Fortinet

Exam Questions FCSS_NST_SE-7.6

FCSS - Network Security 7.6 Support Engineer

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

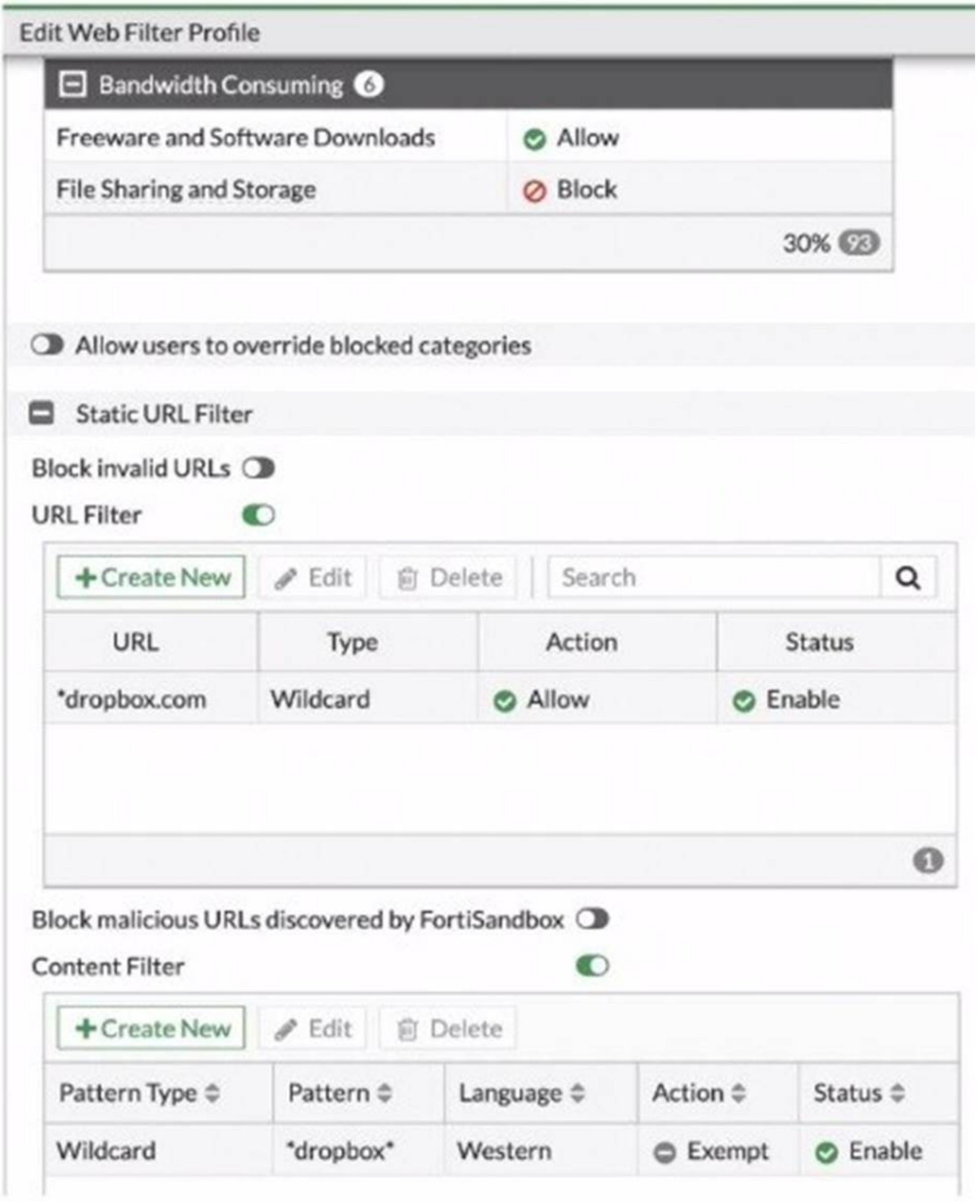
* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Exhibit.



Refer to the exhibit, which shows a partial web fillet profile configuration.
Which action does FortiGate lake if a user attempts to access www. dropbox. com, which is categorized as File Sharing and Storage?

A. FortiGate allows the connection, based on the URL Filter configuration.
B. FortiGate blocks the connection as an invalid URL.
C. FortiGate exempts the connection, based on the Web Content Filter configuration.
D. FortiGate blocks the connection, based on the FortiGuard category based filter configuration.

Answer: D

NEW QUESTION 2
In which two slates is a given session categorized as ephemeral? (Choose two.)

A. A UDP session with only one packet received
B. A UOP session with packets sent and received
C. A TCP session waiting for the SYN ACK
D. A TCP session waiting for FIN ACK

Answer: AC

NEW QUESTION 3
What are two reasons you might see iprope_in_check() check failed, drop when using the debug flow? (Choose two.)

A. Packet was dropped because of policy route misconfiguration.
B. Packet was dropped because of traffic shaping.
C. Trusted host list misconfiguration.
D. VIP or IP pool misconfiguration.

Answer: CD

NEW QUESTION 4
Exhibit.

```
config system fortiguard
    set protocol udp
    set port 8888
    set load-balance-servers1
    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-mpercent2
    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-iD6 ::
    set proxv-server-ip 0.0.0.0
    set proxy-server-port 0
    set proxy-username
    set ddns-server-ip 0.0.0.0
    set dons-server-port 443
end
```

Refer to the exhibit, which shows a FortiGate configuration.
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 do to fix the issue?

A. Disable webfilter-force-off.
B. Increase webfilter-timeout.
C. Enable fortiguard-anycast.
D. Change protocol to TCP.

Answer: A

NEW QUESTION 5
Exhibit 1.

```
config system global
    set snat-route-change disable
end
-------------------
config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

Exhibit 2.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport= av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan cos=0/255
state=log may_dirty npu f00
statistic (bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/ (before, after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c56 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

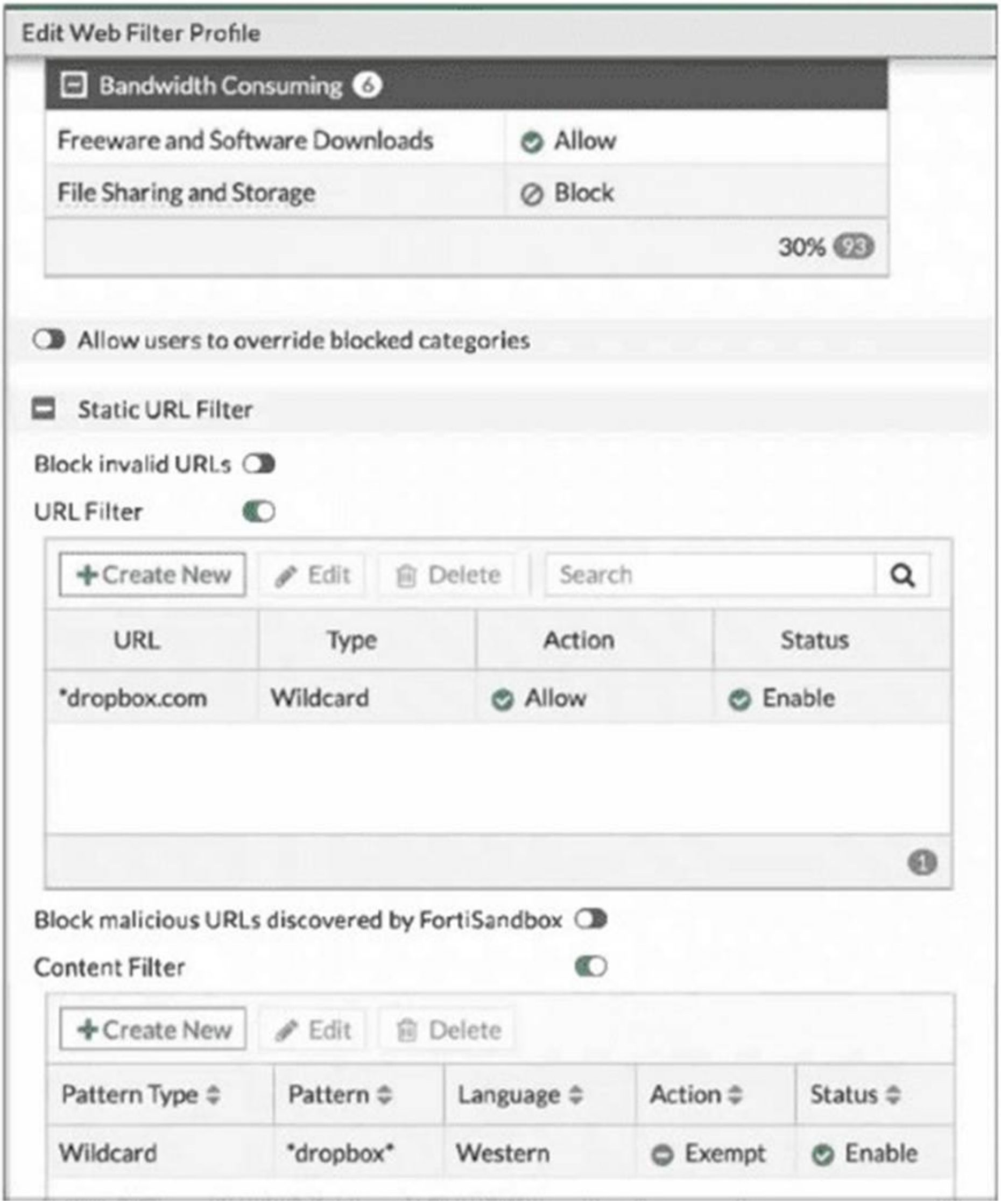
Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.
An administrator would like to lest session failover between the two service provider connections.
Which two changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

A. Change the priority of the port! static route to 11.
B. Change the priority of the port2 static route to 5.
C. Configure unset snat-route-change to return it to the default setting.
D. Configure set snat-route-change enable.

Answer: AD

NEW QUESTION 6
Refer to the exhibit, which shows a partial web filter profile configuration.

Web filter profile



The URL www.dropbox.com is categorized as File Sharing and Storage.
Which action does FortiGate take if a user attempts to access www.dropbox.com?

A. FortiGate blocks the connection as an invalid URL.
B. Based on the URL Filter configuration, FortiGate allows the connection.
C. FortiGate blocks the connection, based on the FortiGuard category-based filter configuration.
D. Based on the Web Content filter configuration, access to www.dropbox.com would be exempted.

Answer: B

NEW QUESTION 7
Refer to the exhibit, which shows the partial output of a real-time OSPF debug.

Real-time OSPF debug output

```
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114 (192.168.37.115 -> 224.0.0.5)
OSPF: ----------------------------------------------------
OSPF: Header
OSPF:   Version 2
OSPF:   Type 1 (Hello)
OSPF:   Packet Len 48
OSPF:   Router ID 0.0.0.112
OSPF:   Area ID 0.0.0.0
OSPF:   Checksum 0x2f85
OSPF:   AuType 0
OSPF: Hello
OSPF:   NetworkMask 255.255.255.0
OSPF:   HelloInterval 10
OSPF:   Options 0x2 (*|-|-|-|-|-|E|-)
OSPF:   RtrPriority 1
OSPF:   RtrDeadInterval 40
OSPF:   DRouter 192.168.37.114
OSPF:   BDRouter 192.168.37.115
OSPF:   # Neighbors 1
OSPF:     Neighbor 0.0.0.111
OSPF: ----------------------------------------------------
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114: Authentication type mismatch
```

Why are the two FortiGate devices unable to form an adjacency?

A. The Hello packet is being sent from an OSPF router with ID 0.0.0.112.
B. The two FortiGate devices attempting adjacency are in area 0.0.0.0.
C. One FortiGate device is configured to require authentication, while the other is not.
D. The passwords on the FortiGate devices do not match.

Answer: C

NEW QUESTION 8
Refer to the exhibit, which contains the output of diagnose vpn tunnel list.

```
# diagnose vpn tunnel list
name=DialUp_0 ver=1 serial=4 10.200.1.1:4500->10.200.3.2:64916 tun_id=10.200.3.2 dst_mtu=1500 dpd-link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/896 options[0380]=rgwy-chg rport-chg frag-rfc  run_state=0 accept_traffic=1 overlay_id=0
parent=DialUp index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=221 txp=0 rxb=35360 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=70
natt: mode=silent draft=32 interval=10 remote_port=64916
proxyid=DialUp proto=0 sa=1 ref=2 serial=3 add-route
  dst: 0:0.0.0.0-255.255.255.255:0
  src: 0:10.0.10.10-10.0.10.10:0
  SA:  ref=3 options=82 type=00 soft=0 mtu=1422 expire=43065/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000079 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43188/43200
  dec: spi=5ed4aafc esp=aes key=16 054852d43abb0e931641b4e8878dd9ce
       ah=sha1 key=20 082eafd018bf7d4d7b65d9c5b7448db5cc01f81d
  enc: spi=69d4231e esp=aes key=16 d5a23d09ab4128d094ac972f5511f9db
       ah=sha1 key=20 54eac30e29ce711d2ceaab9b5e179c20bb83605e
  dec:pkts/bytes=120/10080, enc:pkts/bytes=0/0
```

Which command will capture ESP traffic for the VPN named DialUp_0?

A. diagnose sniffer packet any 'ip proto 50'
B. diagnose sniffer packet any 'host 10.0.10.10'
C. diagnose sniffer packet any 'esp and host 10.200.3.2'
D. diagnose sniffer packet any 'port 4500'

Answer: D

NEW QUESTION 9
An administrator wants to capture encrypted phase 2 traffic between two FotiGate devices using the built-in sniffer.
If the administrator knows that there Is no NAT device located between both FortiGate devices, which command should the administrator run?

A. diagnose sniffer packet any 'udp port 500'
B. diagnose sniffer packet any 'lp proto 50'
C. diagnose sniffer packet any 'udp port 4500'
D. diagnose sniffer packet any 'ah'

Answer: B

NEW QUESTION 10
Exhibit.

```
session info: proto=6 proto_state=01 duration=157 expire=3559 timeout=3600 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=User1 state=log may_dirty authed f00 acct-ext
statistic(bytes/packets/allow_err): org=2137/14/1 reply=1663/12/1 tuples=2
tx speed(Bps/kbps): 1/0 rx speed(Bps/kbps): 1/0
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.1.0.254/10.1.10.1
hook=pre dir=org act=noop 10.1.10.1:34830->35.241.9.150:443(0.0.0.0:0)
hook=post dir=reply act=noop 35.241.9.150:443->10.1.10.1:34830(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14735 auth_info=2 chk_client_info=0 vd=0
serial=0000352e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/anpu_state=0x000100
no_ofld_reason:  npu-flag-off
```

Refer to the exhibit, which shows the output of a session. Which two statements are true? (Choose Two.)

A. The TCP session has been successfully established.
B. The session was initiated from an authenticated user.
C. The session is being inspected using flow inspection.
D. The session is being offloaded.

Answer: AB

NEW QUESTION 10
Which statement about parallel path processing is correct (PPP)?

A. PPP chooses from a group of parallel options lo identity the optimal path tor processing a packet.
B. Only FortiGate hardware configurations affect the path that a packet takes.
C. PPP does not apply to packets that are part of an already established session.
D. Software configuration has no impact on PPP.

Answer: A

Explanation:
Parallel Path Processing (PPP) in FortiOS refers to the system??s ability to evaluate and select among multiple processing paths—often involving dedicated network processors, content processors, or CPU-based workflows—to optimally process packets. The official documentation highlights that the PPP engine dynamically selects which hardware or software path to use for each session based on session characteristics, policy configuration, and traffic type. This dynamic selection results in optimal throughput and resource utilization.
The document specifies that PPP assesses several processing paths in parallel, using decision logic to determine whether a session should be offloaded to specialist hardware (like NP6, CP9, etc.) or stay in the CPU path, ensuring that each packet is handled by the most efficient available method under current load and policy. Hardware and software configurations both influence this outcome, but it is the PPP engine's decision-making that defines the optimal path per session.
[References:, Fortinet FortiGate Handbook: Parallel Path Processing, Fortinet FortiOS Technical Documentation: Packet Flow and Path Selection,]

NEW QUESTION 12
Refer to the exhibit, which shows one way communication of the downstream FortiGate with the upstream FortiGate within a Security Fabric.

```
# diagnose sniffer packet any "tcp port 8013 or udp port 8014" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[tcp port 8013 or udp port 8014]
47.220358 portl in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
48.215338 portl in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
50.218552 portl in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
54.222117 portl in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
```

What three actions must you take to ensure successful communication? (Choose three.)
A. You must authorize the downstream FortiGate on the root FortiGate.
B. FortiGate must not be in NAT mode.
C. Ensure TCP port 8013 is not blocked along the way.
D. You must enable Security Fabric/Fortitelemetry on the receiving interface of the upstream FortiGate.
E. Ensure the port for Neighbor Discovery has been changed.

A.

Answer: ACD

NEW QUESTION 14
Refer to the exhibit, which shows a session entry.

```
session_info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic (bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed (Bps/kbps) : 97/0 rx speed (Bps/kbps) : 97/0
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8 (10.200.1.1:60430)
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

Which statement about this session is true?

A. Return traffic to the initiator is sent to 10.1.0.1.
B. Return traffic to the initiator is sent lo 10.200.1.254.
C. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
D. It is an ICMP session from 10.1.10.1 to 10.200.5.1.

Answer: B

Explanation:
The session output reveals a session with proto=1 (ICMP) and the origin and reply directions show address and NAT translations. Specifically, thehook=post dir=org act=snatshows that source NAT is performed for outgoing packets, where the source 10.1.10.10:40602 is translated to 10.200.5.1:8 (likely ICMP id 8, not a TCP/UDP port). The reply direction,hook=pre dir=reply act=dnat, indicates destination NAT for incoming packets: packets incoming for 10.200.5.1:60430 are destination-NATed to 10.1.10.10:40602. The gateway (gwy) is listed as 10.200.1.254/10.1.0.1, which for outgoing traffic means that return traffic is directed to the gateway (10.200.1.254), per the NAT policy. This is confirmed by the FortiOS Session Table Guide, which explains that the returned ICMP reply will be routed out to this NAT gateway. The session statistics and logical flow (SNAT out, matching DNAT in) reinforce that reply traffic to the initiator traverses via 10.200.1.254.
FortiOS Administration Guide: Session Table, NAT, and Route Interaction
Fortinet Technical Note: Diagnose sys session list, Direction and NAT Analysis

NEW QUESTION 16
Refer to the exhibit, which shows the output of the command get router info bgp neighbors 100.64.2.254 advertised-routes.

```
# get router info bgp neighbors 100.64.2.254 advertised-routes

VRF 0 BGP table version is 3, local router ID is 172.16.1.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network              Next Hop      Metric LocPrf   Weight RouteTag Path

*> 10.20.30.40/24    100.64.2.1           xxx       0        0          100 i <-/->

Total number of prefixes 1
```

What can you conclude from the output?

A. The BGP state of the two BGP participants is OpenConfirm.
B. The router ID of the neighbor is 100.64.2.254.
C. The BGP neighbor is advertising the 10.20.30.40/24 network to the local router.
D. The local router is advertising the 10.20.30.40/24 network to its BGP neighbor.

Answer: D

NEW QUESTION 18
Refer to the exhibit.

```
**** SP Login Dump ****<lasso:Login
xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
LoginDumpVersion="2"><lasso:Request><samlp:AuthnRequest
ID="_EEC718A47FB37B472B205B11153ED409" Version="2.0" IssueInstant="2024-02-
21T00:58:44Z" Destination="https://10.1.10.2/saml-idp/nst/login/"
SignType="0" SignMethod="0" ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://10.1.10.254:1003/remote/saml/login/"><sa
ml:Issuer>https://10.1.10.254:1003/remote/saml/metadata/</saml:Issuer><samlp:
NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
AllowCreate="true"/></samlp:AuthnRequest></lasso:Request><lasso:RemoteProvide
rID>http://10.1.10.2/samlidp/nst/metadata/</lasso:RemoteProviderID><lasso:Msg
Url>https://10.1.10.2/saml-
idp/nst/login/?SAMLRequest=jZJfT8IwFMW%2FytL3OW5sAZtBwhhEEtQF0AdfTN0u0GRr22%2
Fnn29vGWIwUeJLk97eX%2B85p01Q1FXDJ63dqxW8tIDWe68rhbw7GJHWKK4FSuRK1IDcFnw9uVnys
Md4Y7TVha7IGXKZEIhgrNSKeItsRJ5ms%4</lasso:HttpRequestMethod><lasso:RequestID>
_EEC718A47FB37B472B205B11153ED409</lasso:RequestID></lasso:Login>
```

The exhibit shows the output from using the command diagnose debug application samld -1 to diagnose a SAML connection.
Based on this output, what can you conclude?
A. Active Directory is used for authentication.
B. The authentication request is for an SSL VPN connection.
C. The IdP IP address is 10.1.10.254.
D. The IdP IP address is 10.1.10.2.

A.

Answer: D

NEW QUESTION 21
Refer to the exhibit, which contains partial output from an IKE real-time debug.

Debug output

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
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 0:620000:98:                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 the administrator make to the local gateway to resolve the phase 1 negotiation error?

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

Answer: A

NEW QUESTION 23
Refer to the exhibit, which shows a partial output from the get router info routing-table database command.

```
# get router info routing-table database
---omitted---

Routing table for VRF=0
S           0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S           0.0.0.0/0 [10/0] via 100.64.1.254, port1 inactive, [50/0]
---omitted---
```

The administrator wants to configure a default static route for port3 and assign a distance of 50 and a priority of 0.
What will happen to the port1 and port2 default static routes after the port3 default static route is created?

A. The port2 default static route will be injected into the forwarding information base (FIB).
B. The port1 default static route will be injected into the FIB.
C. Neither of the routes shown in the output will be injected into the FIB.
D. Both default static routes shown in the output will be injected into the FIB.

Answer: A

NEW QUESTION 25
Refer to the exhibit, which shows the output of the command get router info ospf neighbor.

```
# get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.0.12          1   Full/DROther    02:14:39    10.10.2.1       wan1
0.0.0.15          1   Full/BDR        04:26:37    10.10.3.2       wan2
0.0.0.18         c1   Full/ -         05:04:36    172.16.1.2      ToHub
```

To what extent does FortiGate operate when looking at its OSPF neighbors? (Choose two.)

A. The local FortiGate has at least one interface that participates in a broadcast network.
B. The local FortiGate has at least one interface that participates in a point-to-point network.
C. The local FortiGate is the DR.
D. Neighbor 0.0.0.18 is the designated router (DR).

Answer: AB

Explanation:
The command on this slide shows a summary of the statuses of all the OSPF neighbors. For each neighbor, it displays the adjacency state and if it is a DR, a BDR, or neither (DROther) Pagina 362 Enterprise_Firewall_7.2_Study. - Point-to-point networks contain only two peers, one at each end of a point-to-point link - Broadcast networks (multi-access) support more than two attached routers. They also support sending messages to multiple recipients (broadcasting). Pagina 365 Enterprise_Firewall_7.2_Study. In any multi-access network there is one DR and one BDR. Pagina 439 Network_Security_Support_Engineer_7.4_Study FULL/- This represents a point-to-point network

NEW QUESTION 30
Exhibit.

```
FGT # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract

Service      : Antispam
Status       : Disable

Service      : Virus Outbreak Prevention
Status       : Disable

Num. of servers : 1
Protocol        : https
Port            : 443
Anycast         : Enable
Default servers : Included

-=- Server List (Mon May  1 03:47:52 2023) -=-

IP                                    Weight    RTT Flags   TZ   FortiGuard-requests  Curr Lost Total Lost           Updated Time
64.26.151.37                              10     45          -5                262432          0        846 Mon May  1 03:47:43 2023
64.26.151.35                              10     46          -5                329072          0       6806 Mon May  1 03:47:43 2023
66.117.56.37                              10     75          -5                 71638          0        275 Mon May  1 03:47:43 2023
65.210.95.240                             20     71          -8                 36875          0         92 Mon May  1 03:47:43 2023
209.22.147.36                             20     103 DI      -8                 34784          0       1070 Mon May  1 03:47:43 2023
208.91.112.194                            20     107 D       -8                 35170          0       1533 Mon May  1 03:47:43 2023
                                                             0                  33728          0        120 Mon May  1 03:47:43 2023
                                                             1                  33797          0        192 Mon May  1 03:47:43 2023
                                                             9                  33754          0        145 Mon May  1 03:47:43 2023
                                                            -5                  26410      26226      26227 Mon May  1 03:47:43 2023
```

Refer to the exhibit, which shows the output of a diagnose command.
What can you conclude about the debug output in this scenario?

A. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.
B. There is a natural correlation between the value in the FortiGuard-requests field and the value in the Weight field.
C. FortiGate used 64.26.151.37 as the initial server to validate its contract.
D. Servers with a negative TZ value are less preferred for rating requests.

Answer: C

Explanation:
The exhibit displays the output from the diagnose debug rating command on a FortiGate device. This command is used to display information about FortiGuard Web Filtering or other security-related queries performed by FortiGate to FortiGuard servers. Official Fortinet documentation outlines the meaning of each field in the server list. The FortiGate maintains a list of available FortiGuard servers, selecting the optimal server based on factors such as weight, round-trip time (RTT), and regional settings.
The very first entry in the server list after "Server List" is the server FortiGate initially uses, prioritized by factors such as proximity and RTT. Here, 64.26.151.37 is listed first, and the FortiGuard-requests value confirms that this server handled the highest number of requests.
The IPs, weights, and lost/failed counters are monitored for server performance and selection over time. FortiGate's default operational logic is to try the first entry for contract validation and use the next in the list if the first is unavailable or has high latency or packet loss.
There is no direct correlation between the Weight and the number of FortiGuard-requests. The servers with higher or lower weights may still handle different request volumes based on availability and performance.
The TZ (time zone) value's sign (positive or negative) does not affect server preference; it is informational, showing the server's location relative to UTC, not a rating metric.
DNS query results for FortiGuard servers are not shown here, and the provided servers are not returned in DNS query order.
This command and interpretation are detailed in the FortiOS Administration Guide??s section describing FortiGuard server selection and contract validation processes.
[References:, , FortiOS Administration Guide: FortiGuard Service Connectivity and Debugging, , Official Technical Notes on diagnose debug rating output structure]

NEW QUESTION 32
Refer to the exhibit, which shows the partial output of command diagnose debug rating.

```
-=- Server List (Mon May  6 03:47:52 2024) -=-
IP                                  Weight    RTT Flags   TZ   FortiGuard-requests  Curr Lost Total Lost           Updated Time
64.26.151.37                            10     45          -5                262432         0        846 Mon May  6 03:47:43 2024
64.26.151.35                            10     46          -5                329072         0       6806 Mon May  6 03:47:43 2024
66.117.56.37                            10     75          -5                 71638         0        275 Mon May  6 03:47:43 2024
65.210.95.240                           20     71          -8                 36875         0         92 Mon May  6 03:47:43 2024
209.22.147.36                           20    103 DI       -8                 34784         0       1070 Mon May  6 03:47:43 2024
208.91.112.194                          20    107 D        -8                 35170         0       1533 Mon May  6 03:47:43 2024
96.45.33.65                             60    144          0                  33720         0        120 Mon May  6 03:47:43 2024
80.85.69.41                             71    226          1                  33797         0        192 Mon May  6 03:47:43 2024
62.209.40.74                           150     97          9                  33754         0        145 Mon May  6 03:47:43 2024
121.111.236.179                         45     44  F       -5                 26410     26226      26227 Mon May  6 03:47:43 2024
```

A. 66.117.56.37
B. 208.91.112.194
C. 209.22.147.36
D. 64.26.151.37

Answer: D

NEW QUESTION 36
Refer to the exhibit, which shows the omitted output of a session table entry.

```
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=16/16, ipid=64/88, vlan=0x0000/0x0000
vlifid=64/88, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
```

Which two statements are true? (Choose two.)

A. The traffic has been tagged for VLAN 0000.
B. NP7 is handling offloading of this session.
C. The traffic matches Policy ID 1.
D. The session has been offloaded.

Answer: BD

NEW QUESTION 37
Refer to the exhibit, which shows the partial output of FortiOS kernel slabs.

```
...
packet_de_duplication     0     0    128    30    1 : tunables  252  126    0 : slabdata     0     0     0
ip6_nat_record            0     0    128    30    1 : tunables  252  126    0 : slabdata     0     0     0
tcp6_session              0     0   1536     5    2 : tunables   60   30    0 : slabdata     0     0     0
ip6_session               0     0   1300     3    1 : tunables   60   30    0 : slabdata     0     0     0
ip_nat_record             0     0     64    59    1 : tunables  252  126    0 : slabdata     0     0     0
sctp_session              0     0   1600     5    2 : tunables   60   30    0 : slabdata     0     0     0
tcp_session               3     5   1500     5    2 : tunables   60   30    0 : slabdata     1     1     0
ip_session                1     3   1200     3    1 : tunables   60   30    0 : slabdata     1     1     0
...
```

Which statement is true?

A. The total slab size of the sctp_session slab is 0 kB and is associated with the user space.
B. The total slab size of the ip_session slab is 3600 kB and is associated with the user space.
C. The total slab size of the ip6_session slab is 1300 kB and is associated with the kernel.
D. The total slab size of the tcp_session slab is 7500 kB and is associated with the kernel.

Answer: D

NEW QUESTION 39
Which two statements about an auxiliary session ate true? (Choose two.)

A. With the auxiliary session selling disabled, only auxiliary sessions are offloaded.
B. With the auxiliary session setting enable
C. ECMP traffic is accelerated to the NP6 processor.
D. With the auxiliary session setting enable
E. lwo sessions are created in case of routing change.
F. With the auxiliary session setting disabled, for each traffic pat
G. FortiGate uses the same auxiliary session.

Answer: BC

NEW QUESTION 44
Refer to the exhibit, which shows the output o! the BGP database.

```
router info bgp network
0 BGP table version is 3, local router ID is 1.1.1.1
tus codes: s suppressed, d damped, h history, * valid, > best, i - internal,
           S Stale
gin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric     LocPrf Weight RouteTag Path
0.0.0.0/0        100.64.2.254    0                100      0         0 ? <-/->
                 100.64.2.1                            32768         0 ? <-/1>
1.2.2.1/32       100.64.2.1                            32768         0 ? <-/1>
8.8.8.8/32       100.64.2.254    0                100      0         0 ? <-/1>
10.20.30.0/24    172.16.54.115   0                100      0         0 i <-/1>

l number of prefixes 4
```

Which two statements are correct? (Choose two.)

A. The advertised prefix of 10.20.30.0'24 was configured using the network command.
B. The first four prefixes are being advertised using a legacy route advertisement.
C. The advertised prefix of 10.20.30.0'24 is being advertised through the redistribution of another routing protocol.
D. The output shows all prefixes advertised by all neighbors as well as the local router.

Answer: AD

NEW QUESTION 47
Refer to the exhibit, which shows the output of get router info ospf neighbor.

```
Spoke1 # get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address       Interface
0.0.0.1           1   Full/DR         00:00:39    10.10.2.1     wan1
0.0.0.3           1   Full/DROther    00:00:37    10.10.3.2     wan2
0.0.0.10          c1  Full/ -         00:00:36    172.16.1.2    ToHub
```

What can you conclude from the command output?

A. The network type connecting the local Fortigate and OSPF neighbor 0.0.0.10 is point-to- point.
B. All neighbors are in area 0.0.0.0.
C. The local FortiGate is the BDR.
D. The local FortiGate is not a DROther.

Answer: A

NEW QUESTION 51
Refer to the exhibit, which shows partial outputs from two routing debug commands.

```
FortiGate # get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 qwy=100.64.1.254 dev=3 (port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.2.254 dev=6 (port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9 (port3)

FortiGate # get router info routing-table all

Routing table for VRF=0
S*          0.0.0.0/0 [10/0] via 100.64.1.254, port1
                             [10/0] via 100.64.2.254, port2, [10/0]
C           10.1.0.0/24 is directly connected, port3
S           10.1.10.0/24 [10/0] via 10.1.0.1, port3
C           100.64.1.0/24 is directly connected, port1
C           100.64.2.0/24 is directly connected, port2
```

Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

A. Set snat-route-change to enable.
B. Set the priority of the static default route using port2 to 1.
C. Set preserve-session-route to enable.
D. Set the priority of the static default route using port1 to 10.

Answer: D

NEW QUESTION 52
Refer to the exhibit, which shows a partial output of a real-time LDAP debug.

```
# diagnose debug application fnbamd -1
# diagnose debug enable
fnbamd_fsm.c[1274] handle_req-Rcvd auth req 8781845 for jsmith in Lab opt=27 prot=0
fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
fnbamd_ldap.c[232] start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith
fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 8781845
fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

What two conclusions can you draw from the output? (Choose two.)

A. The user was found in the LDAP tree, whose root is TAC.ottawa.fortinet.com.
B. FortiOS performs a bind to the LDAP server using the user's credentials.
C. FortiOS collects the user group information.
D. FortiOS is performing the second step (Search Request) in the LDAP authentication process.

Answer: AD

NEW QUESTION 53
Exhibit.

```
# diagnose automation test HAFailOver
automation test failed(1). stitch:HAFailOver
```

Refer to the exhibit, which shows the output of diagnose automation test. What can you observe from the output? (Choose two.)

A. The automation stitch test is not being logged.
B. The automation stitch test failed but the HA failover was successful.
C. An HA failover occurred.
D. The test was unsuccessful.

Answer: AD

NEW QUESTION 58
Exhibit.

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500,ifindex=7.
ike 0: IKEv1 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 1em=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response.
ike 0: Remotesite:3: VID DD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated                FC77570100
ike 0: Remotesite:3: VID FORTIGATE 8299031757A3608
ike 0: Remotesite:3: peer is Fortifate/Fartios, (v2C6A621DE00000000
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EB0 bo)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: received peer identifier FQDNCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: negotiation result             'remote"
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/
ike 0: Remotesite:3:               type=OAKLEY _ENCnone
ike 0: Remotesite:3:               type=OAKLEY HASHRYPT _ALG, val=AES CBC, key-len=128
ike 0: Remotesite:3:           type=AUTH METHOD, vaALG, val=SHA.
ike 0: Remotesite:3:           type=OAKLEY _GROUP,l=PRESHARED KEY.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400      val=MODP1024.
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key 16:39915120ED73E520787C801DE3678916
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 A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A07809026CA8B2
ike 0: Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000O5C64D5CBA90B873F150CB8B5CCZA
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/06689c022d4df682
```

Refer to the exhibit, which contains partial output from an IKE real-time debug. Which two statements about this debug output are correct? (Choose two.)

A. Perfect Forward Secrecy (PFS) is enabled in the configuration.
B. The local gateway IP address is 10.0.0.1.
C. It shows a phase 2 negotiation.
D. The initiator provided remote as its IPsec peer ID.

Answer: CD

NEW QUESTION 63
.....

Relate Links

100% Pass Your FCSS_NST_SE-7.6 Exam with Exambible Prep Materials

https://www.exambible.com/FCSS_NST_SE-7.6-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/