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.geekcert.com/nse8_812.html

100% Passing Guarantee
100% Money Back Assurance

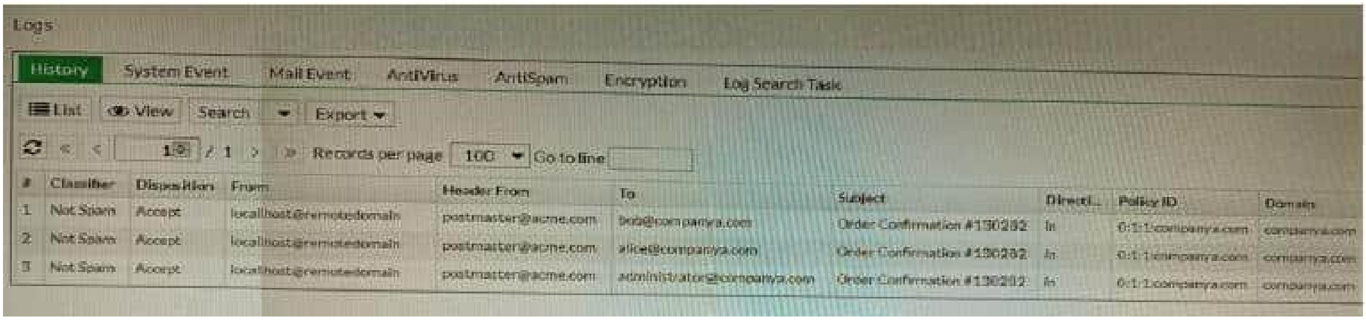
Following Questions and Answers are all new published by Fortinet Official Exam Center

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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

Refer to the exhibit showing the history logs from a FortiMail device.



#	Classifier	Disposition	From	Header From	To	Subject	Direct...	Policy ID	Domain
1	Not Spam	Accept	localhost@remotedomain	postmaster@acme.com	bob@companya.com	Order Confirmation #130282	In	0:1:1:companya.com	companya.com
2	Not Spam	Accept	localhost@remotedomain	postmaster@acme.com	alice@companya.com	Order Confirmation #130282	In	0:1:1:companya.com	companya.com
3	Not Spam	Accept	localhost@remotedomain	postmaster@acme.com	administrator@companya.com	Order Confirmation #130282	In	0:1:1:companya.com	companya.com

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

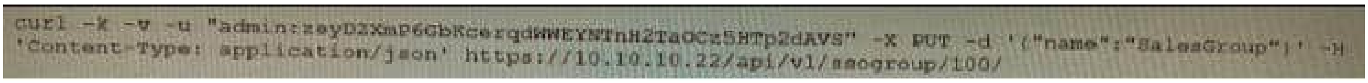
D. Soft fail SPF validation in an antispam profile

Correct Answer: C

Explanation: 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/administrationguide/103663/impersonation-analysis

QUESTION 2

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

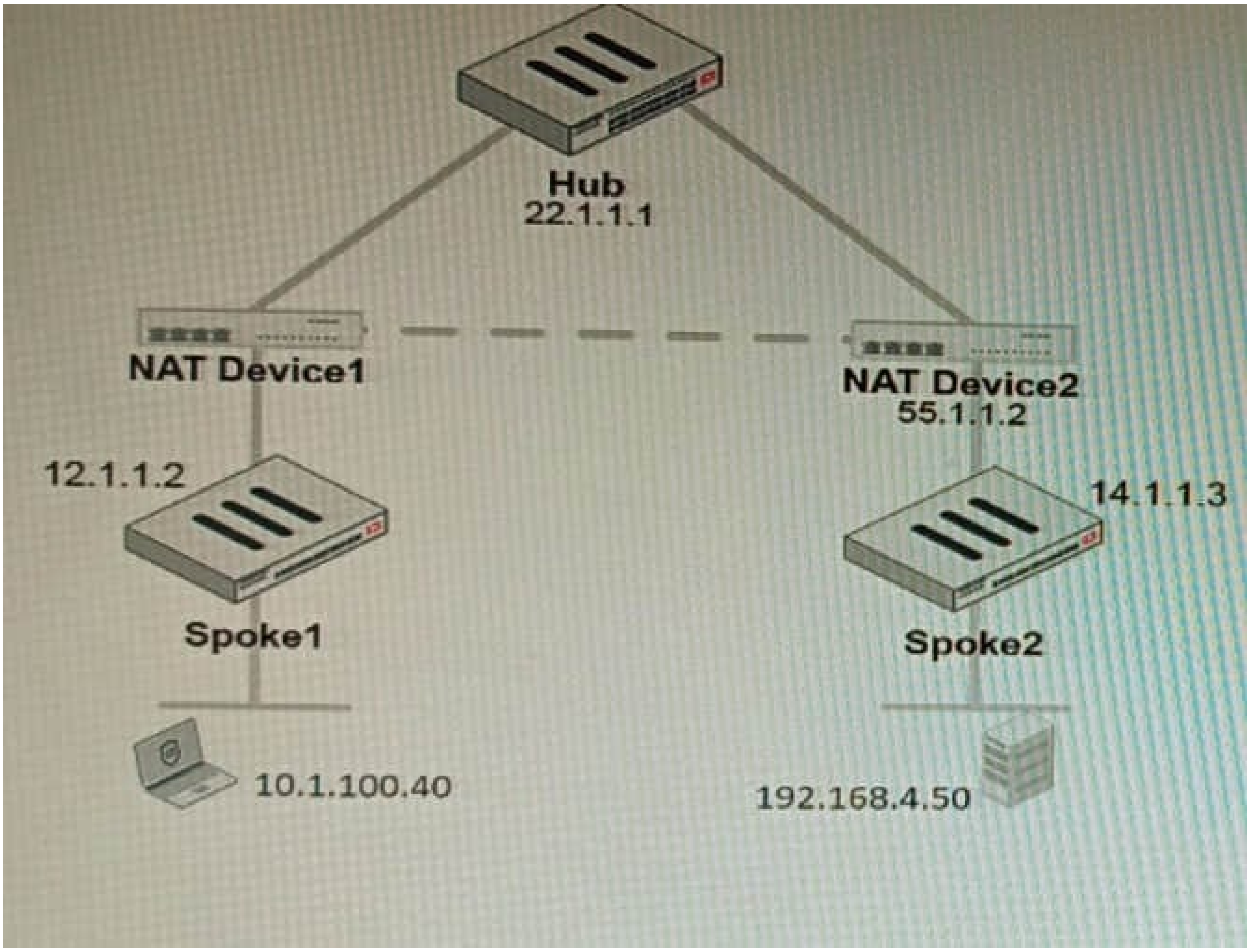
"Authorization: Bearer "

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

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

Which feature must you enable on the BGP neighbors to accomplish this goal?

A. Graceful-restart

B. Deterministic-med

C. Synchronization

D. Soft-reconfiguration

Correct Answer: A

Explanation: 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

QUESTION 5

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

Correct Answer: AC

Explanation: ZTNA supports SSH connection rules that allow remote workers to access SSH servers inside the network through an HTTPS tunnel between the client and the access proxy (FortiGate). The access proxy acts as an SSH client to connect to the real SSH server on behalf of the user, and performs host-key validation to verify the identity of the server. The user can use any SSH client that supports HTTPS proxy settings, such as PuTTY or OpenSSH. References:https://docs.fortinet.com/document/fortigate/7.0.0/ztna- deployment/899992/configuring-ztna-rules-to-control-access

NSE8_812 PDF Dumps NSE8_812 Practice Test NSE8_812 Braindumps