NSE7_EFW-6.4^{Q&As}

Fortinet NSE 7 - Enterprise Firewall 6.4

Pass Fortinet NSE7_EFW-6.4 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse7_efw-6-4.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

Which two statements about an auxiliary session are true? (Choose two.)

A. With the auxiliary session setting enabled, ECMP traffic is accelerated to the NP6 processor.

B. With the auxiliary session setting enabled, two sessions will be created in case of routing change.

C. With the auxiliary session setting disabled, for each traffic path, FortiGate will use the same auxiliary session.

D. With the auxiliary session disabled, only auxiliary sessions will be offloaded.

Correct Answer: CD

Reference: https://docs.fortinet.com/document/fortigate/7.0.1/administration- guide/14295/controllingreturn-path-with-auxiliary-session

---

QUESTION 2

What global configuration setting changes the behavior for content-inspected traffic while FortiGate is in system conserve mode?

A. av-failopen

B. mem-failopen

C. utm-failopen

D. ips-failopen

Correct Answer: A

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles- 54/Other_Profile_Considerations/Conserve%20mode.htm

---

QUESTION 3

Refer to the exhibit, which shows a FortiGate configuration.

```
config system fortiguard
    set protocol udp
    set port 8888
    set load-balance-servers 1
    set auto-join-forticloud enable
    set update-server-location any
    set sandbox-region ''
    set fortiguard-anycast disable
    set antispam-force-off disable
    set antispam-cache enable
    set antispam-cache-ttl 1800
    set antispam-cache-mpercent 2
    set antispam-timeout 7
    set webfilter-force-off enable
    set webfilter-cache enable
    set webfilter-cache-ttl 3600
    set webfilter-timeout 15
    set sdns-server-ip "208.91.112.220"
    set sdns-server-port 53
    unset sdns-options
    set source-ip 0.0.0.0
    set source-ip6 ::
    set proxy-server-ip 0.0.0.0
    set proxy-server-port 0
    set proxy-username ''
    set ddns-server-ip 0.0.0.0
    set ddns-server-port 443
end
```

An administrator is troubleshooting a web filter issue on FortiGate. The administrator has configured a web filter profile and applied it to a policy; however, the web filter is not inspecting any traffic that is passing through the policy.

What must the administrator change to fix the issue?

A. The administrator must increase webfilter-timeout.

B. The administrator must disable webfilter-force-off.

C. The administrator must change protocol to TCP.

D. The administrator must enable fortiguard-anycast.

Correct Answer: D

Reference: https://docs.fortinet.com/document/fortigate/6.4.5/cli-reference/109620/config- systemfortiguard

QUESTION 4

What is the purpose of an internal segmentation firewall (ISFW)?

A. It inspects incoming traffic to protect services in the corporate DMZ.

B. It is the first line of defense at the network perimeter.

C. It splits the network into multiple security segments to minimize the impact of breaches.

D. It is an all-in-one security appliance that is placed at remote sites to extend the enterprise network.

Correct Answer: C

ISFW splits your network into multiple security segments. They serve as a breach containers from attacks that come from inside.

QUESTION 5

Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7. . . .
ike 0: IKEv2 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response. . .
ike 0: Remotesite:3: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated
ike 0: Remotesite:3: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0: Remotesite:3: peer is FortiGate/FortiOS (v0 b0)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: received peer identifier FQDN 'remote'
ike 0: Remotesite:3: negotiation result
ike 0: Remotesite:3: proposal id = 1:
ike 0: Remotesite:3:     protocol id = ISAKMP:
ike 0: Remotesite:3:         trans_id = KEY_IKE.
ike 0: Remotesite:3:         encapsulation = IKE/none.
ike 0: Remotesite:3:             type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0: Remotesite:3:             type=OAKLEY_HASH_ALG, val=SHA.
ike 0: Remotesite:3:             type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: Remotesite:3:             type=OAKLEY_GROUP, val=MODP1024.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key
16:39915120ED73ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc
A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A07BE09026CA8B2
ike 0: Remotesite:3: out
A2FBD6BB6394401A06B89C022D4DF68208100401000000000000005C64D5CBA90B873F150CB8B5CC2A
ike 0: Remotesite:3: sent IKE msg (agg_i2send): 10.0.0.1:500->10.0.0.2:500, len=140,
id=a2fbd6bb6394401a/
ike 0: Remotesite:3: established IKE SA a2fbd6bb6394401a/06b89c022d4df682
```

Which two statements about this debug output are correct? (Choose two.)

A. The remote gateway IP address is 10.0.0.1.

B. The initiator provided remote as its IPsec peer ID.

C. It shows a phase 1 negotiation.

D. The negotiation is using AES128 encryption with CBC hash.

Correct Answer: BC

[NSE7_EFW-6.4 PDF Dumps](#)

[NSE7_EFW-6.4 Practice Test](#)

[NSE7_EFW-6.4 Braindumps](#)