

Exam : FCSS_EFW_AD-7.4

**Title : FCSS - Enterprise Firewall
7.4 Administrator**

Version : DEMO

1.An administrator must ensure that users cannot access sites containing malware and spyware, while also protecting them from phishing attempts.

What is the most resource-efficient method to block access to these sites?

- A. Enable antivirus profiles to scan all web traffic and block downloads from these malicious sites.
- B. Configure FortiGuard Web Filtering and block the categories malware, spyware, and phishing to prevent access to such sites.
- C. Create a custom IPS policy to monitor and block all outbound traffic related to malware, spyware, and phishing sites.
- D. Set up a DNS filter and block domains related to these categories to stop users from reaching malicious content.

Answer: B

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

Answer: A

3.Examine the following traffic log; then answer the question below.

date=20xx-02-01 time=19:52:01 devname=masterdevice_id="xxxxxxx" log_id=0100020007 type=event subtype=system pri critical vd=root service=kemel status=failure msg="NAT port is exhausted."

What does the log mean?

- A. There is not enough available memory in the system to create a new entry in the NAT port table.
- B. The limit for the maximum number of simultaneous sessions sharing the same NAT port has been reached.
- C. FortiGate does not have any available NAT port for a new connection.
- D. The limit for the maximum number of entries in the NAT port table has been reached.

Answer: B

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

```

ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C9688696FC77570100
ike 0:624000:98: VID FRAGMENTATION 404887D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 404887D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
ike 0:624000:98:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
ike 0:624000:98:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:       type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
ike 0:624000:98:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:       type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
ike 0:624000:98:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:       type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:       type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen

```

The administrator does not have access to the remote gateway.

Based on the debug output, which configuration change can the administrator make to the local gateway to resolve the phase 1 negotiation error?

- A. In the phase 1 network configuration, set the IKE version to 2.
- B. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.
- C. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.
- D. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.

Answer: D

5.Refer to the exhibit, which shows a partial web filter profile configuration.

FortiGuard Category Based Filter

Name	Action
Bandwidth Consuming 6	
Freeware and Software Downloads	Allow
File Sharing and Storage	Block

Static URL Filter

URL Filter

+ Create New

Edit

Delete

Search

URL	Type	Action	Status
*.dropbox.com	Wildcard	Allow	Enable

Content Filter

+ Create New

Edit

Delete

Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	Exempt	Enable

Which action will FortiGate take if a user attempts to access www.dropbox.com, which is categorized as File Sharing and Storage?

- A. FortiGate will block the connection, based on the FortiGuard category based filter configuration.
- B. FortiGate will block the connection as an invalid URL.
- C. FortiGate will exempt the connection, based on the Web Content Filter configuration.
- D. FortiGate will allow the connection, based on the URL Filter configuration.

Answer: D