NSE8_812 Q&As

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/nse8_812.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

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
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

Explanation: 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 thecurlcommand. 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 thewebhookaction.

References:

Automation webhook stitches:

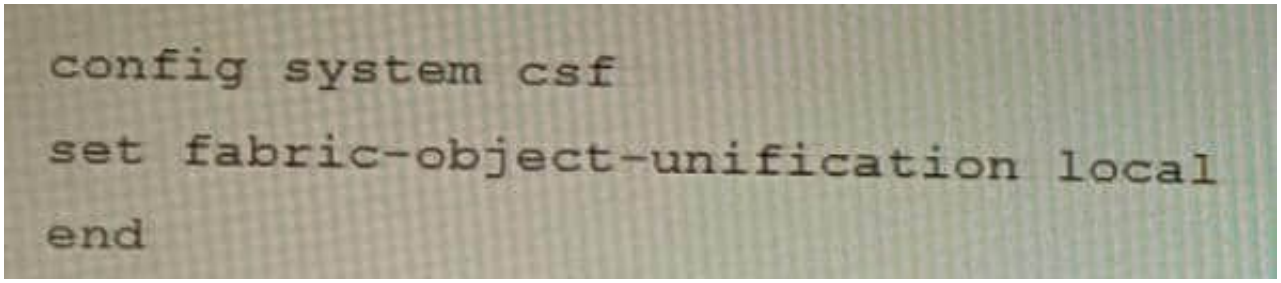
https://docs.fortinet.com/document/fortigate/7.4.0/administration- guide/989735/webhook-action

Webhooks: https://en.wikipedia.org/wiki/Webhook

QUESTION 2

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.

Correct Answer: C

Explanation: 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

QUESTION 3

Refer to the exhibits.

Exhibit A

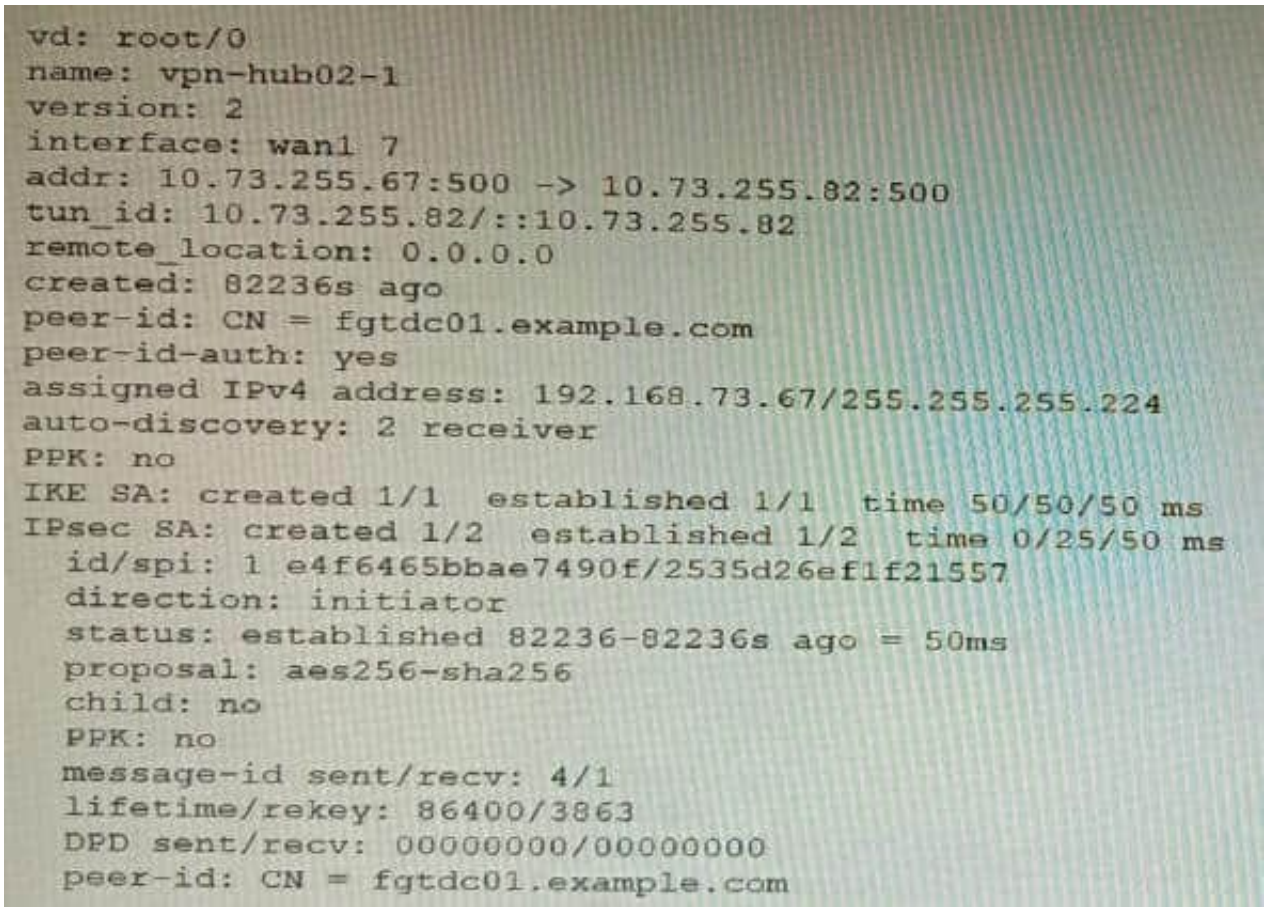


Exhibit B

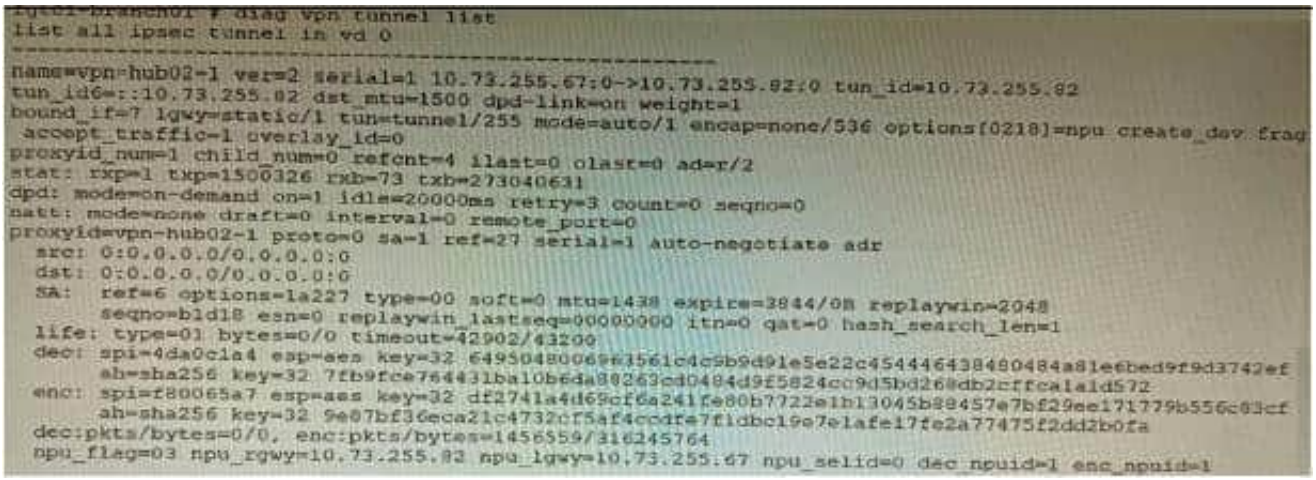
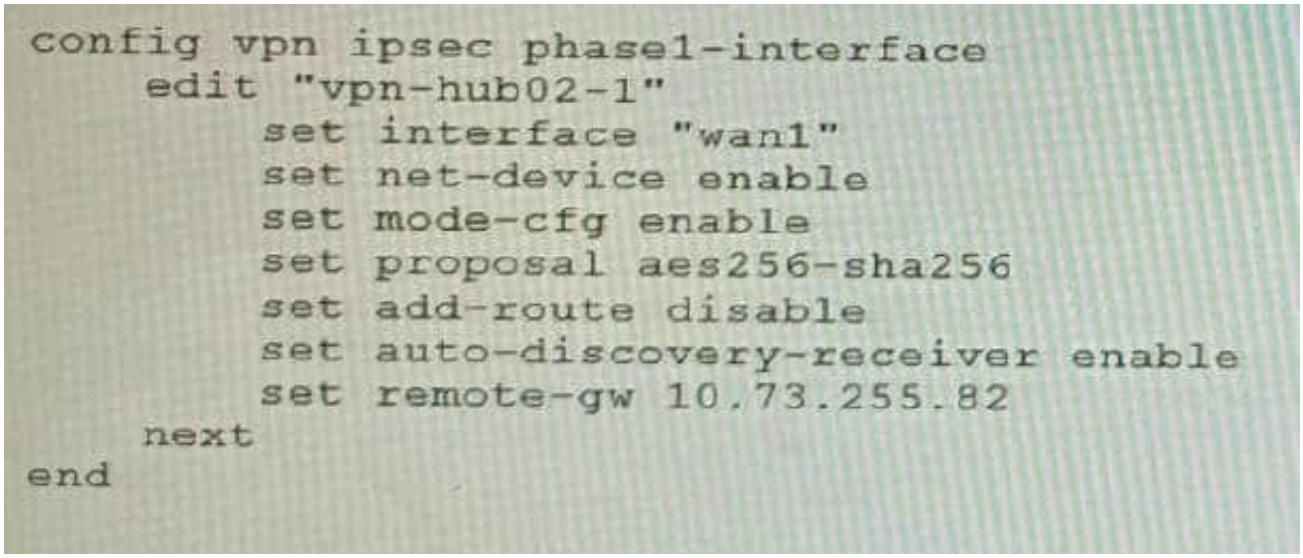


Exhibit C



```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set interface "wan1"
        set net-device enable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set auto-discovery-receiver enable
        set remote-gw 10.73.255.82
    next
end
```

A customer is trying to set up a VPN with a FortiGate, but they do not have a backup of the configuration. Output during a troubleshooting session is shown in the exhibits A and B and a baseline VPN configuration is shown in Exhibit C Referring to the exhibits, which configuration will restore VPN connectivity?

A.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 1
        set authmethod signature
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

B.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set net-device enable
        set psksecret fortinet
    next
end
```

C.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set authmethod signature
        set npu-offload disable
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

D.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set authmethod signature
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

A. Option A

B. Option B

C. Option C

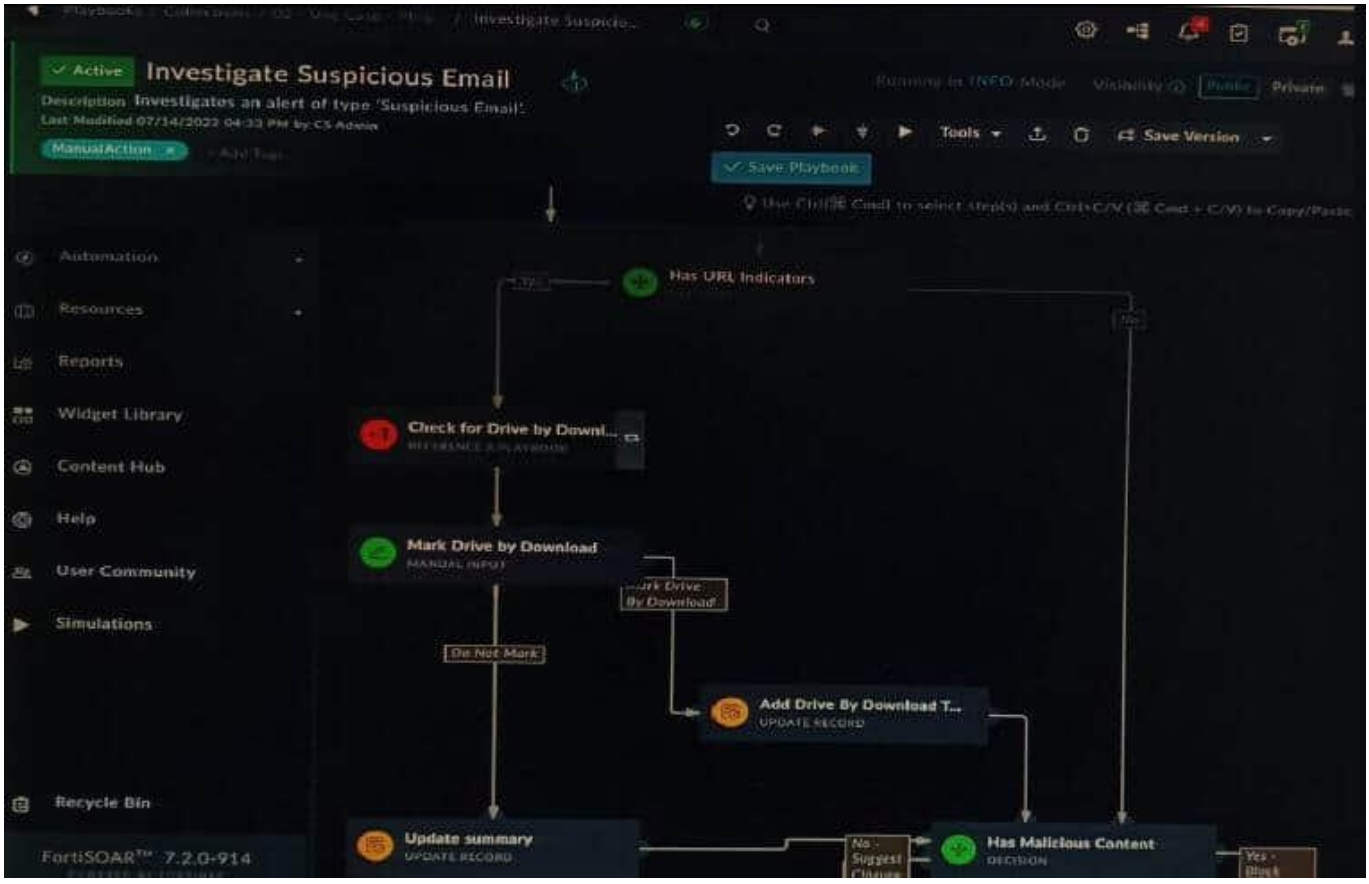
D. Option D

Correct Answer: C

Explanation: The output in Exhibit A shows that the VPN tunnel is not established because the peer IP address is incorrect. The output in Exhibit B shows that the peer IP address is 192.168.1.100, but the baseline VPN configuration in Exhibit C shows that the peer IP address should be 192.168.1.101. To restore VPN connectivity, you need to change the peer IP address in the VPN tunnel configuration to 192.168.1.101. The correct configuration is shown below: config vpn ipsec phase1-interface edit "wan" set peer-ip 192.168.1.101 set peer-id 192.168.1.101 set dhgrp 1 set auth-mode psk set psk SECRET_PSK next end Option A is incorrect because it does not change the peer IP address. Option B is incorrect because it changes the peer IP address to 192.168.1.100, which is the incorrect IP address. Option D is incorrect because it does not include the necessary configuration for the VPN tunnel.

QUESTION 4

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

Correct Answer: A

Explanation: 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.

QUESTION 5

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

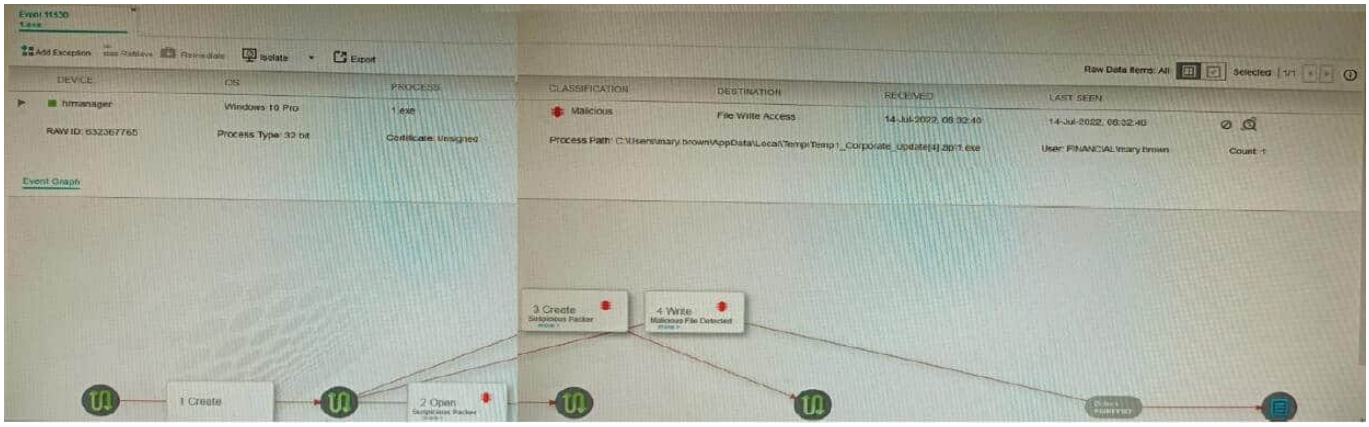
D. Option D

Correct Answer: C

Explanation: 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 securityprofiles to scan multicast traffic for threats and violations. References:https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/968606/configurin g-multicast-forwarding

QUESTION 6

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

Correct Answer: B

Explanation: The exhibit shows that the FortiEDR core has detected an exfiltration attack. The attack is attempting to copy files from the device to an external location. The FortiEDR core has blocked the attack, and the files have not been

exfiltrated. The exhibit also shows that the attack is using the Cobalt Strike beacon. Cobalt Strike is a penetration testing tool that can be used for both legitimate and malicious purposes. In this case, the Cobalt Strike beacon is being used to

exfiltrate files from the device. The other options are incorrect. Option A is incorrect because the attack has not been stopped. Option C is incorrect because the attack is not a ransomware attack. Option D is incorrect because the FortiEDR

core has not stopped the attack.

References:

FortiEDR Forensics:

https://docs.fortinet.com/document/fortiedr/6.0.0/administration- guide/733983/forensics

Cobalt Strike: https://www.cobaltstrike.com/

QUESTION 7

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

Correct Answer: AD

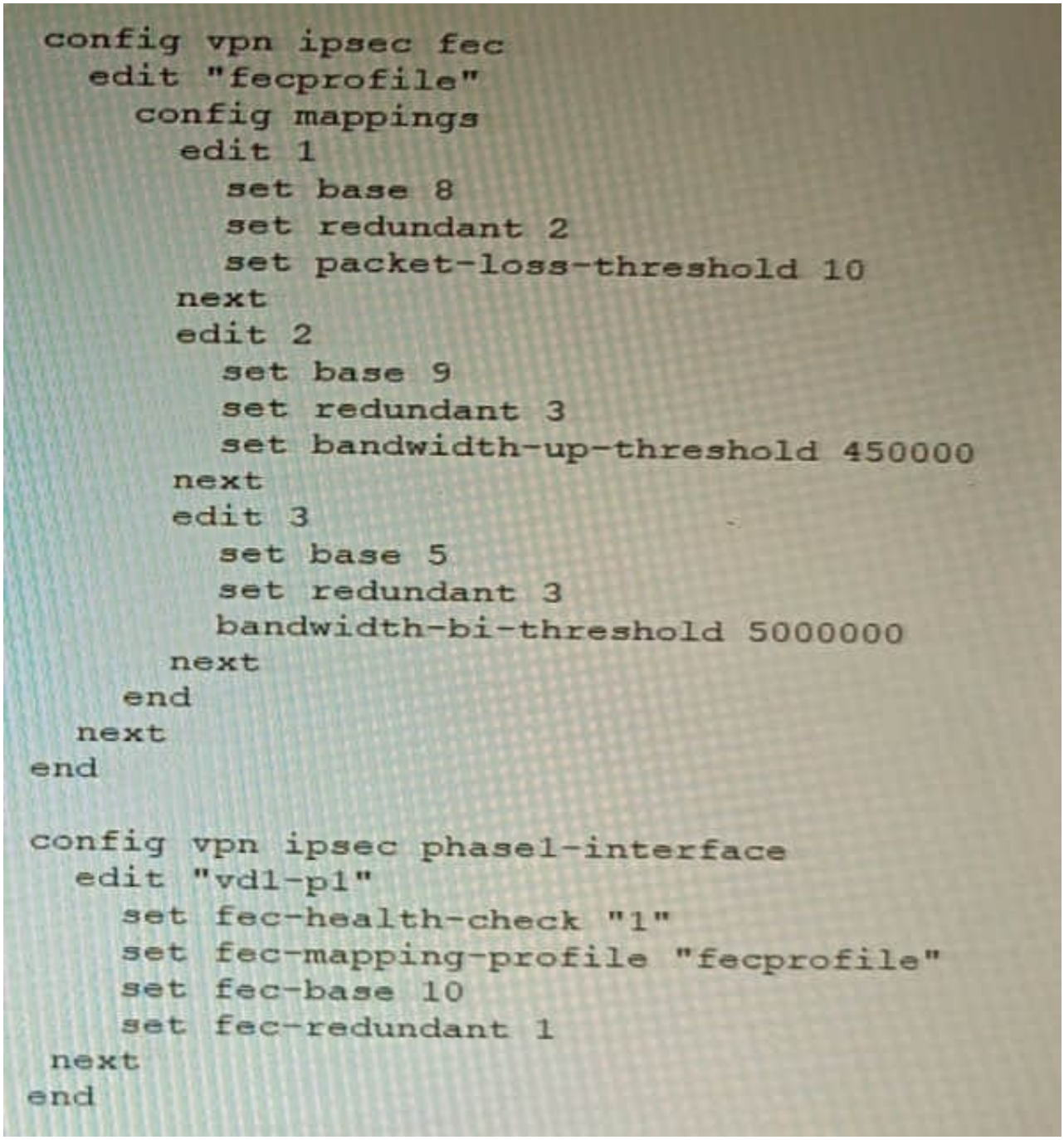
Explanation: To ensure that unnecessary multicast traffic is pruned from links that do not have a multicast listener, you must disable IGMP flood traffic on the ICL trunks and enable IGMP flood reports on the ISL and FortiLink trunks. Disabling

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.

QUESTION 8

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

Correct Answer: C

Explanation: 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.

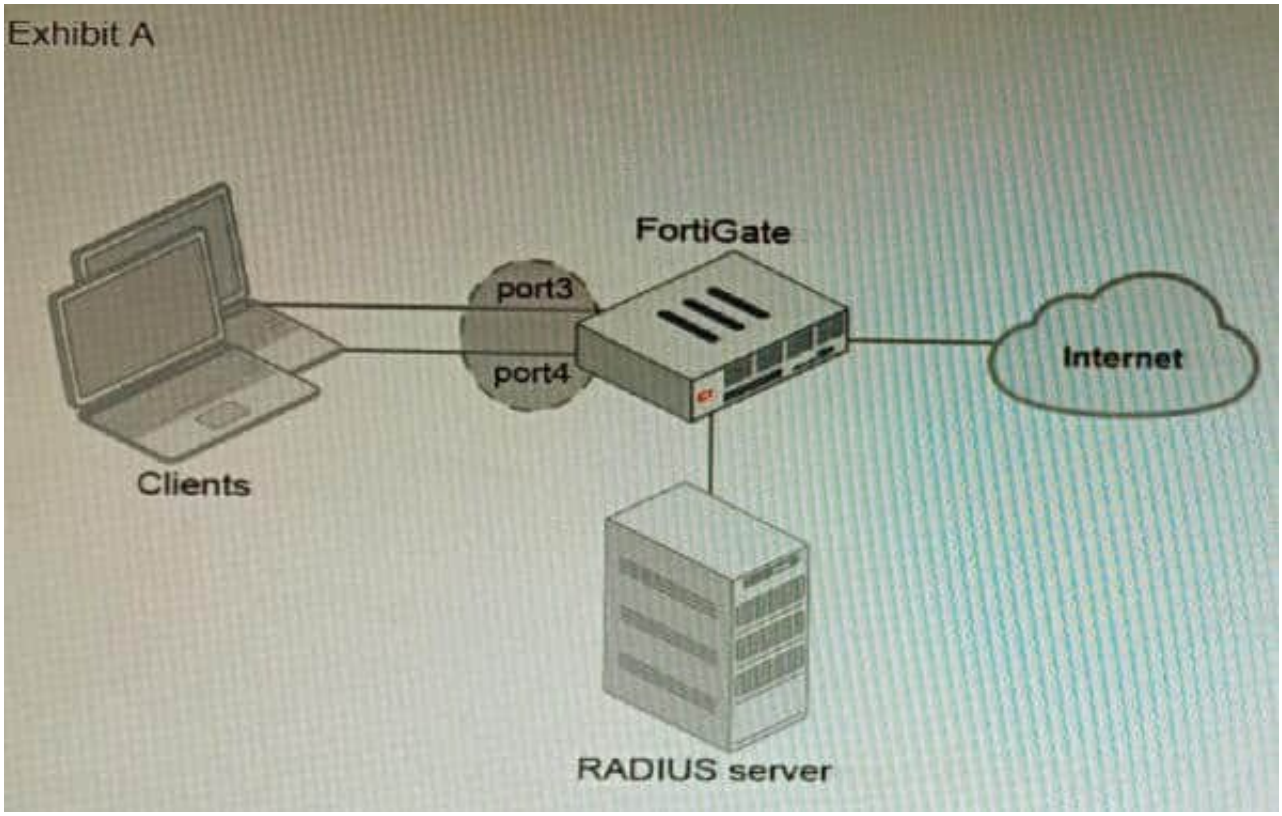
The mappings are matched from top to bottom, so the first mapping that matches the conditions will be used. In this case, the first mapping matches because the packet loss is greater than 10%. Therefore, the FEC behavior will be 2

redundant packets for every 8 base packets.

Reference: https://docs.fortinet.com/document/fortigate/7.0.0/new- features/169010/adaptive-forward-error-correction-7-0-2

QUESTION 9

Refer to the exhibits.



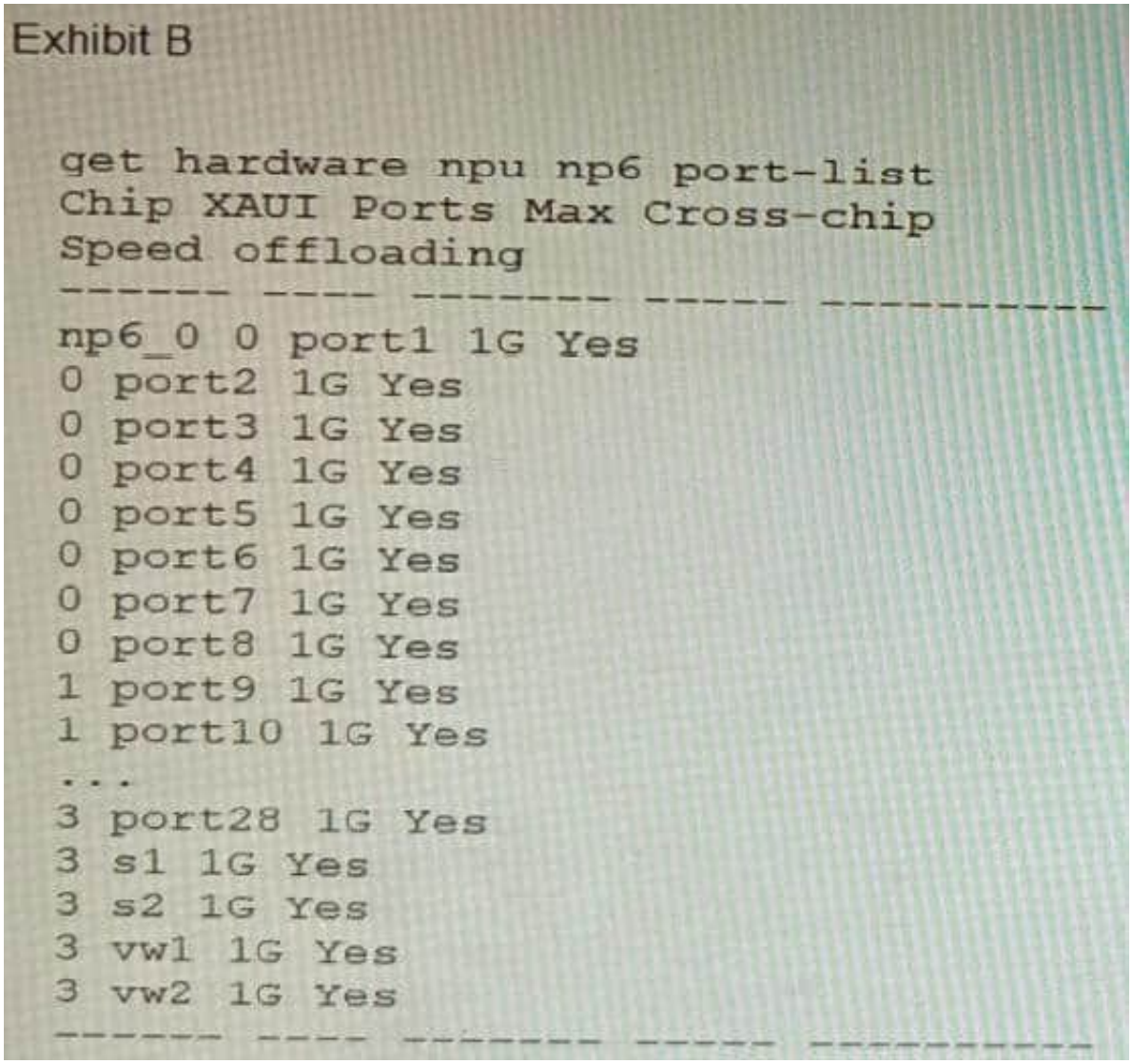


Exhibit B

```
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

Correct Answer: BD

Explanation: 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 "sslinspection". 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-switchinterfaceshttps://docs.fortinet.com/document/fortigate/7.0.0/administration- guide/19662/802-1x-authentication

QUESTION 10

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:zeyD2XmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS" -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.

Correct Answer: BD

Explanation: 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 "

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