NSE8$^{Q\&As}$

Fortinet Network Security Expert 8 Written (800)

Pass Fortinet NSE8 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse8.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A customer wants to implement a RADIUS Single Sign On (RSSO) solution for multiple FortiGate devices. The customer\\'s network already includes a RADIUS server that can generate the logon and logoff accounting records. However, the

RADIUS server can send those records to only one destination.

What should the customer do to overcome this limitation?

A. Send the RADIUS records to an LDAP server and add the LDAP server to the FortiGate configuration.

B. Send the RADIUS records to an RSSO Collector Agent.

C. Send the RADIUS records to one of the FortiGate devices, which can replicate them to the other FortiGate units.

D. Use the RADIUS accounting proxy feature available in FortiAuthenticator devices.

Correct Answer: B

References: http://docs.fortinet.com/uploaded/files/1937/fortigate-authentication-52.pdf

QUESTION 2

You have received an issue report about users not being able to use a video conferencing application. This application uses two UDP ports and two TCP ports to communicate with servers on the Internet. The network engineering team has

confirmed there is no routing problem. You are given a copy of the FortiGate configuration.

Which three configuration objects will you inspect to ensure that no policy is blocking this traffic? (Choose three.)

A. config firewall interface-policy

B. config firewall DoS-policy

C. config firewall policy

D. config firewall multicast-policy

E. config firewall sniffer-policy

Correct Answer: BCE

QUESTION 3

Given the following FortiOS 5.2 commands:

Which vulnerability is being addresses when managing FortiGate through an encrypted management protocol?

A. Remote Exploit Vulnerability in Bash (ShellShock)

B. Information Disclosure Vulnerability in OpenSSL (Heartbleed)

C. SSL v3 POODLE Vulnerability

D. SSL/TLS MITM vulnerability (CVE-2014-0224)

Correct Answer: C

References: http://kb.fortinet.com/kb/documentLink.do?externalID=FD36913

QUESTION 4

You are asked to implement a wireless network for a conference center and need to provision a high number of access points to support a large number of wireless client connections. Which statement describes a valid solution for this requirement?

A. Use a captive portal for guest access. Use both 2.4 GHz and 5 GHz bands. Enable frequency and access point hand-off. Use more channels, thereby supporting more clients.

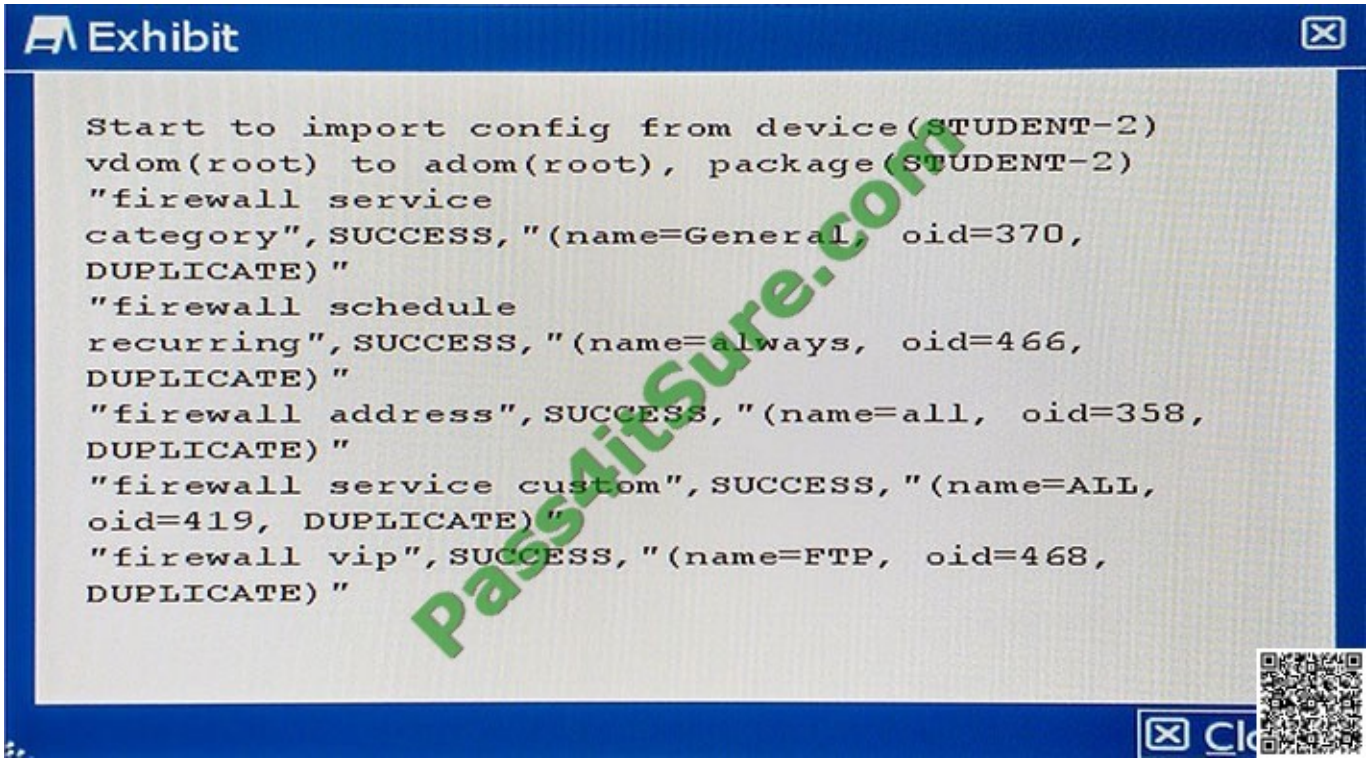
B. Use an open wireless network with no portal. Use both 2.4 GHz and 5 GHz bands. Use 802.11ac capable access points and configure channel bonding to support greater throughput for wireless clients.

C. Use a pre-shared key only for wireless client security. Use the 5 GHz band only for greater security. Use 802.11ac capable access points and configure channel bonding to support greater throughput for wireless clients.

D. Use a captive portal for guest access. Use both the 2.4 GHz and 5 GHz bands, and configure frequency steering. Configure rogue access point detection in order to automatically control the transmit power of each AP.

Correct Answer: D

QUESTION 5



The output shown in the exhibit from FortiManager is displayed during an import of the device configuration. Which statement describes the correct action taken for these duplicate objects?

A. The import fails because of the duplicate entries detected which exist in the ADOM database.

B. FortiManager installs these duplicate objects to the managed device from the ADOM database.

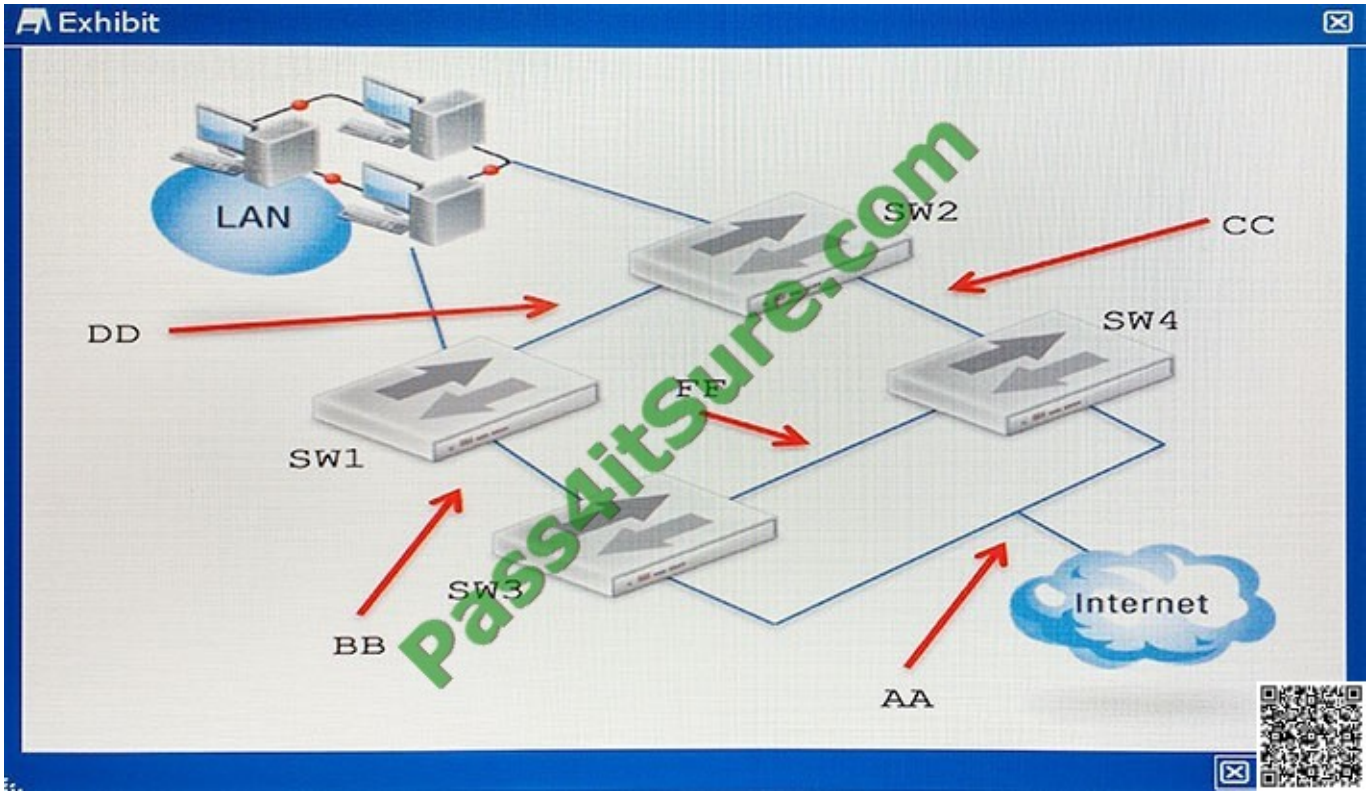
C. FortiManager does not import these duplicate entries into the ADOM database because they already exist in the ADOM database.

D. FortiManager creates indexed duplicate entries for these objects in the ADOM database.

Correct Answer: B

References: http://docs.fortinet.com/uploaded/files/2905/FortiManager-5.4.0-Administration-Guide.pdf

QUESTION 6



A customer wants to secure the network shown in the exhibit with a full redundancy design. Which security design would you use?

A. Place a FortiGate FGCP Cluster between DD and AA, then connect it to SW1, SW2, SW3, and SW4.

B. Place a FortiGate FGCP Cluster between BB and CC, then connect it to SW1, SW2, SW3, and SW4.

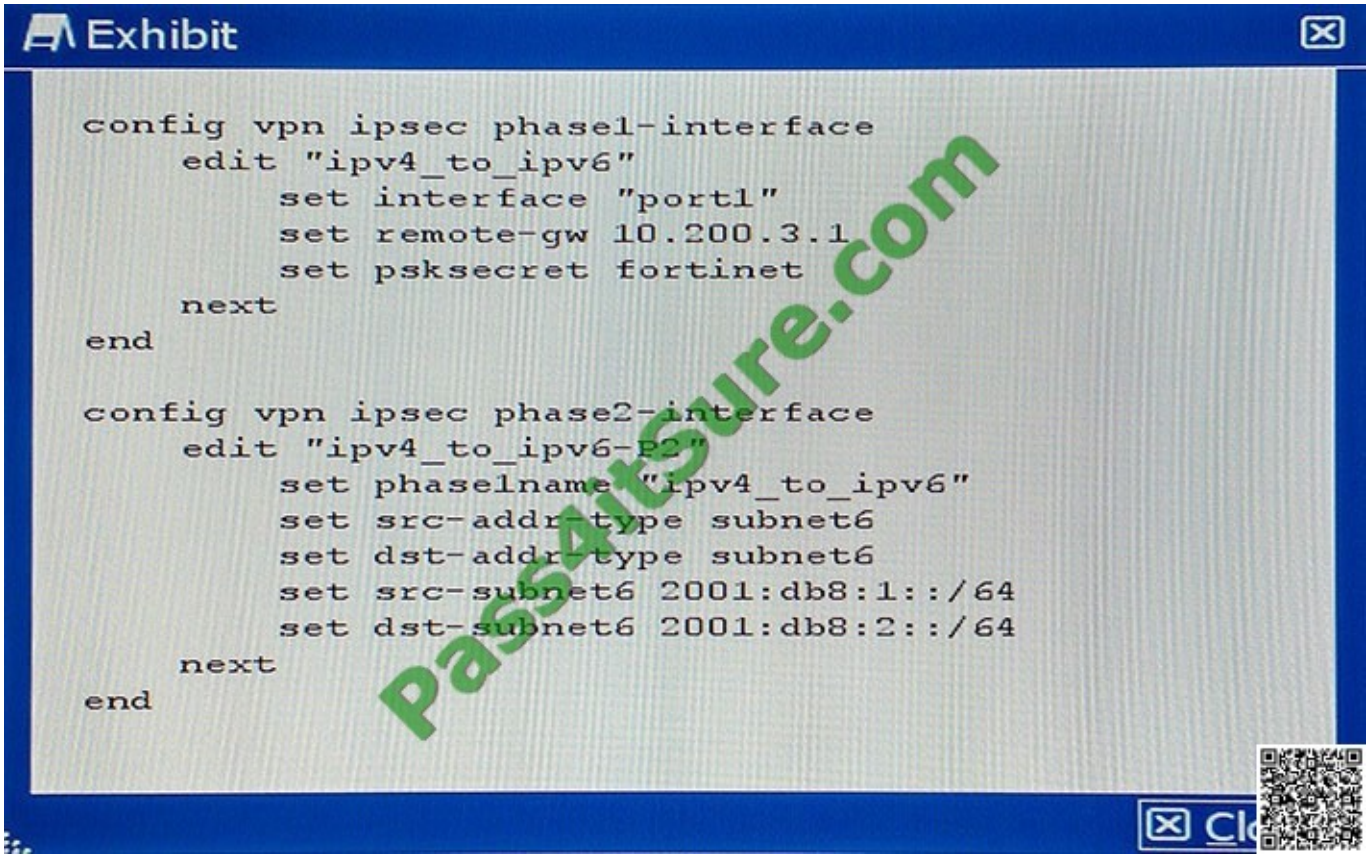
C. Place a FortiGate FGCP Cluster between BB and AA, then connect it to SW1, SW2, SW3, and SW4.

D. Place a FortiGate FGCP Cluster between DD and FF, then connect it to SW1, SW2, SW3, and SW4.

Correct Answer: A

QUESTION 7

You want to enable traffic between 2001:db8:1::/64 and 2001:db8:2::/64 over the public IPv4 Internet.



Given the CLI configuration shown in the exhibit, which two additional settings are required on this device to implement tunneling for the IPv6 transition? (Choose two.)

A. IPv4 firewall policies to allow traffic between the local and remote IPv6 subnets.

B. IPv6 static route to the destination phase2 destination subnet.

C. IPv4 static route to the destination phase2 destination subnet.

D. IPv6 firewall policies to allow traffic between the local and remote IPv6 subnets.

Correct Answer: D

References: http://docs.fortinet.com/uploaded/files/1969/IPv6%20Handbook%20for%20FortiOS%205.2.pdf

QUESTION 8

A company has just installed a new FortiGate in their core to route and inspect traffic between their subnetted VLANs. The security department reports that after the installation, their IP video cameras no longer work. Research by the IT

department shows that the video system uses a multicast stream to send the video to multiple video receivers.

Which two commands must be configured to resolve this problem? (Choose two.)

A.

```
config firewall multicast-policy
    edit 1
        set action accept
    next
end
```

B.

```
config system settings
    set multicast-forward enable
    set multicast-skip-policy disable

end
```

C.

```
config system multicast
    edit 1
        set forward enable
    next
end
```

D.

```
config firewall policy
    edit 1
        set srcintf "any"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set service "multicast"
    next
end
```


A. B. C. D.

Correct Answer: BD

http://kb.fortinet.com/kb/documentLink.do?externalID=FD36500

QUESTION 9

You are asked to write a FortiAnalyzer report that lists the session that has consumed the most bandwidth. You are required to include the source IP, destination IP, application, application category, hostname, and total bandwidth consumed. Which dataset meets these requirements?

A. select from_itime(itime) as timestamp, srcip, dstip, app, appcat, hostname, sum(coalesce(`sentbyte", 0) +coalesce

(`recbyte ", 0)) as bandwidth from $log where $filter LIMIT 1

B. select from_itime(itime) as timestamp, srcip, dstip, app, appcat, hostname, sum(coalesce(`sentbyte", 0) +coalesce (`recbyte", 0)) as bandwidth from $log where $filter LIMIT 1

C. select from_itime(itime) as timestamp, srcip, dstip, app, appcat, hostname, sum(coalesce(`sentbyte", 0) +coalesce (`rcvdbyte", 0)) as bandwidth from $log where $filter LIMIT 1

D. select from_itime(itime) as timestamp, sourceip, destip, app, appcat, hostname, sum(coalesce(`sentbyte\\', 0)+coalesce (`rcvdbyte", 0)) as bandwidth from $log where $filter LIMIT 1

Correct Answer: C

References: http://docs.fortinet.com/uploaded/files/2617/fortianalyzer-5.2.4-dataset-reference.pdf

QUESTION 10

There is an interface-mode IPsec tunnel configured between FortiGate1 and FortiGate2. You want to run OSPF over the IPsec tunnel. On both FortiGates. the IPsec tunnel is based on physical interface port1. Port1 has the default MTU

setting on both FortiGate units.

Which statement is true about this scenario?

A. A multicast firewall policy must be added on FortiGate1 and FortiGate2 to allow protocol 89.

B. The MTU must be set manually in the OSPF interface configuration.

C. The MTU must be set manually on the IPsec interface.

D. An IP address must be assigned to the IPsec interface on FortiGate1 and FortiGate2.

Correct Answer: B

If MTU doesn\\'t match then the neighbour ship gets stuck in exchange state.

QUESTION 11

You verified that application control is working from previous configured categories. You just added Skype on blocked signatures. However, after applying the profile to your firewall policy, clients running Skype can still connect and use the

application.

What are two causes of this problem? (Choose two.)

A. The application control database is not updated.

B. SSL inspection is not enabled.

C. A client on the network was already connected to the Skype network and serves as relay prior to configuration changes to block Skype

D. The FakeSkype.botnet signature is included on your application control sensor.

Correct Answer: AB

QUESTION 12

Which two features are supported only by FortiMail but not by FortiGate? (Choose two.)

A. DNSBL

B. built-in MTA

C. end-to-end IBE encryption

D. FortiGuard Antispam

Correct Answer: AB

QUESTION 13

A university is looking for a solution with the following requirements:

-wired and wireless connectivity

-authentication (LDAP)

-Web filtering, DLP and application control

-data base integration using LDAP to provide access to those students who are up-to-date with their monthly payments

-support for an external captive portal

Which solution meets these requirements?

A. FortiGate for wireless controller and captive portal FortiAP for wireless connectivity FortiAuthenticator for user authentication and REST API for DB integration FortiSwitch for PoE connectivity FortiAnalyzer for log and report

B. FortiGate for wireless controller FortiAP for wireless connectivity FortiAuthenticator for user authentication, captive portal and REST API for DB integration FortiSwitch for PoE connectivity FortiAnalyzer for log and report

C. FortiGate for wireless control and user authentication FortiAuthenticator for captive portal and REST API for DB integration FortiAP for wireless connectivity FortiSwitch for PoE connectivity FortiAnalyzer for log and report

D. FortiGate for wireless controller FortiAP for wireless connectivity and captive portal FortiSwitch for PoE connectivity FortiAuthenticator for user authentication and REST API for DB integration FortiAnalyzer for log and reports

Correct Answer: A

QUESTION 14

Which command syntax would you use to configure the serial number of a FortiGate as its host name?

A.
```
config system global
set hostname &SerialNum
end
```

B.
```
config system global
set hostname @SerialNum
end
```

C.
```
config system global
set hostname $SerialNum
end
```

D.
```
config system global
set hostname SerialNum
end
```


A. B. C. D.

Correct Answer: C

References:
http://docs.fortinet.com/uploaded/files/2002/FortiOS%20Handbook%20-%20System%20Administration%205.2.pdf

QUESTION 15

Your company uses a cluster of two FortiGate 3600C units in active-passive mode to protect the corporate network. The FortiGate cluster sends its logs to a FortiAnalyzer and you have configured scheduled weekly reports for the Internet

bandwidth usage of each corporate VLAN. During a scheduled maintenance window, you make a series of configuration changes. When the next FortiAnalyzer weekly report is generated, you notice that Internet bandwidth usage reported by

the FortiAnalyzer is far less than expected.

What is the reason for this discrepancy?

A. You applied an antivirus profile on some of the policies, and no traffic can be accelerated.

B. You disabled all security profiles on some of the firewall policies, and the traffic matching those policies is now accelerated.

C. You enabled HA session-pickup, which is turn disabled session accounting.

D. You changed from active-passive to active-active, causing the session traffic counters to become inaccurate.

Correct Answer: D

Because of Active/Active failover traffic segregate to boxes where it reduces the bandwidth utilization