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.leads4pass.com/nse8_812.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibits.

Exhibit A

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

Exhibit B

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

A customer wants to deploy 12 FortiAP 431F devices on high density conference center, but they do not currently have any PoE switches to connect them to. They want to be able to run them at full power while having network redundancy From the FortiSwitch models and sample retail prices shown in the exhibit, which build of materials would have the lowest cost, while fulfilling the customer\\'s requirements?

A. 1x FortiSwitch 248EFPOE

B. 2x FortiSwitch 224E-POE

C. 2x FortiSwitch 248E-FPOE

D. 2x FortiSwitch 124E-FPOE

Correct Answer: C

Explanation: The customer wants to deploy 12 FortiAP 431F devices on a high density conference center, but they do not have any PoE switches to connect them to. They want to be able to run them at full power while having network redundancy. PoE switches are switches that can provide both data and power to connected devices over Ethernet cables, eliminating the need for separate power adapters or outlets. PoE switches are useful for deploying devices such as wireless access points, IP cameras, and VoIP phones in locations where power outlets are scarce or inconvenient. The FortiAP 431F is a wireless access point that supports PoE+ (IEEE 802.3at) standard, which can deliver up to 30W of power per port. The FortiAP 431F has a maximum power consumption of 25W when running at full power. Therefore, to run 12 FortiAP 431F devices at full power, the customer needs PoE switches that can provide at least 300W of total PoE power budget (25W x 12). The customer also needs network redundancy, which means that they need at least two PoE switches to connect the FortiAP devices in case one switch fails or loses power. From the FortiSwitch models and sample retail prices shown in the exhibit, the build of materials that has the lowest cost while fulfilling the customer\\'s requirements is 2x FortiSwitch 248E- FPOE. The FortiSwitch 248E-FPOE is a PoE switch that has 48 GE ports with PoE+ capability and a total PoE power budget of 370W. It also has 4x 10 GE SFP+ uplink ports for high-speed connectivity. The sample retail price of the FortiSwitch 248E-FPOE is $1,995, which means that two units will cost $3,990. This is the lowest cost among the other options that can meet the customer\\'s requirements. Option A is incorrect because the FortiSwitch 248EFPOE is a non-PoE switch that has no PoE capability or power budget. It cannot provide power to the FortiAP devices over Ethernet cables. Option B is incorrect because the FortiSwitch 224E-POE is a PoE switch that has only 24 GE ports with PoE+ capability and a total PoE powerbudget of 185W. It cannot provide enough ports or power to run 12 FortiAP devices at full power. Option D is incorrect because the FortiSwitch 124E-FPOE is a PoE switch that has only 24 GE ports with PoE+ capability and a total PoE power budget of 185W. It cannot provide enough ports or power to run 12 FortiAP devices at full power. References: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSwitch_Secure_Access_Series.pdfhttps://www.fortinet.com/content/dam/fortine t/assets/data-sheets/FortiAP_400_Series.pdf

QUESTION 2

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.

Correct Answer: AD

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

If the access control rule to relay from Office 365 servers FQDN is missing, then FortiMail will not be able to send emails to Office 365. This is because the access control rule specifies which IP addresses or domains are allowed to relay

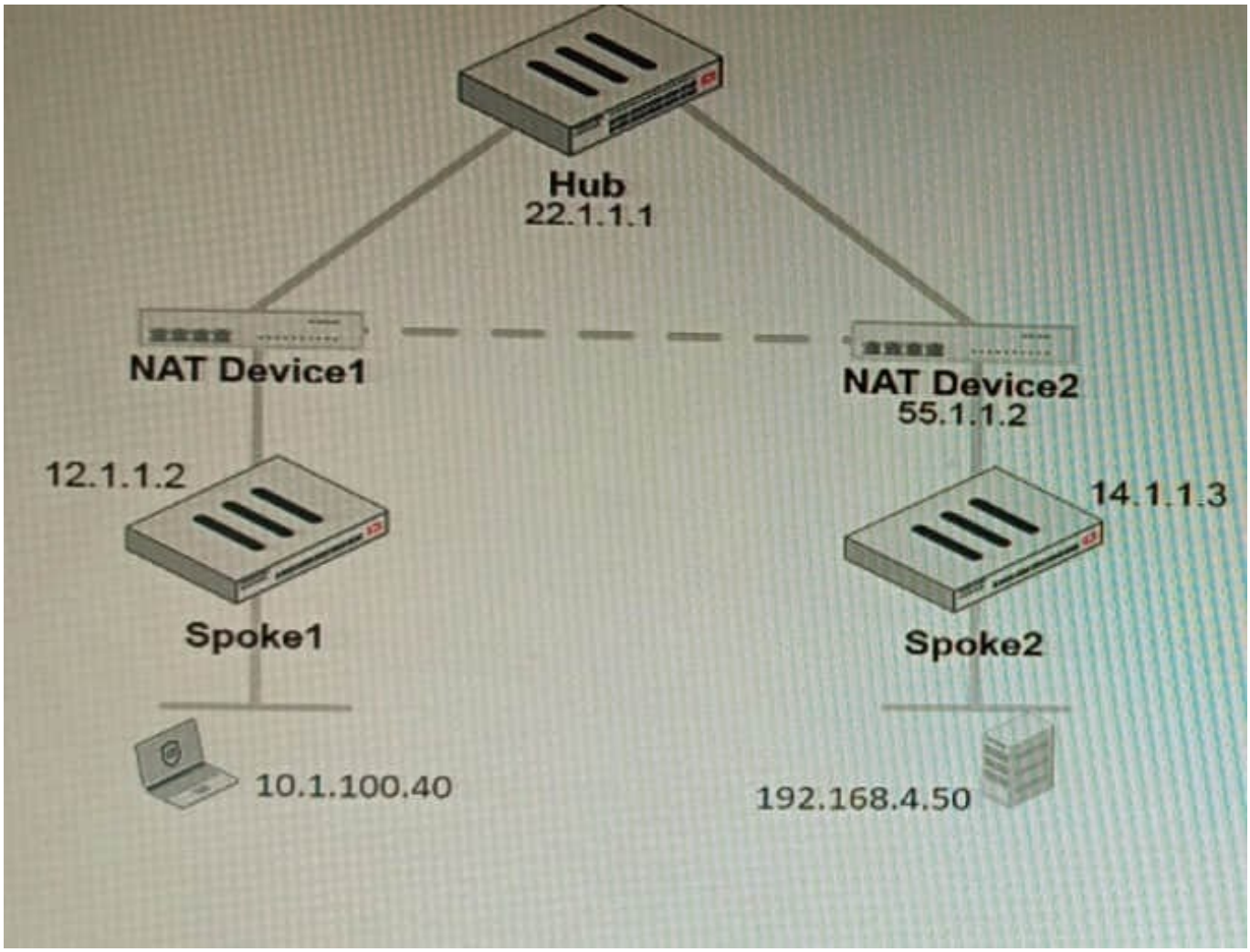
emails through FortiMail. D. A Mail Flow connector from the Exchange Admin Center has not been set properly to the FortiMail Cloud FQDN.

If the Mail Flow connector from the Exchange Admin Center is not set properly to the FortiMail Cloud FQDN, then Office 365 will not be able to send emails to FortiMail. This is because the Mail Flow connector specifies which SMTP server is

used to send emails to external recipients.

QUESTION 3

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

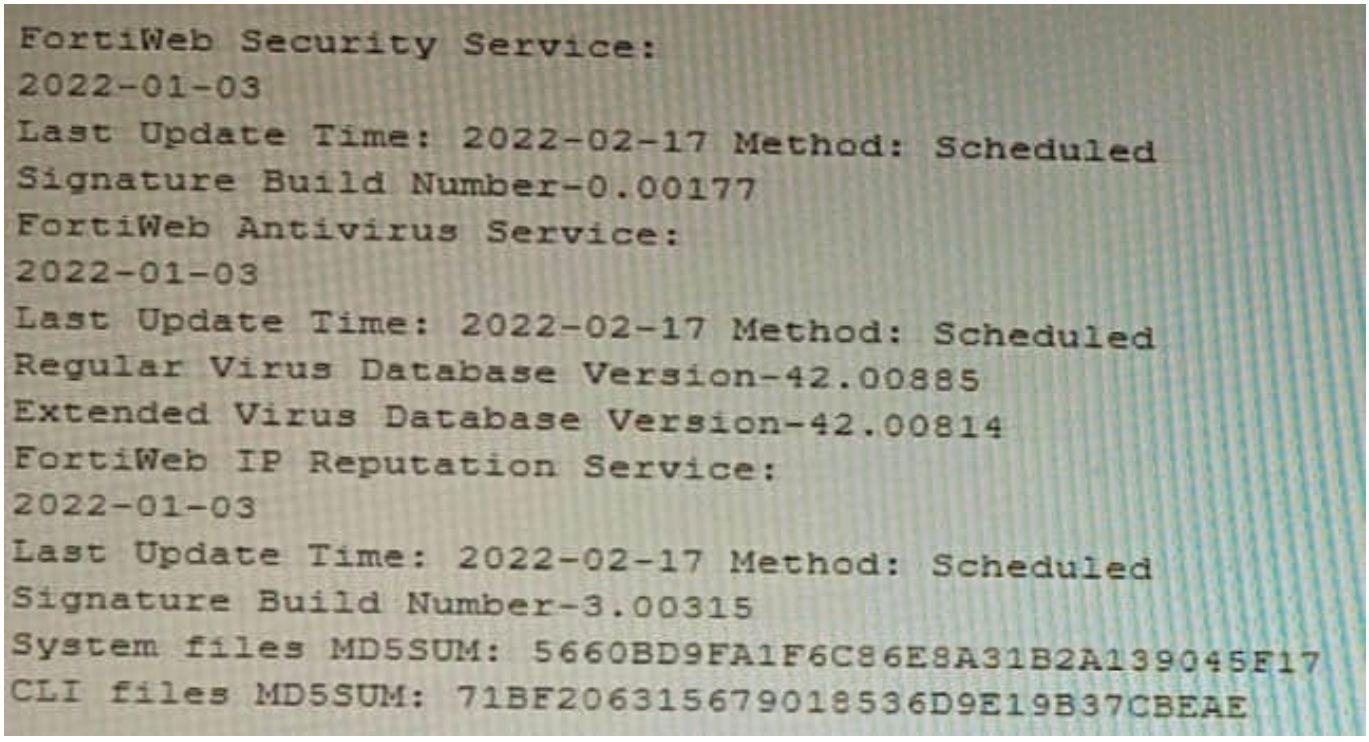
D. Spoke1 will establish an ADVPN shortcut to Spoke2

Correct Answer: D

Explanation: 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

QUESTION 4

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

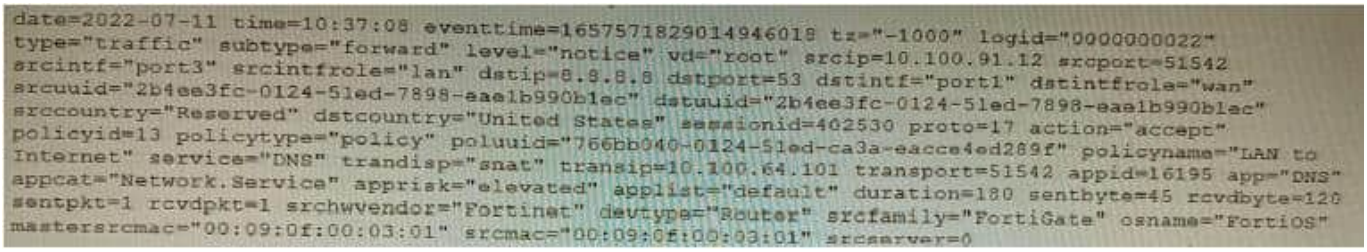
E. Reputation from blacklisted IP addresses from DHCP or PPPoE pools can be restored

Correct Answer: BE

Explanation: 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 belongto 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-reputationhttps://docs.fortinet.com/document/fortiweb/6.4.0/administration- guide/19662/geographical-ip-policies

QUESTION 5

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

Correct Answer: C

Explanation: 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. References:https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration- guide/103664/time-zone-and-daylight-saving-time