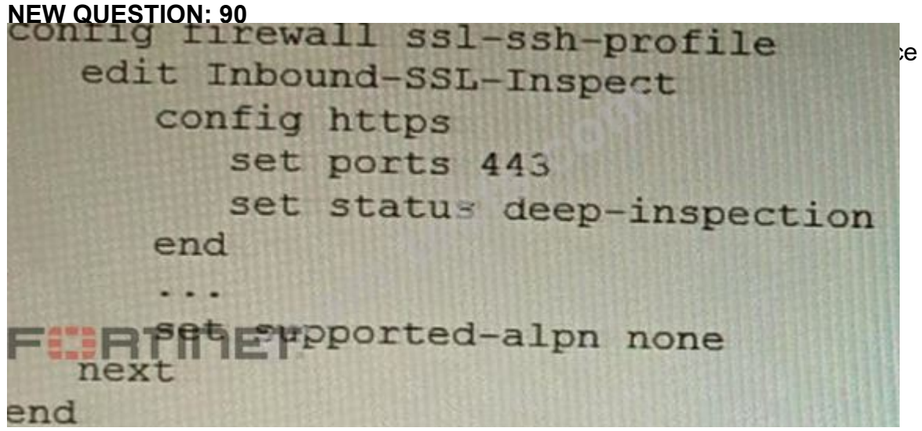
C. ADVPN is not supported when spokes are behind NAT

D. Spoke1 will establish an ADVPN shortcut to Spoke2

Answer: (SHOW ANSWER)

D is correct because Spoke1 will establish an ADVPN shortcut to Spoke2 when it detects that there is a demand for traffic between them. This is explained in the Fortinet Community article on Technical Tip: Fortinet Auto Discovery VPN (ADVPN) under Summary - ADVPN sequence of events. References: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Fortinet-Auto-Discovery-VPN-ADVPN/ta-p/195698

NEW QUESTION: 90



ce configured to protect a web server:

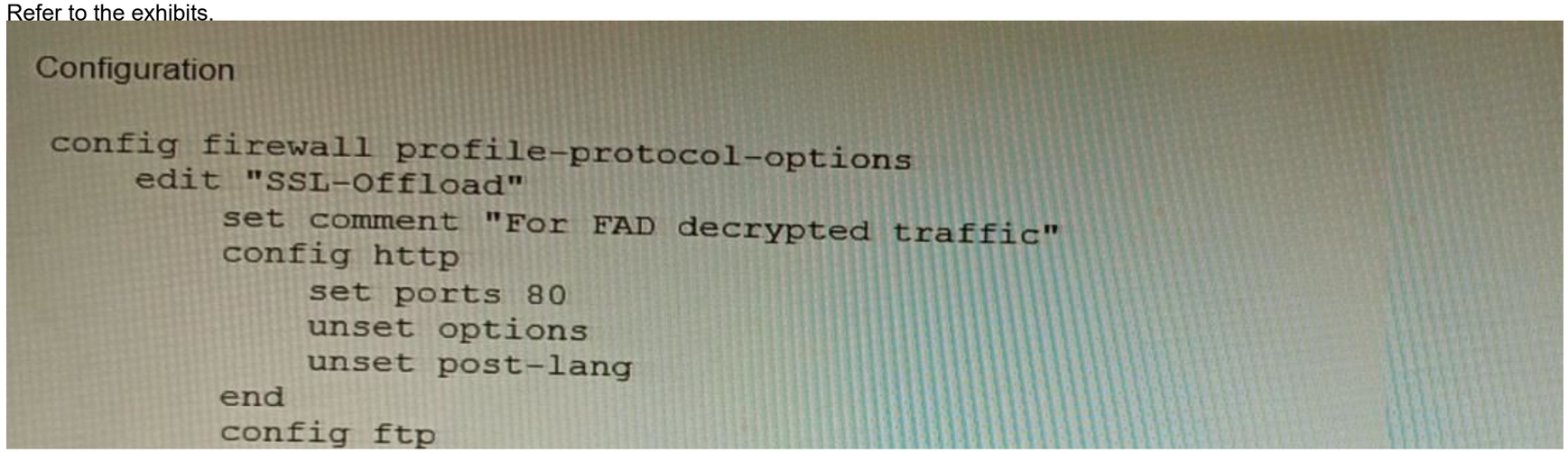
Based on the information shown, what is the expected behavior when an HTTP/2 request comes in?

A. FortiGate will reject all HTTP/2 ALPN headers.

B. FortiGate will strip the ALPN header and forward the traffic.
C. FortiGate will rewrite the ALPN header to request HTTP/1.
D. FortiGate will forward the traffic without modifying the ALPN header.
Answer: B (LEAVE A REPLY)
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2-support-in-proxy-mode-ssl- inspection

NEW QUESTION: 91
A customer with a FortiDDoS 200F protecting their fibre optic internet connection from incoming traffic sees that all the traffic was dropped by the device even though they were not under a DoS attack. The traffic flow was restored after it was rebooted using the GUI. Which two options will prevent this situation in the future? (Choose two)
A. Change the Adaptive Mode.
B. Create an HA setup with a second FortiDDoS 200F
C. Move the internet connection from the SFP interfaces to the LC interfaces
D. Replace with a FortiDDoS 1500F
Answer: (SHOW ANSWER)
To prevent the situation where all the traffic was dropped by the FortiDDoS 200F even though there was no DoS attack, the following options can be considered:
Change the Adaptive Mode. The Adaptive Mode is a feature that allows the FortiDDoS 200F to automatically adjust its detection and prevention thresholds based on the traffic patterns and behavior. However, if the Adaptive Mode is not configured properly, it may cause false positives and drop legitimate traffic. Therefore, changing the Adaptive Mode settings or disabling it may help to avoid this situation.
Create an HA setup with a second FortiDDoS 200F. The HA setup is a feature that allows two FortiDDoS 200F devices to work together as a cluster and provide redundancy and load balancing. If one device fails or drops traffic, the other device can take over and continue to protect the network. Therefore, creating an HA setup with a second FortiDDoS 200F may help to avoid this situation. Reference: https://docs.fortinet.com/document/fortiddos-f/6.2.0/handbook/380639/understanding-fortiddos-adaptive-mode https://docs.fortinet.com/document/fortiddos-f/6.2.0/handbook/380639/configuring-fortiddos-ha

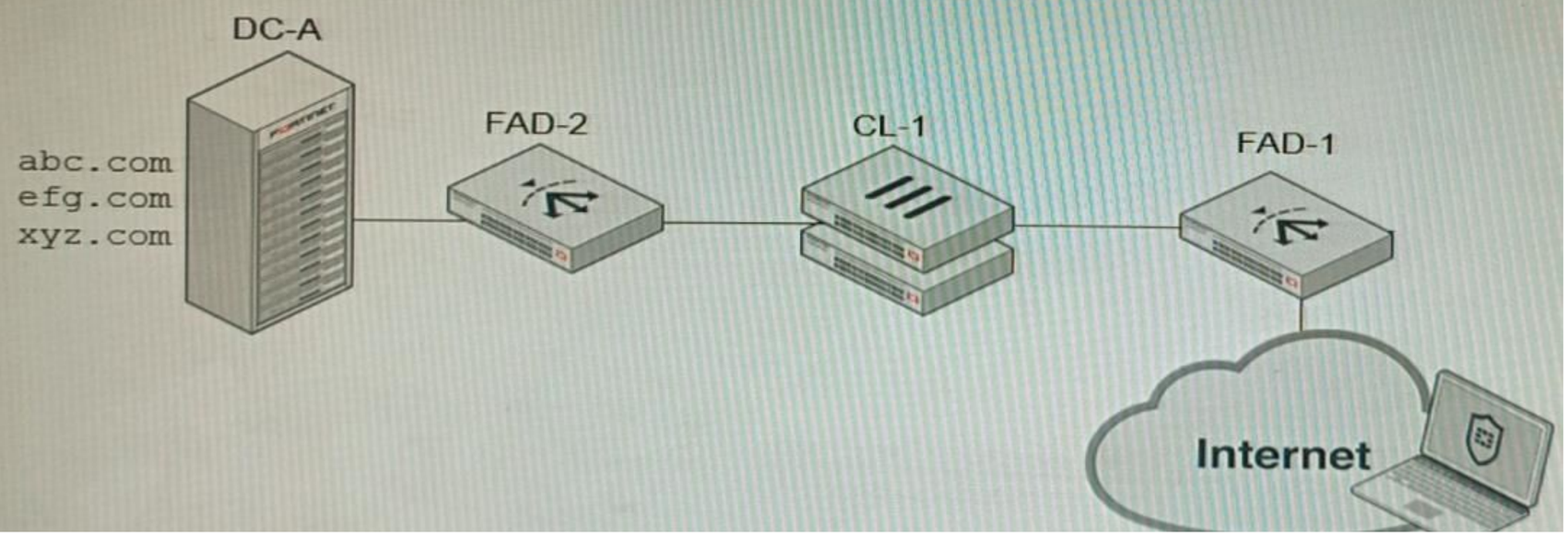
NEW QUESTION: 92
Refer to the exhibits.



```
            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.) A)

```
config firewall profile-protocol-options
    edit SSL-Offload
        config http
            set ssl-offloaded yes
        end
    next
end
```

B)

```
config firewall profile-protocol-options
    edit SSL-Offload
        config https
            set options splice
        end
    next
end
```

```
config application list
    edit SSL-Offload-App-Detect
        set force-inclusion-ssl-di-sigs enable
    next
end
```

```
config application list
    edit SSL-Offload-App-Detect
        set deep-app-inspection enable
    next
end
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: (SHOW ANSWER)

To enable application detection on plain-text traffic that has been decrypted by FortiADC, the administrator must perform two configuration tasks on CL-1:

Enable SSL offloading in the firewall policy and select the SSL-Offload protocol options profile.

Enable application control in the firewall policy and select the SSL-Offload-App-Detect application list. References: https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103438/application-detection-on-ssl-offloaded-traffic

NEW QUESTION: 93

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)

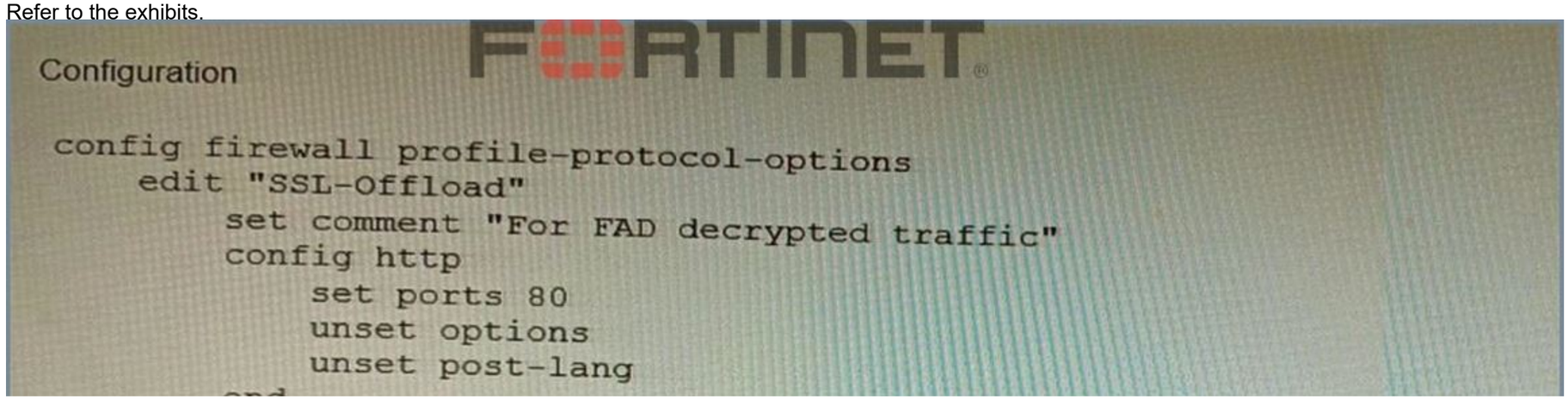
To retrieve an SSO group called SalesGroup using the FortiAuthenticator REST API, the following issues need to be fixed in the API call:

* 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/927310/introduction https://docs.fortinet.com/document/fortiauthenticator/6.4.1/rest-api-solution-guide/927311/sso-groups

NEW QUESTION: 94

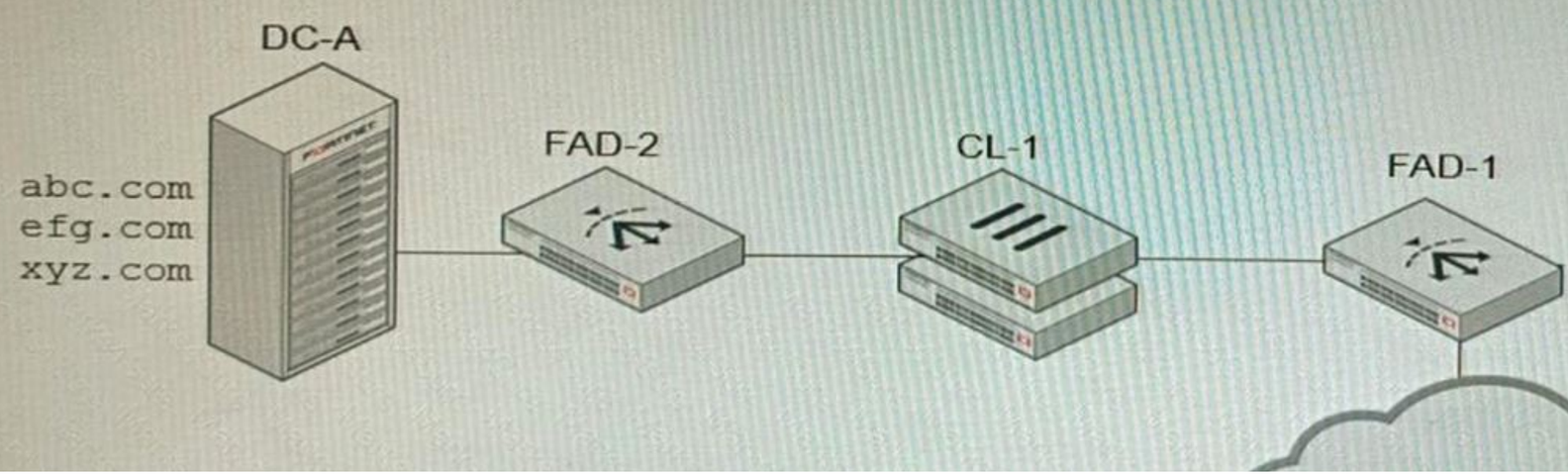
Refer to the exhibits.



```
        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.)

A.

```
config firewall profile-protocol-options
    edit SSL-Offload
        config http
            set ssl-offloaded yes
        end
    next
end
```

B.

```
config firewall profile-protocol-options
    edit SSL-Offload
        config https
            set options splice
        end
    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
```

Answer: B,C (LEAVE A REPLY)

To enable application detection on plain-text traffic that has been decrypted by FortiADC, the administrator must perform two configuration tasks on CL-1:

* Enable SSL offloading in the firewall policy and select the SSL-Offload protocol options profile.

* Enable application control in the firewall policy and select the SSL-Offload-App-Detect application list.

References: https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103438/application-detection- on-ssl-offloaded-traffic

NEW QUESTION: 95

Refer to the exhibit, which shows a Branch1 configuration and routing table.

```
Branch1 # show system sdwan
config system sdwan
    set status enable
    set load-balance-mode source-dest-ip-based
    config zone
        edit "internet"
        next
        edit "overlay"
        next
    end
    config members
        edit 1
            set interface "wan1"
                set zone "internet"
        next
        edit 2
            set interface "wan2"
                set zone "internet"
        next
        edit 3
            set interface "vpn1-net"
            set zone "overlay"
        next
        edit 4
            set interface "vpn2-mpls"
            set zone "overlay"
        next
    end
```

```
        config service
        end
end

##############################

Branch1 # show router static
config router static
    edit 0
        set distance 1
        set sdwan-zone "internet" "overlay"
    next
end

##############################

Branch1 # get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default


Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 10.198.1.1, wan1, [1/0]
                  [1/0] via 10.198.2.1, wan2, [1/0]
                  [1/0] via vpn1-net tunnel 10.198.5.2, [1/0]
                  [1/0] via vpn1-mpls tunnel 10.198.6.2, [1/0]
C       10.1.1.0/24 is directly connected, port3
...
```

In the SD-WAN implicit rule, you do not want the traffic load balance for the overlay interface when all members are available.
In this scenario, which configuration change will meet this requirement?

A. Change the load-balance-mode to source-ip-based.
B. Create a new static route with the internet sdwan-zone only
C. Configure the cost in each overlay member to 10.
D. Configure the priority in each overlay member to 10.

Answer: (SHOW ANSWER)

The default load balancing mode for the SD-WAN implicit rule is source IP based. This means that traffic will be load balanced evenly between the overlay members, regardless of the member's priority.

To prevent traffic from being load balanced, you can configure the priority of each overlay member to 10.

This will make the member ineligible for load balancing.

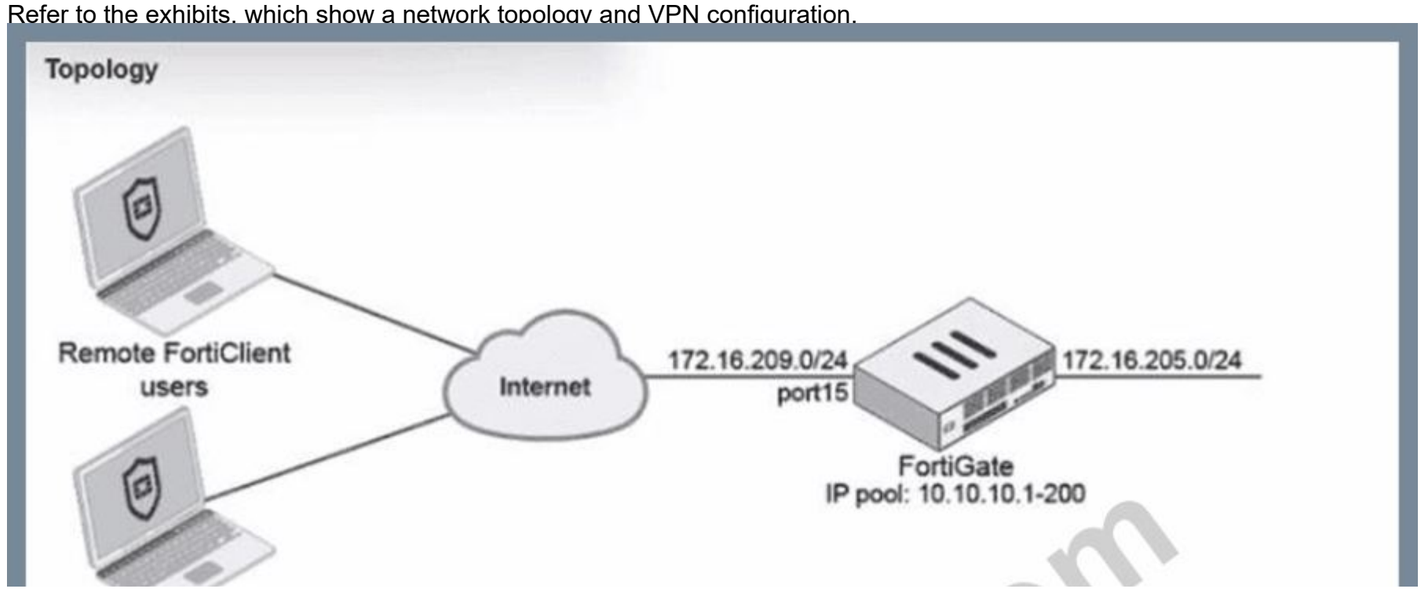
The other options are not correct. Changing the load balancing mode to source-IP based will still result in traffic being load balanced. Creating a new static route with the internet sdwan-zone only will not affect the load balancing of the overlay interface. Configuring the cost in each overlay member to 10 will also not affect the load balancing, as the cost is only used when the implicit rule cannot find a match for the destination IP address.

Option	Description
Change the load-balance-mode to source-ip-based	Will still result in traffic being load balanced.
Create a new static route with the internet sdwan-zone only	Will not affect the load balancing of the overlay interface.
Configure the cost in each overlay member to 10	Will not affect the load balancing, as the cost is only used when the implicit rule cannot find a match for the destination IP address.
Configure the priority in each overlay member to 10	Will prevent traffic from being load balanced.

https://docs.fortinet.com/document/fortigate/6.4.0/sd-wan-deployment-for-mssps/775385/defining-interface- members

NEW QUESTION: 96

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



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: D (LEAVE A REPLY)

NEW QUESTION: 97
Which two statements are correct on a FortiGate using the FortiGuard Outbreak Protection Service (VOS)? (Choose two.)

A. The FortiGuard VOS can be used only with proxy-base policy inspections.
B. If third-party AV database returns a match the scanned file is deemed to be malicious.
C. The antivirus database queries FortiGuard with the hash of a scanned file
D. The AV engine scan must be enabled to use the FortiGuard VOS feature
E. The hash signatures are obtained from the FortiGuard Global Threat Intelligence database.
Answer: C,E (LEAVE A REPLY)
c) The antivirus database queries FortiGuard with the hash of a scanned file. This is how the FortiGuard VOS service works. The FortiGate queries FortiGuard with the hash of a scanned file, and FortiGuard returns a list of known malware signatures that match the hash.
e) The hash signatures are obtained from the FortiGuard Global Threat Intelligence database. This is where the FortiGuard VOS service gets its hash signatures from. The FortiGuard Global Threat Intelligence database is updated regularly with new malware signatures.

NEW QUESTION: 98
A customer is planning on moving their secondary data center to a cloud-based IaaS. They want to place all the Oracle-based systems Oracle Cloud, while the other systems will be on Microsoft Azure with ExpressRoute service to their main data center.
They have about 200 branches with two internet services as their only WAN connections. As a security consultant you are asked to design an architecture using Fortinet products with security, redundancy and performance as a priority.
Which two design options are true based on these requirements? (Choose two.)
A. Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud.
B. Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure.
C. Branch FortiGate devices must be configured as VPN clients for the branches' internal network to be able to access Oracle services without using public IPs.
D. Two ExpressRoute services to the main data center are required to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge
Answer: B,D (LEAVE A REPLY)
To secure the traffic between Azure and the main data center, a FortiGate VM can be deployed in Azure and configured to use IPSEC over ExpressRoute, as traffic is not encrypted by Azure by default. This also allows the use of Fortinet security features such as antivirus, IPS, web filtering, and application control. To implement SD-WAN between Azure and the main data center, two ExpressRoute services are required to provide redundant paths and load balancing. A FortiGate device at the data center edge can be configured to use SD-WAN rules to select the best path based on performance, availability, and cost.
Reference: https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103440/ipsec-vpn-between-fortigate-and-azure https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103441/sd-wan-between-fortigate-and-azure

NEW QUESTION: 99
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/dhcpcd)
```

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: 100
You have configured a Site-to-Site IPsec VPN tunnel between a FortiGate and a third-party device but notice that one of the error counters on the tunnel interface keeps increasing.

```
VPN-TUNNEL Link encap:Unknown
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1420 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:337 errors:4 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:451856798 (430.9 MB) TX bytes:266756340 (254.4 MB)
```

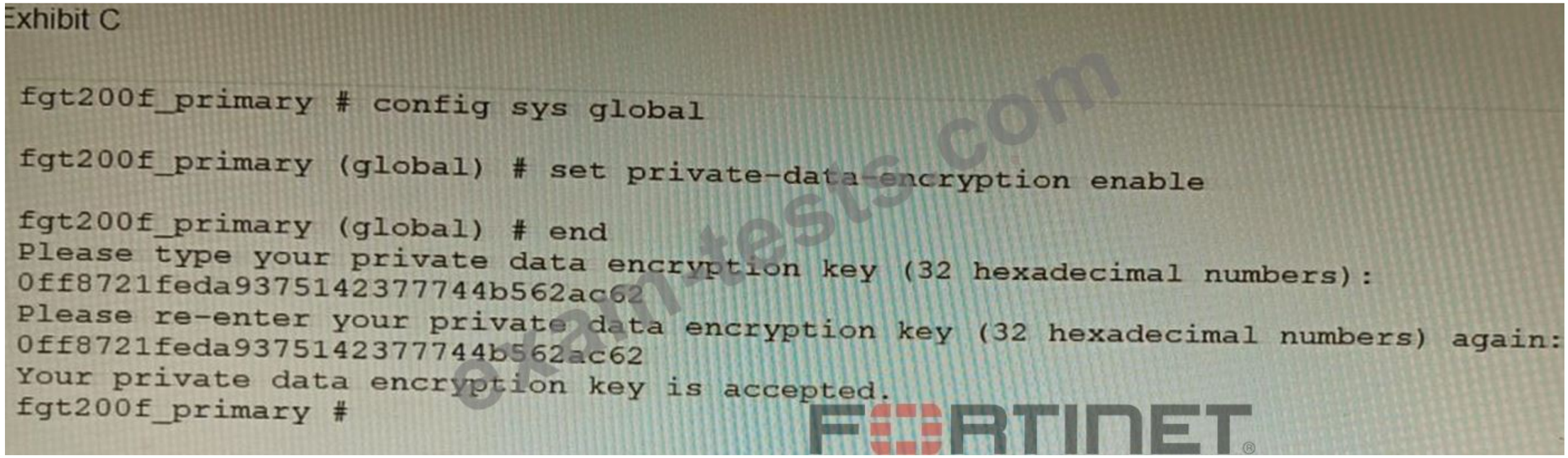
Which two configuration options can resolve this problem? (Choose two.)
A. Adjust the MTU of the physical interface to which the IPsec tunnel is bound.
B. Adjust the MTU of the IPsec interface.
C. Enable DF-bit honoring in the global settings.
D. Enable Forward Error Correction (FEC) on the VPN interface for egress traffic.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 101
A FortiGate deployment contains the following configuration:

```
config system vdom-exception
   edit 1
      set object router.route-map
      set scope inclusive
      set vdom SERVICES
   next
end
```

What is the result of this configuration?
A. Route-maps are not configurable in VDOM SERVICES
B. Route-maps from the Root VDOM configuration are available in VDOM SERVICES
C. Route-maps from VDOM SERVICES are available in all other VDOMs
D. Route-maps for VDOM SERVICES are excluded from HA configuration synchronization
Answer: D (LEAVE A REPLY)
https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/105611

NEW QUESTION: 102
Refer to the exhibit.



A customer has deployed a FortiGate 200F high-availability (HA) cluster that contains & TPM chip. The exhibit shows output from the FortiGate CLI session where the administrator enabled TPM.
Following these actions, the administrator immediately notices that both FortiGate high availability (HA) status and FortiManager status for the FortiGate are negatively impacted.
What are the two reasons for this behavior? (Choose two.)

A. The private-data-encryption key entered on the primary did not match the value that the TPM expected.
B. Configuration for TPM is not synchronized between FortiGate HA cluster members.
C. The FortiGate has not finished the auto-update process to synchronize the new configuration to FortiManager yet.
D. TPM functionality is not yet compatible with FortiGate HA.
E. The administrator needs to manually enter the hex private data encryption key in FortiManager.
Answer: (SHOW ANSWER)
https://docs.fortinet.com/document/fortimanager/7.4.2/administration-guide/30332/verifying-devices-with- private-data-encryption-enabled

NEW QUESTION: 103
Refer to the exhibits.

Exhibit A

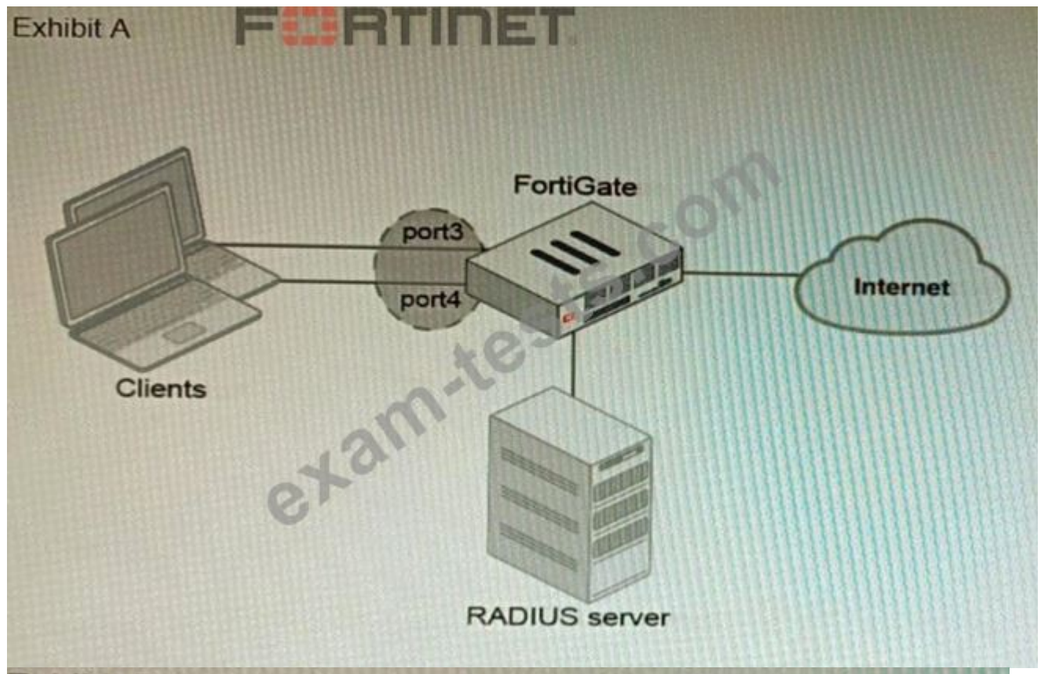


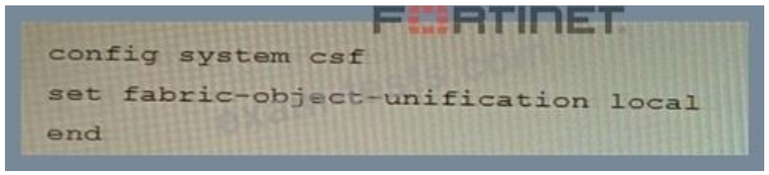
Exhibit B

```
get hardware npu np6 port-list
Chip XAUI Ports Max Cross-chip
Speed offloading
------ ---- ------- ----- ----------
np6_0 0 port1 1G Yes
0 port2 1G Yes
0 port3 1G Yes
0 port4 1G Yes
0 port5 1G Yes
0 port6 1G Yes
0 port7 1G Yes
0 port8 1G Yes
1 port9 1G Yes
1 port10 1G Yes
...
3 port28 1G Yes
3 s1 1G Yes
3 s2 1G Yes
3 vw1 1G Yes
3 vw2 1G Yes
------ ---- ------- ----- ----------
```

A customer is looking for a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E.
Referring to the exhibits, which two conditions allow authentication to the client devices before assigning an IP address? (Choose two.)
A. FortiGate devices with NP6 and hardware switch interfaces cannot support 802.1X authentication.
B. Devices connected directly to ports 3 and 4 can perform 802 1X authentication.
C. Ports 3 and 4 can be part of different switch interfaces.
D. Client devices must have 802 1X authentication enabled
Answer: B,D (LEAVE A REPLY)
The customer wants to deploy a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E device. A hardware switch interface is an interface that combines multiple physical interfaces into one logical interface, allowing them to act as a singleswitch with one IP address and one set of security policies. The customer wants to use 802.1X authentication for this solution, which is a standard protocol for port-based network access control (PNAC) that authenticates clients based on their credentials before granting them access to network resources. One condition that allows authentication to the client devices before assigning an IP address is that devices connected directly to ports 3 and 4 can perform 802.1X authentication. This is because ports 3 and 4 are part of the hardware switch interface named "lan", which has an IP address of 10.10.10.254/24 and an inbound SSL inspection profile named "ssl-inspection". The inbound SSL inspection profile enables the FortiGate device to intercept and inspect SSL/TLS traffic from clients before forwarding it to servers, which allows it to apply security policies and features such as antivirus, web filtering, application control, etc. However, before performing SSL inspection, the FortiGate device needs to authenticate the clients using 802.1X authentication, which requires the clients to send their credentials (such as username and password) to the FortiGate device over a secure EAP (Extensible Authentication Protocol) channel. The FortiGate device then verifies the credentials with an authentication server (such as RADIUS or LDAP) and grants or denies access to the clients based on the authentication result. Therefore, devices connected directly to ports 3 and 4 can perform 802.1X authentication before assigning an IP address.
Another condition that allows authentication to the client devices before assigning an IP address is that client devices must have 802.1X authentication enabled. This is because 802.1X authentication is a mutual process that requires both the client devices and the FortiGate device to support and enable it. The client devices must have 802.1X authentication enabled in their network settings, which allows them to initiate the authentication process when they connect to the hardware switch interface of the FortiGate device. The client devices must also have an 802.1X supplicant software installed, which is a program that runs on the client devices and handles the communication with the FortiGate device using EAP messages. The client devices must also have a trusted certificate installed, which is used to verify the identity of the FortiGate device and establish a secure EAP channel. Therefore, client devices must have 802.1X authentication enabled before assigning an IP address. References:
https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/hardware- switch-interfaceshttps://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/802-1x- authentication
https://docs.fortinet.com/document/fortigate/7.2.0/new-features/959502/support-802-1x-on-virtual-switch-for- certain-np6-platforms

NEW QUESTION: 104
Refer to the exhibit.

You have deployed a security fabric with three FortiGate devices as shown in the exhibit. FGT_2 has the following configuration:



FGT_1 and FGT_3 are configured with the default setting. Which statement is true for the synchronization of fabric-objects?

A. Objects from the FortiGate FGT_2 will be synchronized to the upstream FortiGate.

B. Objects from the root FortiGate will only be synchronized to FGT__2.

C. Objects from the root FortiGate will not be synchronized to any downstream FortiGate.

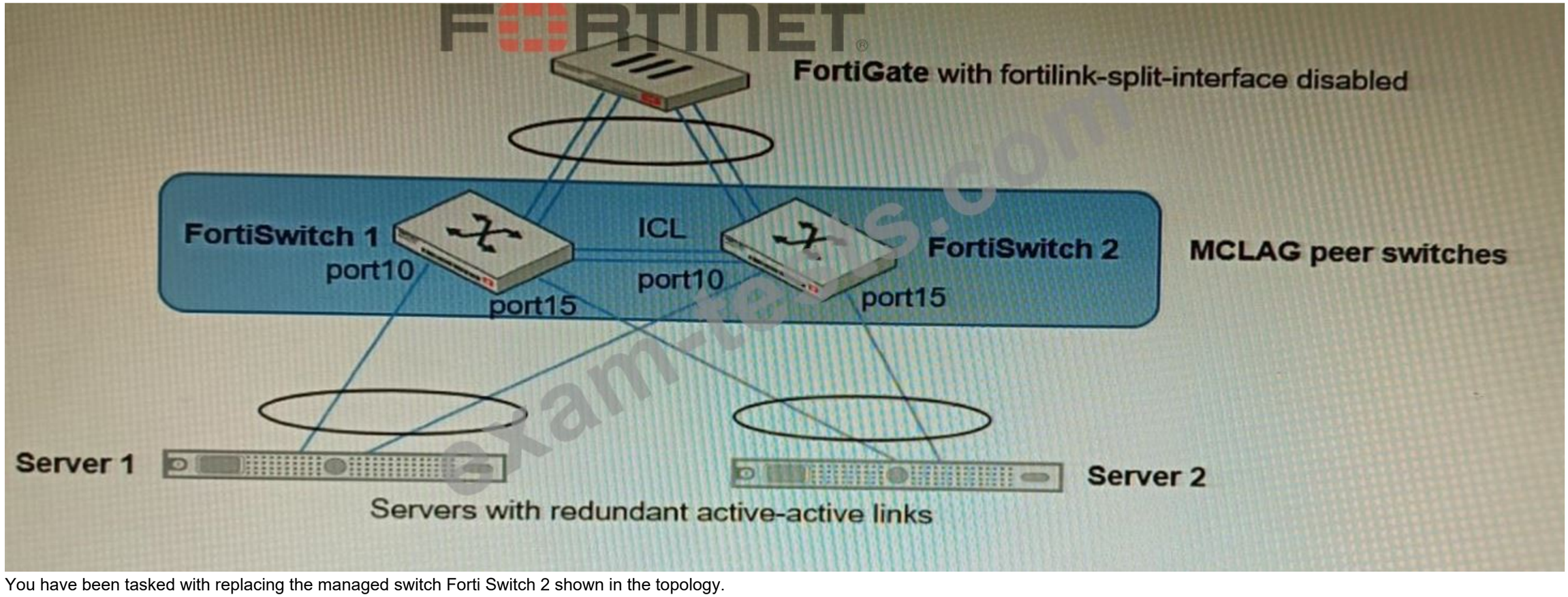
D. Objects from the root FortiGate will only be synchronized to FGT_3.

Answer: (SHOW ANSWER)

The security fabric shown in the exhibit consists of three FortiGate devices connected in a hierarchical topology, where FGT_1 is the root device, FGT_2 is a downstream device, and FGT_3 is a downstream device of FGT_2. FGT_2 has a configuration setting that enables fabric-object synchronization for all objects except firewall policies and firewall policy packages (set sync-fabric-objects enable). Fabric-object synchronization is a feature that allows downstream devices to synchronize their objects (such as addresses, services, schedules, etc.) with their upstream devices in a security fabric. This simplifies object management and ensures consistency across devices. Therefore, in this case, objects from FGT_2 will be synchronized to FGT_1 (the upstream device), but not to FGT_3 (the downstream device). Objects from FGT_1 will not be synchronized to any downstream device because the default setting for fabric-object synchronization is disabled. Objects from FGT_3 will not be synchronized to any device because it does not have fabric-object synchronization enabled. Reference: https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/fabric-object-synchronization

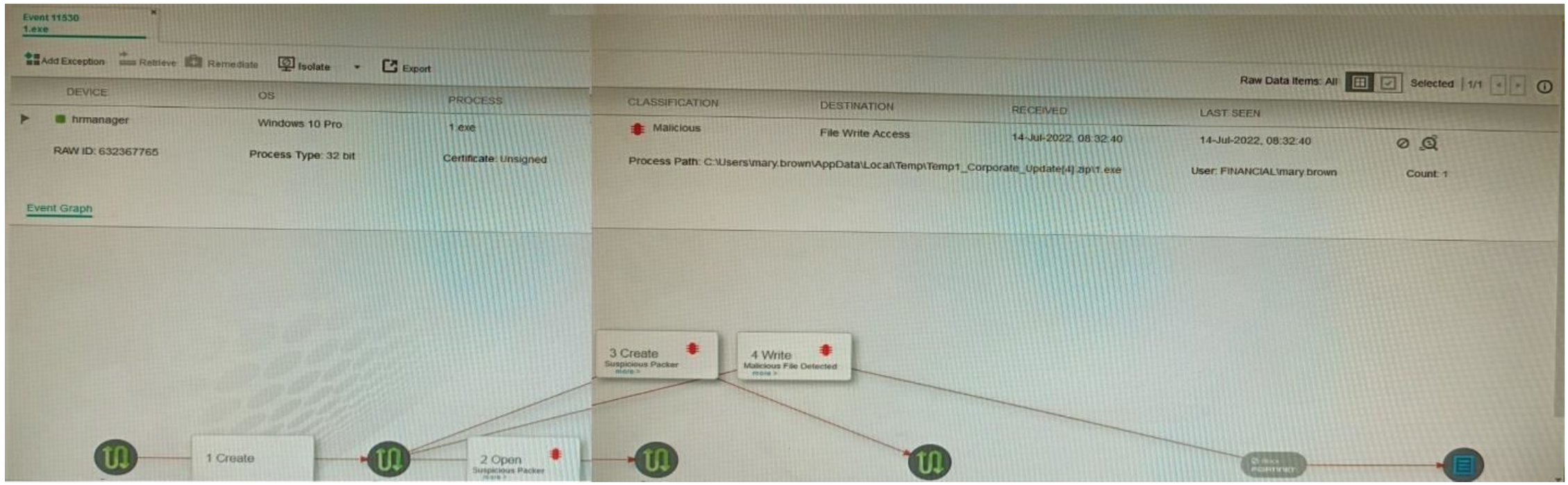
NEW QUESTION: 105

Refer to the exhibit.



You have been tasked with replacing the managed switch Forti Switch 2 shown in the topology.
Which two actions are correct regarding the replacement process? (Choose two.)
A. After replacing the FortiSwitch unit, the automatically created trunk name does not change
B. CLAG-ICL needs to be manually reconfigured once the new switch is connected to the FortiGate
C. After replacing the FortiSwitch unit, the automatically created trunk name changes.
D. MCLAG-ICL will be automatically reconfigured once the new switch is connected to the FortiGate.
Answer: A,B (LEAVE A REPLY)
A is correct because the automatically created trunk name is based on the MAC address of the FortiSwitch unit. When the FortiSwitch unit is replaced, the MAC address will change, but the trunk name will not change.
B is correct because CLAG-ICL is a manually configured link aggregation group. When the FortiSwitch unit is replaced, the CLAG-ICL configuration will need to be manually reconfigured on the new FortiSwitch unit.
The other options are incorrect. Option C is incorrect because the automatically created trunk name does not change when the FortiSwitch unit is replaced. Option D is incorrect because MCLAG-ICL is a manually configured link aggregation group and will not be automatically reconfigured when the FortiSwitch unit is replaced.
References:
Configuring link aggregation on FortiSwitches | FortiSwitch / FortiOS 7.0.4 - Fortinet Document Library Managing FortiLink | FortiGate / FortiOS 7.0.4 - Fortinet Document Library

NEW QUESTION: 106
Refer to the exhibit.



The exhibit shows the forensics analysis of an event detected by the FortiEDR core In this scenario, which statement is correct regarding the threat?

A. This is an exfiltration attack and has been stopped by FortiEDR.

B. This is an exfiltration attack and has not been stopped by FortiEDR

C. This is a ransomware attack and has not been stopped by FortiEDR.

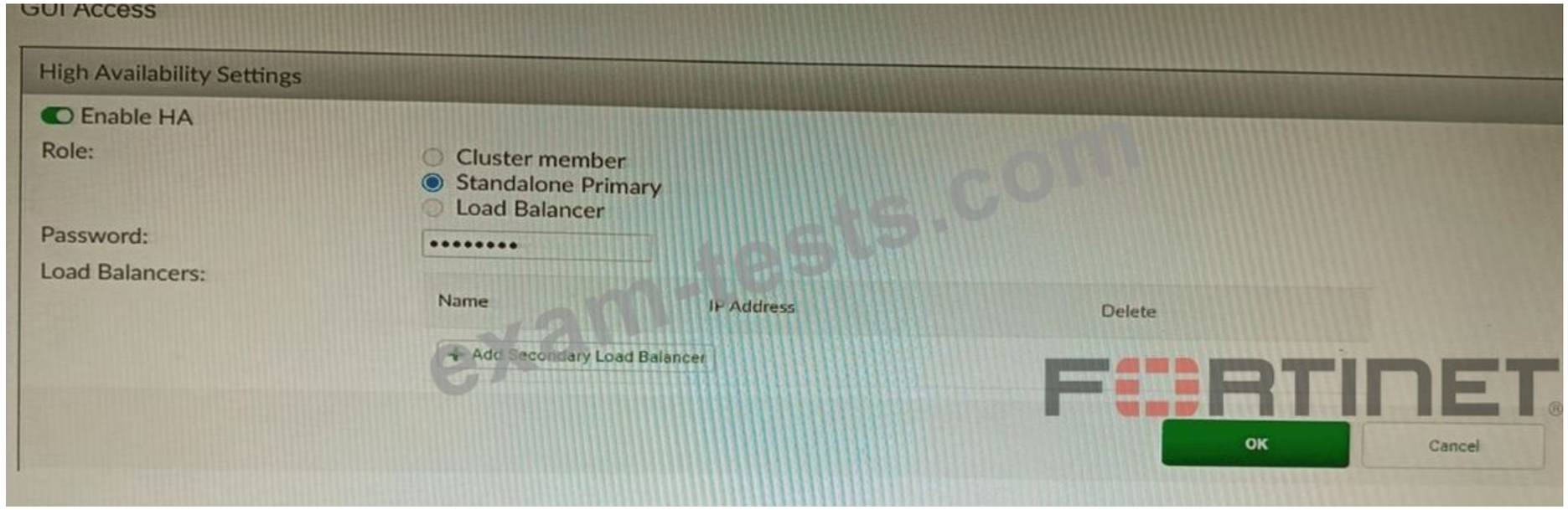
D. This is a ransomware attack and has been stopped by FortiEDR

Answer: (SHOW ANSWER)

The exhibit shows the forensics analysis of an event detected by the FortiEDR core. The event graph indicates that a process named svchost.exe was launched by a malicious file named 1.exe, which was downloaded from a suspicious URL. The process then attempted to encrypt files in various folders, such as Documents, Pictures, and Desktop, which are typical targets of ransomware attacks. However, FortiEDR was able to stop the process and prevent any file encryption by applying its real-time post-execution prevention feature. Therefore, this is a ransomware attack and has been stopped by FortiEDR.
Reference: https://docs.fortinet.com/document/fortiedr/6.0.0/administration-guide/733983/forensics https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf

NEW QUESTION: 107

Refer to the exhibit, which shows the high availability configuration for the FortiAuthenticator (FAC1).



Based on this information, which statement is true about the next FortiAuthenticator (FAC2) member that will join an HA cluster with this FortiAuthenticator (FAC1)?

A. FAC2 can only process requests when FAC1 fails.

B. FAC2 can have its HA interface on a different network than FAC1.

C. The FortiToken license will need to be installed on the FAC2.

D. FSSO sessions from FAC1 will be synchronized to FAC2.

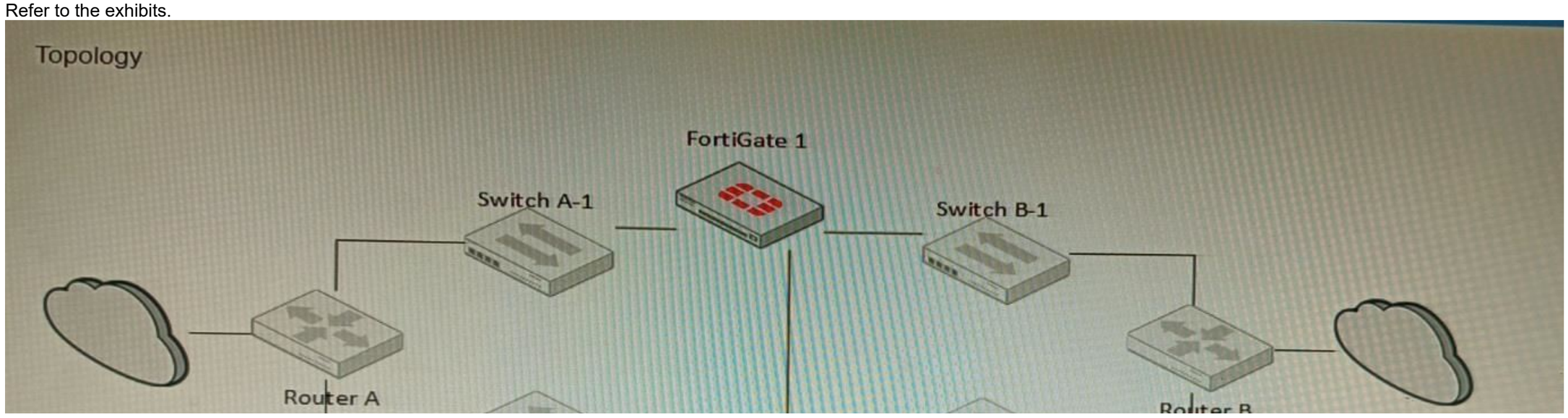
Answer: B (LEAVE A REPLY)

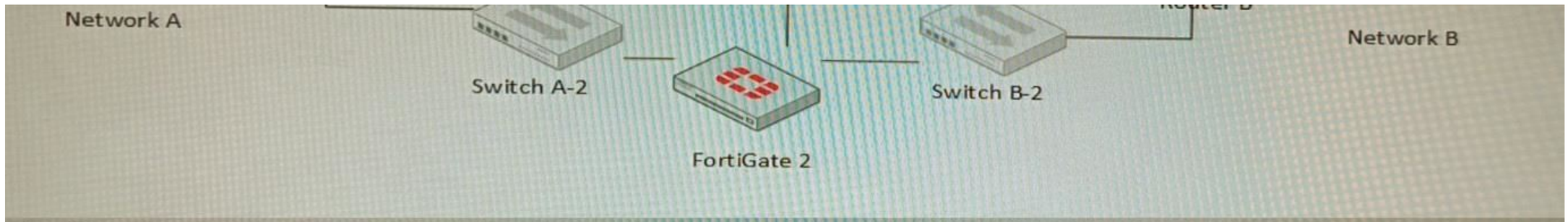
https://docs.fortinet.com/document/fortiauthenticator/6.5.3/administration-guide/122076/high-availability

https://docs.fortinet.com/document/fortiauthenticator/6.5.3/administration-guide/122076/high- availability#Standalo

NEW QUESTION: 108

Refer to the exhibits.





Configuration

```
FGT-HA-1 # get system ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 1:35:12
Cluster state change time: 2019-05-16 14:53:05
Master selected using:
    <2019/05/16 14:53:05> FGVMEVLQOG33WM3D is selected as the
master because it has the largest value of uptime.
    <2019/05/16 14:45:53> FGVMEVLQOG33WM3D is selected as the
master because it's the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
unicast_hb: peerip=192.168.40.1, myip=192.168.40.2,
hasync_port='port3'
Configuration Status:
    FGVMEVLQOG33WM3D(updated 2 seconds ago): in-sync
    FGVMEVGCJNHFYI4A(updated 0 seconds ago): in-sync
```

Configuration -

```
FGT-HA-1 # get system ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 1:35:12
Cluster state change time: 2019-05-16 14:53:05
Master selected using:
    <2019/05/16 14:53:05> FGVMEVLQOG33WM3D is selected as the
master because it has the largest value of uptime.
    <2019/05/16 14:45:53> FGVMEVLQOG33WM3D is selected as the
master because it's the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
unicast_hb: peerip=192.168.40.1, myip=192.168.40.2,
hasync_port='port3'
Configuration Status:
FGVMEVLQOG33WM3D(updated 2 seconds ago): in-sync
FGVMEVGCJNHFYI4A(updated 0 seconds ago): in-sync
```

The exhibits show a FortiGate network topology and the output of the status of high availability on the FortiGate.

Given this information, which statement is correct?

A. The ethertype values of the HA packets are 0x8890, 0x8891, and 0x8892

B. The cluster mode can support a maximum of four (4) FortiGate VMs

C. The cluster members are on the same network and the IP addresses were statically assigned.

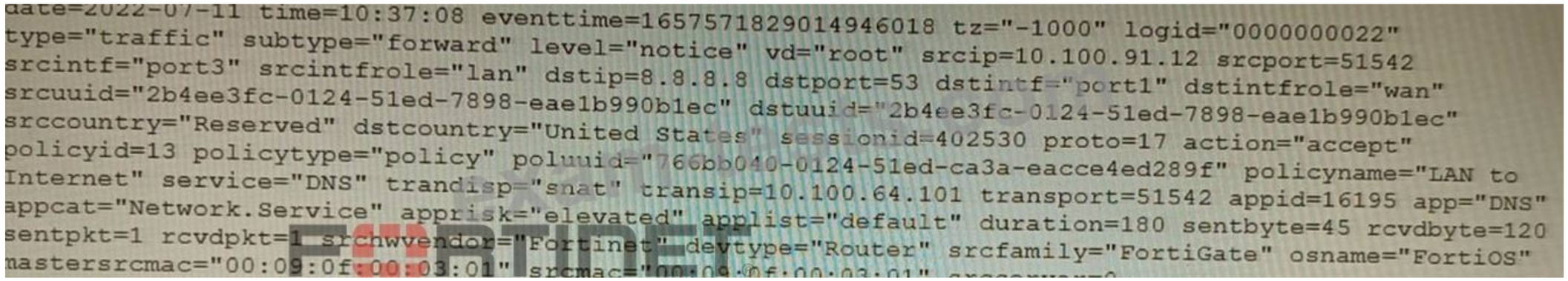
D. FGVMEVLQOG33WM3D and FGVMEVGCJNHFYI4A share a virtual MAC address.

Answer: C (LEAVE A REPLY)
The output of the status of high availability on the FortiGate shows that the cluster mode is active-passive, which means that only one FortiGate unit is active at a time, while the other unit is in standby mode. The active unit handles all traffic and also sends HA heartbeat packets to monitor the standby unit. The standby unit becomes active if it stops receiving heartbeat packets from the active unit, or if it receives a higher priority from another cluster unit. In active-passive mode, all cluster units share a virtual MAC address for each interface, which is used as the source MAC address for all packets forwarded by the cluster.
References:
https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103439/high-availability-with-two-fortigates

NEW QUESTION: 109
SD-WAN is configured on a FortiGate. You notice that when one of the internet links has high latency the time to resolve names using DNS from FortiGate is very high.
You must ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work.
What should you configure?
A. Configure local out traffic to use the outgoing interface based on SD-WAN rules with a manual defined IP associated to a loopback interface and configure an SD-WAN rule from the loopback to the DNS server.
B. Configure an SD-WAN rule to the DNS server and use the FortiGate interface IPs in the source address.
C. Configure two DNS servers and use DNS servers recommended by the two internet providers.
D. Configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server.
Answer: D (LEAVE A REPLY)
SD-WAN is a feature that allows users to optimize network performance and reliability by using multiple WAN links and applying rules based on various criteria, such as latency, jitter, packet loss, etc. One way to ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work is to configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server. This means that the FortiGate will use the best WAN link available to send DNS queries to the DNS server according to the SD-WAN rule, and use its own interface IP as the source address. This avoids NAT issues and ensures optimal DNS performance. Reference: https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan/19662/sd-wan

NEW QUESTION: 110
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: A,C (LEAVE A REPLY)
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. Reference: https://docs.fortinet.com/document/fortigate/7.0.0/ztna-deployment/899992/configuring-ztna-rules-to-control-access

NEW QUESTION: 111
You must analyze an event that happened at 20:37 UTC. One log relevant to the event is extracted from FortiGate logs:



The devices and the administrator are all located in different time zones Daylight savings time (DST) is disabled

* The FortiGate is at GMT-1000.

* The FortiAnalyzer is at GMT-0800

* Your browser local time zone is at GMT-03.00

You want to review this log on FortiAnalyzer GUI, what time should you use as a filter?

A. 20:37:08

B. 10:37:08

C. 17:37:08

D. 12.37:08

Answer: (SHOW ANSWER)

To review this log on FortiAnalyzer GUI, the administrator should use the time filter that matches the local time zone of FortiAnalyzer, which is GMT-0800. Since the log was generated at 20:37 UTC (GMT +0000), the corresponding time in GMT-0800 is 20:37 - 8 hours = 12:37. However, since DST is disabled on FortiAnalyzer, the administrator should add one hour to account for daylight saving time difference, resulting in 12:37 + 1 hour = 13:37. Therefore, the time filter to use is 13:37:08. Reference: https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/103664/time-zone-and-daylight-saving-time