Fortinet

Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

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
Refer to the exhibit, which contains the output of a BGP debug command.

```
FGT # get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS  MsgRcvd MsgSent  TblVer InQ OutQ  Up/Down  State/PfxRcd
10.125.0.60     4 65060  1698    1756     103     0    0   03:02:49        1
10.127.0.75     4 65075  2206    2250     102     0    0   02:45:55        1
100.64.3.1      4 65501  101     115       0      0    0   never       Active

Total number of neighbors 3
```

Which statement about the exhibit is true?

A. The local router has received a total of three BGP prefixes from all peers.
B. The local router has not established a TCP session with 100.64.3.1.
C. Since the counters were last reset, the 10.200.3.1 peer has never been down.
D. The local router BGP state is OpenConfirm with the 10.127.0.75 peer.

Answer: B

NEW QUESTION 2
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: IKEv1 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 16:39915120ED73E520787C801DE3678916
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 A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A078E09026CA8B2
ike 0:Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000005C64D5CBA90B873F150CB8B5CC2A
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 initiator provided remote as its IPsec peer ID.
B. It shows a phase 2 negotiation.
C. Perfect Forward Secrecy (PFS) is enabled in the configuration.
D. The local gateway IP address is 10.0.0.1.

Answer: AD

Explanation:
A because : received peer identifier FQDN 'remote' D because : ike 0: comes 10.0.0.2:500 -> 10.0.0.1:500

NEW QUESTION 3
Which ADVPN configuration must be configured using a script on FortiManager, when using VPN Manager to manage FortiGate VPN tunnels?

A. Set protected network to all
B. Enable AD-VPN in IPsec phase 1
C. Configure IP addresses on IPsec virtual interfaces
D. Disable add-route on hub

Answer: B

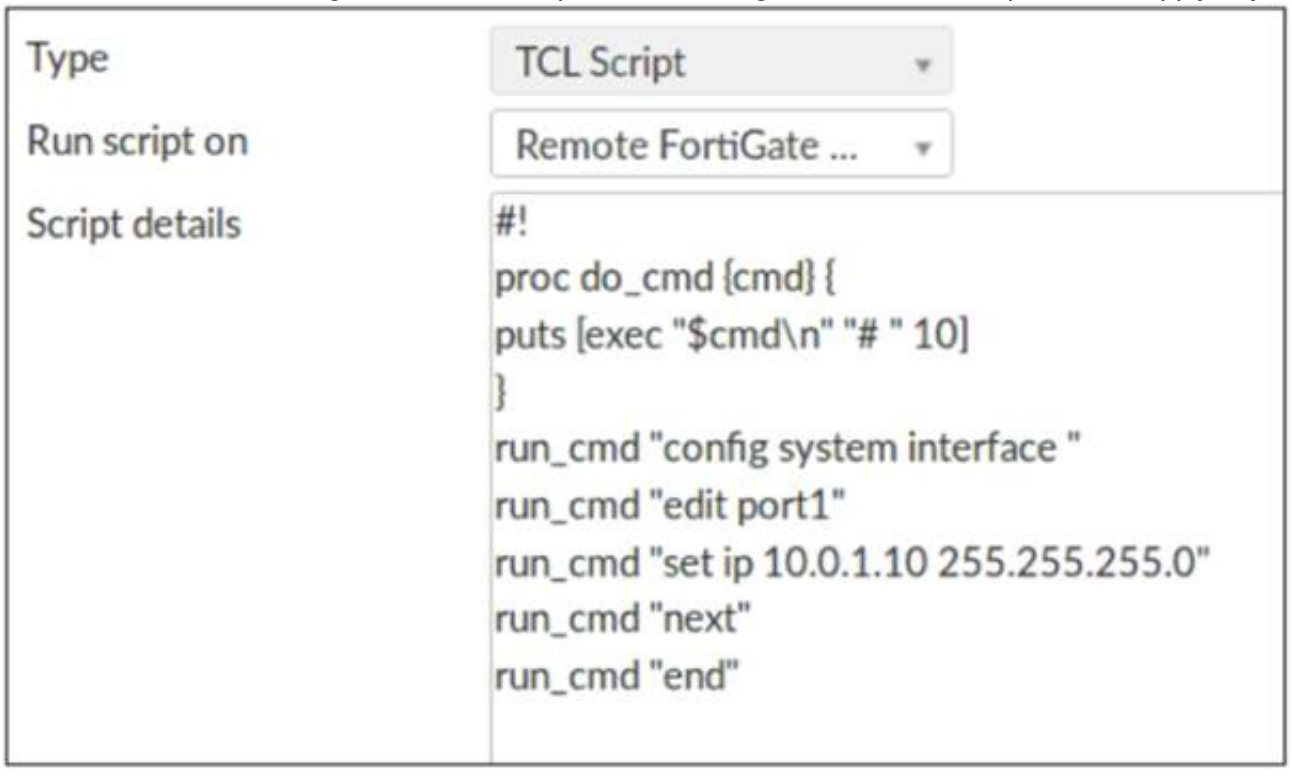
NEW QUESTION 4
An administrator has decreased all the TCP session timers to optimize the FortiGate memory usage. However, after the changes, one network application started to have problems. During the troubleshooting, the administrator noticed that the FortiGate deletes the sessions after the clients send the SYN packets, and before the arrival of the SYN/ACKs. When the SYN/ACK packets arrive to the FortiGate, the unit has already deleted the respective sessions. Which TCP session timer must be increased to fix this problem?

A. TCP half open.
B. TCP half close.
C. TCP time wait.
D. TCP session time to live.

Answer: A

Explanation:
http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=CLI_get_Commands.58.25.html
The tcp-halfopen-timer controls for how long, after a SYN packet, a session without SYN/ACKremains in the table.
The tcp-halfclose-timer controls for how long, after a FIN packet, a session without FIN/ACKremains in the table.
The tcp-timewait-timer controls for how long, after a FIN/ACK packet, a session remains in thetable. A closed session remains in the session table for a few seconds more to allow any out-of-sequence packet.

NEW QUESTION 5
Refer to the exhibit, which contains a TCL script configuration on FortiManager.
An administrator has configured the TCL script on FortiManager, but the TCL script failed to apply any changes to the managed device after being run.



Why did the TCL script fail to make any changes to the managed device?

A. The TCL command run_cmd has not been created.
B. The TCL script must start with tinclude <>.
C. Incomplete commands are ignored in TCL scripts.
D. Changes to an interface configuration can be made only by a CLI script.

Answer: A

Explanation:
https://docs.fortinet.com/document/fortimanager/7.2.2/administration-guide/914165/tcl-scripts

NEW QUESTION 6
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0: comes 10.0.0.2:500-> 10.0.0.1:500, ifindex-7...
ike 0: IKEV1 exchange-Aggressive id-baf47d0988e9237f/2f405ef3952f6fda len 430
ike 0: in
BAF47D0988E9237F2F405EF3952F6FDA01100400000000000000001AE0400003C000000010000000100000030010100
ike 0: RemoteSite:4: initiator: aggressive mode get 1st response
ike 0: RemoteSite:4: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0: RemoteSite:4: VID DPD AFCAD71368A1F1c96B8696FC77570100
ike 0: RemoteSite:4: VID FORTIGATE 8299031757A36082C6A621DE000502D7
ike 0: RemoteSite:4: peer is FortiGate/FortiOS (v6 b932)
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: RemoteSite:4: received peer identifier FQDN 'remote'
ike 0: RemoteSite:4: negotiation result
ike 0: RemoteSite:4: proposal id = 1:
ike 0: RemoteSite:4:    protocol id - ISAKMP:
ike 0: RemoteSite:4:         trans_id - KEY_IKE.
ike 0: RemoteSite:4:         encapsulation - IKE/none
ike 0: RemoteSite:4:              type=OAKLEY_ENCRYPT_ALG,  val=AES_CBC, key-len=128
ike 0: RemoteSite:4:              type=OAKLEY_HASH_ALG, val-SHA
ike 0: RemoteSite:4:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: RemoteSite:4:              type=OAKLEY_GROUP, val=MODP1024.
ike 0: RemoteSite:4: ISAKMP SA lifetime=86400
ike 0: RemoteSite:4: ISAKMP SA baf47d0988e9237f/2f405ef3952f6fda key
16:B25B6C9384D8BDB24E3DA3DC90CF5E73
ike 0: RemoteSite:4: PSK authentication succeeded
ike 0: RemoteSite:4: authentication OK
ike 0: RemoteSite:4: add INITIAL-CONTACT
ike 0: RemoteSite:4: enc
BAF47D0988E9237F2F405EF3952F6FDA08100401000000000000000801400001B1F2E48BFD8E9D603F
ike 0: RemoteSite:4: out
BAF47D0988E9237F2F405EF3952F6FDA08100401000000000000008c2E3FC9BA061816A396F009A12
ike 0: RemoteSite:4: sent IKE msg (agg_12send) : 10.0.0.1:500 ->10.0.0.2:500, len-140, id-
baf47d0988e9237f/2
ike 0: RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda
```

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

A. The remote gateway IP address is 10.0.0.1.
B. It shows a phase 1 negotiation.
C. The negotiation is using AES128 encryption with CBC hash.
D. The initiator has provided remote as its IPsec peer ID.

Answer: BD

NEW QUESTION 7
Refer to the exhibit, which contains a screenshot of some phase 1 settings.

The VPN is not up. To diagnose the issue, the administrator enters the following CLI commands to an SSH session on FortiGate: diagnose vpn ike log-filter dst-addr4 10.0.10.1 diagnose debug application ike -1
However, the IKE real-time debug does not show any output. Why?

A. The administrator must also run the command diagnose debug enable.
B. The administrator must enable the following real-time debug: diagnose debug application ipsec -1.
C. The log-filter setting is incorrec
D. The VPN traffic does not match this filter.
E. The debug shows only error message
F. If there is no output, then the phase 1 and phase 2 configurations match.

Answer: A

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-IPSec-VPN-Diagnostics-Possible-reasons/ta-p/1920

NEW QUESTION 8
Which two statements about the Security Fabric are true? (Choose two.)

A. Only the root FortiGate collects network information and forwards it to FortiAnalyzer.
B. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.
C. All FortiGate devices in the Security Fabric must have bidirectional FortiTelemetry connectivity.
D. Branch FortiGate devices must be configured first.

Answer: BC

NEW QUESTION 9
Refer to the exhibit, which contains the partial output of a diagnose command.

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN ver=1 serial=1 10.200.5.1:0->10.200.4.1:0
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
     src: 0:10.1.2.0/255.255.255.0:0
     dst: 0:10.1.1.0/255.255.255.0:0
     SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=2048 seqno=1 esn=0
replaywin_lastseq=00000000
     life: type=01 bytes=0/0 timeout=43177/43200
     dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
            ah=sha1 key=20 c68091d68753578785de6a7a6b276b506c527efe
     enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
           ah=sha1 key=20 889f7529887c215c25950be2ba83e6fe1a5367be
     dec: pkts/bytes=0/0, enc:pkts/bytes=0/0
```

Based on the output, which two statements are correct? (Choose two.)

A. Anti-replay is enabled
B. The remote gateway IP is 10.200.4.1.
C. DPD is disabled.
D. Quick mode selectors are disabled.

Answer: AB

NEW QUESTION 10
Refer to the exhibit, which contains partial output from an IKE real-time debug.

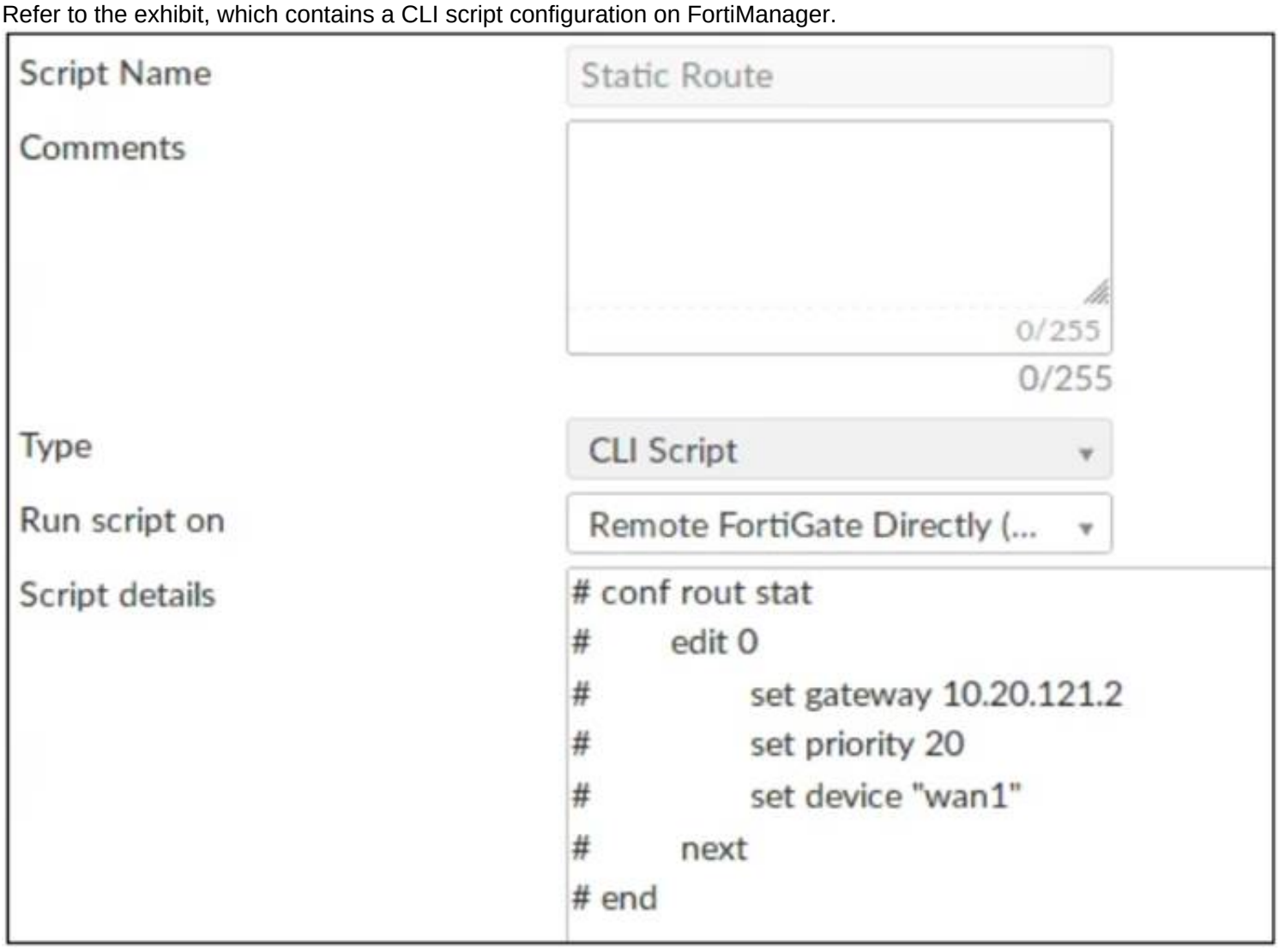
```
ike 0:H2S_0_1:1249: notify msg received: SHORTCUT-QUERY
ike 0:H2S_0_1:  recv shortcut-query 12594932268010586978 4384dd592d62cd52/0000000000000000 100.64.3.1
10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 32 nat 0 ver 1 mode 0
ike 0:H2S_0: iif 13 10.1.1.254->10.1.2.254 route lookup oif 13
ike 0:H2S_0_0: forward shortcut-query 12594932268010586978 4384dd592d62cd52/0000000000000000
100.64.3.1 10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 31 ver 1 mode 0, ext-ma
ike 0:H2S_0_0:1248: sent IKE msg (SHORTCUT-QUERY): 100.64.1.1:500->100.64.5.1:500, len=236,
id=e2beec89f13c7074/06a73dfb3a5d3b54:340a645c
ike 0: comes 100.64.5.1:500->100.64.1.1:500, ifindex=3. . .
ike 0: IKEv1 exchange=Informational id=e2beec89f13c7074/06a73dfb3a5d3b5d:26254ae9 len=236
ike 0:H2S_0_0:1248: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0: recv shortcut-reply 12594932268010586978 4384dd592d62cd52/89bf040f5f7408c0 100.64.5.1
to 10.1.1.254 psk 64 ppk 0 ver 1 mode 0 ext-mapping 100.64.3.1:500
ike 0:H2S_0: iif 13.10.1.2.254->10.1.1.254 route lookup oif 13
ike 0:H2S 0 1: forward shortcut-reply 12594932268010586978 4384dd592d62cd52/89bf040f5f7408c0
100.64.5.1 to 10.1.1.254 psk 64 ppk 0 ttl 31 ver 1 mode 0 ext-mapping 100.
```

Based on the debug output, which phase 1 setting is enabled in the configuration of this VPN?

A. auto-discovery-shortcut
B. auto-discovery-forwarder
C. auto-discovery-sender
D. auto-discovery-receiver

Answer: D

NEW QUESTION 10
Refer to the exhibit, which contains a CLI script configuration on FortiManager.



An administrator configured the CLI script on FortiManager, but the script failed to apply any changes to the managed device after being executed.
What are two reasons why the script did not make any changes to the managed device? (Choose two.)

A. Static routes can be added using only TCL scripts.
B. The commands that start with the # sign did not run.
C. CLI scripts must start with #!.
D. Incomplete commands can cause CLI scripts to fail.

Answer: BD

Explanation:
ref CLI scripts do not include Tool Command Language (Tcl) commands, and the first line of the script is not “#!” as it is for Tcl scripts.
https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1000_Device%20Manager/2400_Sc

NEW QUESTION 12
Examine the partial output from two web filter debug commands; then answer the question below:

```
# diagnose test application urlfilter 3
Domain | IP    DB Ver   T URL
34000000| 34000000   16.40224 P Bhttp://www.fgt99.com/
# get webfilter categories
g07 General Interest - Business:
   34 Finance and Banking
   37 Search Engines and Portals
   43 General Organizations
   49 Business
   50 Information and Computer Security
   51 Government and Legal Organizations
   52 Information Technology
```

Based on the above outputs, which is the FortiGuard web filter category for the web site www.fgt99.com?

A. Finance and banking
B. General organization.
C. Business.
D. Information technology.

Answer: C

NEW QUESTION 15
An LDAP user cannot authenticate against a FortiGate device. Examine the real time debug output shown in the exhibit when the user attempted the authentication; then answer the question below.

```
#   debug application fnbamd -1
#   diagnose debug enable
#   diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd auth req 5 for student in WindowsLDAP opt=27 prot=0
fnbamd_fsm.c[336] __compose_group_list_from_req-Group 'WindowsLDAP'
fnbamd_pop3.c[573] fnbamd_pop3_start-student
fnbamd_cfg.c[932] __fnbamd_cfg_get_ldap_list_by_server-Loading LDAP server
'WindowsLDAP'
fnbamd_ldap.c[992] resolve_ldap_FQDN-Resolved address 10.0.1.10, result 10.0.1.10
fnbamd_fsm.c[428] create_auth_session-Total 1 server(s) to try
fnbamd_ldap.c[437] start_search_dn-base:'cn=user,dc=trainingAD,dc=training,dc=lab'
filter:cn=student
fnbamd_ldap.c[1730] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[2407] auth_ldap_result-Continue pending for req 5
fnbamd_ldap.c[480] get_all_dn-Found no DN
fnbamd_ldap.c[503] start_next_dn_bind-No more DN left
fnbamd_ldap.c[2028] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2188] fnbamd_auth_poll_ldap-Result for ldap svr 10.0.1.10 is denied
fnbamd_comm.c[169] fnbamd_comm_send_result-Sending result 1 for req 5
fnbamd_fsm.c[568] destroy_auth_session-delete session 5
authenticate 'student' against 'WindowsLDAP' failed!
```

Based on the output in the exhibit, what can cause this authentication problem?

A. User student is not found in the LDAP server.
B. User student is using a wrong password.
C. The FortiGate has been configured with the wrong password for the LDAP administrator.
D. The FortiGate has been configured with the wrong authentication schema.

Answer: A

NEW QUESTION 19
Refer to the exhibit, which contains the output of diagnose sys session list.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 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
state=may_dirty synced none app_ntf
statistic(bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary unit is zero (0), which statement about the output is true?

A. This session cannot be synced with the slave unit.
B. The inspection of this session has been offloaded to the slave unit.
C. The master unit is processing this traffic.
D. This session is for HA heartbeat traffic.

Answer: C

NEW QUESTION 24
Which of the following statements are true regarding the SIP session helper and the SIP application layer gateway (ALG)? (Choose three.)

A. SIP session helper runs in the kernel; SIP ALG runs as a user space process.
B. SIP ALG supports SIP HA failover; SIP helper does not.
C. SIP ALG supports SIP over IPv6; SIP helper does not.
D. SIP ALG can create expected sessions for media traffic; SIP helper does not.
E. SIP helper supports SIP over TCP and UDP; SIP ALG supports only SIP over UDP.

Answer: BCD

NEW QUESTION 28
Examine the output of the 'diagnose debug rating' command shown in the exhibit; then answer the question below.

```
# diagnose debug rating
Locale        : english
License       : Contract
Expiration    : Wed Mar 27 17:00:00 20xx
-=- Server List (Mon Apr 16 15:32:55 20xx) -=-
IP                Weight   RTT   Flags   TZ   Packets   Curr Lost   Total Los
69.195.205.101    10       45             -5   262432    0           846
69.195.205.102    10       46             -5   329072    0           6806
209.222.147.43    10       75             -5   71638     0           275
96.45.33.65       20       71             -8   36875     0           92
208.91.112.196    20       103    DI      -8   34784     0           1070
208.91.112.198    20       107    D       -8   35170     0           1533
80.85.69.41       60       144             0   33728     0           120
62.209.40.73      71       226             1   33797     0           192
121.111.236.180   150      197             9   33754     0           145
69.195.205.103    45       44     F       -5   26410     26226       26227
```

Which statement are true regarding the output in the exhibit? (Choose two.)

A. There are three FortiGuard servers that are not responding to the queries sent by the FortiGate.
B. The TZ value represents the delta between each FortiGuard server's time zone and the FortiGate's time zone.
C. FortiGate will send the FortiGuard queries to the server with highest weight.
D. A server's round trip delay (RTT) is not used to calculate its weight.

Answer: BC

NEW QUESTION 29
A FortiGate has two default routes:

```
config router static
   edit 1
     set gateway 10.200.1.254
     set priority 5
     set device "port1"
   next
   edit2
     set gateway 10.200.2.254
     set priority 10
     set device "port2"
   next
end
```

All Internet traffic is currently using port1. The exhibit shows partial information for one sample session of Internet traffic from an internal user:

```
# diagnose sys session list
Session info: proto=6 proto_state=01 duration =17 expire=7 timeout=3600
flags= 00000000 sockflag=00000000 sockport=0 av idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic (bytes/packets/allow_err): org=575/7/1 reply=23367/19/1 tuples=2
origin->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)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What would happen with the traffic matching the above session if the priority on the first default route (IDd1) were changed from 5 to 20?

A. The session would be deleted, and the client would need to start a new session.
B. The session would remain in the session table, and its traffic would start to egress from port2.
C. The session would remain in the session table, but its traffic would now egress from both port1 and port2.
D. The session would remain in the session table, and its traffic would still egress from port1.

Answer: D

NEW QUESTION 30
Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

A. Only the DR receives link state information from non-DR routers.
B. Non-DR and non-BDR routers form full adjacencies to DR only.
C. Non-DR and non-BDR routers send link state updates and acknowledgements to 224.0.0.6.
D. FortiGate first checks the OSPF ID to elect a DR.

Answer: C

Explanation:
Some special IP multicast addresses are reserved for OSPF: 224.0.0.5: All OSPF routers must be able to transmit and listen to this address. 224.0.0.6: All DR and BDR routers must be able to transmit and listen to this address. https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

NEW QUESTION 32
Refer to the exhibit, which contains the debug output of diagnose dvm device list.

```
FMG-VM64# diagnose dvm device list
There are currently 1 devices/vdoms managed:
TYPE    OID    SN      HA       IP          NAME          ADOM       IPS  FIRMWARE
fmg/    217    FGVM01… -    10.200.1.1 Local-FortiGate  My_ADOM 15.0.0831 6.0 MR4 (1579)
faz enabled                                                          (regular)
     |-  STATUS: db: modified; conf: in sync; cond: pending; dm: retrieved;  conn: up

     |- vdom: [3] root flags:0 adom:My_ADOM pkg: [imported] Local-FortiGate_root
```

Which two statements about the output shown in the exhibit are correct? (Choose two.)

A. ADOMs are disabled on the FortiManager
B. The FortiGate configuration is in sync with latest running revision history.
C. There are pending device-level changes yet to be installed on Local-FortiGate.
D. The policy package has been modified for Local-FortiGate.

Answer: BC

NEW QUESTION 35
Refer to the exhibit, which shows the output of a web filtering diagnose command.

```
# diagnose webfilter fortiguard statistics list

Rating Statistics:
==================
DNS failures                    :        273
DNS lookups                     :        280
Data send failures              :          0
Data read failures              :          0
Wrong package type              :          0
Hash table miss                 :          0
Unknown server                  :          0
Incorrect CRC                   :          0
Proxy request failures          :          0
Request timeout                 :          1
Total requests                  :       2409
Requests to FortiGuard servers  :       1182
Server errored responses        :          0
Relayed rating                  :          0
Invalid profile                 :          0

Allowed                         :       1021
Blocked                         :       3909
Logged                          :       3927
Blocked Errors                  :        565
Allowed Errors                  :          0
Monitors                        :          0
Authenticates                   :          0
Warnings:                       :         18
Ovrd request timeout            :          0
Ovrd send failures              :          0
Ovrd read failures              :          0
Ovrd errored responses          :          0
...
```

```
# diagnose webfilter fortiguard statistics list
...

Cache Statistics:
=================
Maximum memory                  :          0
Memory usage                    :          0

Nodes                           :          0
  Leaves                        :          0
  Prefix nodes                  :          0
  Exact nodes                   :          0

Requests                        :          0
Misses                          :          0
Hits                            :          0
  Prefix hits                   :          0
  Exact hits                    :          0

No cache directives             :          0
Add after prefix                :          0
Invalid DB put                  :          0
DB updates                      :          0

Percent full                    :         0%
  Branches                      :         0%
  Leaves                        :         0%
    Prefix nodes                :         0%
    Exact nodes                 :         0%

Miss rate                       :         0%
Hit rate                        :         0%
  Prefix hits                   :         0%
  Exact hits                    :         0%
```

Which configuration change would result in non-zero results in the cache statistics section?

A. set server-type rating under config system central-management
B. set webfilter-cache enable under config system fortiguard
C. set webfilter-force-off disable under config system fortiguard
D. set ngfw-mode policy-based under config system settings

Answer: B

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 362

NEW QUESTION 38
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:c49e59846861b0f6/0000000000000000:278: responder: main mode get 1st message…
ike 0:c49e59846861b0f6/0000000000000000:278: incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 0:
ike 0:c49e59846861b0f6/0000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:     trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:     encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: my proposal, gw VPN:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 1:
ike 0:c49e59846861b0f6/0000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:     trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:     encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=256
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:c49e59846861b0f6/0000000000000000:278:
proposal chosen
...
```

Why didn’t the tunnel come up?

A. The pre-shared keys do not match.
B. The remote gateway’s phase 2 configuration does not match the local gateway’s phase 2 configuration.
C. The remote gateway’s phase 1 configuration does not match the local gateway’s phase 1 configuration.
D. The remote gateway is using aggressive mode and the local gateway is configured to use man mode.

Answer: C

NEW QUESTION 40
Refer to the exhibit, which shows a partial routing table.

```
FGT # get router info routing-table all
...
Routing table for VRF=7
C       10.73.9.0/24 is directly connected, port2

Routing table for VRF=12
C       10.1.0.0/24 is directly connected, port3
S       10.10.4.0/24 [10/0] via 10.1.0.100, port3
C       10.64.1.0/24 is directly connected, port1

Routing table for VRF=21
S       10.1.0.0/24 [10/0] via 10.72.3.254, port4
C       10.72.3.0/24 is directly connected, port4
S       192.168.2.0/24 [10/0] via 10.72.3.254, port4
...
```

Assuming all the appropriate firewall policies are configured, what two changes would an administrator need to make if they wanted to send traffic from a client directly connected to port3, to a server directly connected to port4? (Choose two.)

A. Configure route leaking between VRF 12 and VRF 21.
B. Disable auto-asic-offload as this is not supported between VRF instances.
C. Configure RIPv2 to exchange route information between the VRF instances.
D. Configure route leaking between port3 and port4.
E. Enable SNAT on the relevant firewall policies to prevent RPF check drops.

Answer: AE

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 148, 159

NEW QUESTION 41
Examine the output of the 'get router info bgp summary' command shown in the exhibit; then answer the question below.

```
Student# get router info bgp summary
BGP router indentifier 10.200.1.1, local AS number 65500
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor  V     AS    MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.200.3.1 4  65501       92      112       0    0     0     never    Connect

Total number of neighbors 1
```

Which statement can explain why the state of the remote BGP peer 10.200.3.1 is Connect?

A. The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.
B. The TCP session for the BGP connection to 10.200.3.1 is down.
C. The local peer has received the BGP prefixed from the remote peer.
D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Answer: B

Explanation:
http://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=4

NEW QUESTION 46
Refer to the exhibit, which shows a partial routing table.

```
FGT # get router info routing-table all
...
Routing table for VRF=7
C       10.73.9.0/24 is directly connected, port2

Routing table for VRF=12
C       10.1.0.0/24 is directly connected, port3
S       10.10.4.0/24 [10/0] via 10.1.0.100, port3
C       10.64.1.0/24 is directly connected, port1

Routing table for VRF=21
S       10.1.0.0/24 [10/0] via 10.72.3.254, port4
C       10.72.3.0/24 is directly connected, port4
```

Assuming all the appropriate firewall policies are configured, which two pings will FortiGate route? (Choose two.)

A. Source IP address: 10.1.0.10. Destination IP address: 10.64.1.52
B. Source IPaddress: 10.72.3.52. Destination IP address: 10.1.0.254
C. Source IPaddress: 10.10.4.24, Destination IPaddress: 10.72.3.20
D. Source IPaddress: 10.73.9.10, Destination IPaddress: 10.72.3.15

Answer: AB

NEW QUESTION 51
Which action will FortiGate take when using the default settings for SSL certificate inspection, where the server name indication (SNI) does not match either the common name (CN) or any of the subject altemative names (SAN) in the server certificate?

A. FortiGate uses the CN information from the Subject field in the server certificate.
B. FortiGate uses the first entry listed in the SAN field in the server certificate.
C. FortiGate uses the SNI from the user's web browser.
D. FortiGate closes the connection because this represents an invalid SSL/TLS configuration.

Answer: A

Explanation:
#Config firewall ssl-ssh-profile
edit <profile_name> config https
set sni-server-cert-check [enable* | strict | disable]
Enable: If the SNI does NOT match the CN or SAN fields in the returned server's certificate, FG uses the CN field instead of the SNI to obtain the FQDN.
Strict: If the SNI does NOT match the CN or SAN fields in the returned server's certificate, FG closes the connection.
Disable: FG does not check the SNI.

NEW QUESTION 53
Examine the output of the 'get router info bgp summary' command shown in the exhibit; then answer the question below.

```
# get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.125.0.60	4	65060	1698	1756	103	0	0	03:02:49	1
10.127.0.75	4	65075	2206	2250	102	0	0	02:45:55	1
10.200.3.1	4	65501	101	115	0	0	0	never	Active

```
Total number of neighbors 3
```

Which statements are true regarding the output in the exhibit? (Choose two.)

A. BGP state of the peer 10.125.0.60 is Established.
B. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.
C. Local BGP peer has not received an OpenConfirm from 10.200.3.1.
D. The local BGP peer has received a total of 3 BGP prefixes.

Answer: AC

NEW QUESTION 57
View the exhibit, which contains the output of a BGP debug command, and then answer the question below.

```
# get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.125.0.60     4 65060     1698     1756     103    0     0 03:02:49            1
10.127.0.75     4 65075     2206     2250     102    0     0 02:45:55            1
10.200.3.1      4 65501      101      115       0    0     0 never              Active

Total number of neighbors 3
```

Which of the following statements about the exhibit are true? (Choose two.)

A. For the peer 10.125.0.60, the BGP state of is Established.
B. The local BGP peer has received a total of three BGP prefixes.
C. Since the BGP counters were last reset, the BGP peer 10.200.3.1 has never been down.
D. The local BGP peer has not established a TCP session to the BGP peer 10.200.3.1.

Answer: AD

NEW QUESTION 59
Which two statements about an auxiliary session are true? (Choose two.)

A. With the auxiliary session setting disabled, only auxiliary sessions are offloaded.
B. With the auxiliary session setting enabled, two sessions are created in case of routing change.
C. With the auxiliary session setting enabled, ECMP traffic is accelerated to the NP6 processor.
D. With the auxiliary session setting disabled, for each traffic path, FortiGate uses the same auxiliary session.

Answer: BC

NEW QUESTION 64
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 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
iike 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 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

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/238852

NEW QUESTION 69
Examine the following partial output from a sniffer command; then answer the question below.

```
# diagnose sniff packet any 'icmp' 4
interfaces= [any]
filters = [icmp]
2.101199 wan2 in 192.168.1.110-> 4.2.2.2: icmp: echo request
2.101400 wan1 out 172.17.87.16-> 4.2.2.2: icmp: echo request
.....
2.123500 wan2 out 4.2.2.2-> 192.168.1.110: icmp: echo reply
244 packets received by filter
5 packets dropped by kernel
```

What is the meaning of the packets dropped counter at the end of the sniffer?

A. Number of packets that didn't match the sniffer filter.
B. Number of total packets dropped by the FortiGate.
C. Number of packets that matched the sniffer filter and were dropped by the FortiGate.
D. Number of packets that matched the sniffer filter but could not be captured by the sniffer.

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=11655

NEW QUESTION 71
How are bulk configuration changes made using FortiManager CLI scripts? (Choose two.)

A. When run on the All FortiGate in ADOM, changes are automatically installed without the creation of a new revision history.
B. When run on the Device Database, changes are applied directly to the managed FortiGate device.
C. When run on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.
D. When run on the Policy Package, ADOM database, you must use the installation wizard to apply the changes to the managed FortiGate device

Answer: CD

Explanation:
CLI scripts can be run in three different ways:Device Database: By default, a script is executed on the
device database. It is recommend you run the changes on the device database (default setting), as this allows you to check what configuration changes you will send to the managed device. Once scripts are run on the device database, you can install these changes to a managed device using the installation wizard.
Policy Package, ADOM database: If a script contains changes related to ADOM level objects and policies, you can change the default selection to run on Policy Package, ADOM database and can then be installed using the installation wizard.
Remote FortiGate directly (through CLI): A script can be executed directly on the device and you don't need to install these changes using the installation wizard. As the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.

NEW QUESTION 72
What is the diagnose test application ipsmonitor 99 command used for?

A. To enable IPS bypass mode
B. To provide information regarding IPS sessions
C. To disable the IPS engine
D. To restart all IPS engines and monitors

Answer: D

NEW QUESTION 73
Refer to the exhibit, which contains partial outputs from two routing debug commands.

```
FortiGate # get router into routing-table database

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

FortiGate # get router info routing-table all

S*   0.0.0.0/0 [10/0] via 100.64.1.254, port1
```

Why is the port2 default route not in the second command's output?

A. It has a higher priority value than the default route using port1.
B. It is disabled in the FortiGate configuration.
C. It has a lower priority value than the default route using port1.
D. It has a higher distance than the default route using port1.

Answer: D

NEW QUESTION 74
Which of the following conditions must be met for a static route to be active in the routing table? (Choose three.)

A. The next-hop IP address is up.
B. There is no other route, to the same destination, with a higher distance.
C. The link health monitor (if configured) is up.
D. The next-hop IP address belongs to one of the outgoing interface subnets.
E. The outgoing interface is up.

Answer: CDE

Explanation:
A configured static route only goes to routing table from routing database when all the following are met :
- The outgoing interface is up
- There is no other matching route with a lower distance
- The link health monitor (if configured) is successful
- The next-hop IP address belongs to one of the outgoing interface subnets

NEW QUESTION 76
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.

Answer: C

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

NEW QUESTION 77
View the exhibit, which contains a partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:H2S_0_1: shortcut 10.200.5.1.:0   10.1.2.254->10.1.1.254
…
ike 0:H2S_0_1:15:  sent IKE msg (SHORTCUT-OFFER):  10.200.1.1:500->10.200.5.1:500,
len=164, id=4134df8580d5cdd/ce54851612c7432f:a21f14fe
ike 0: comes 10.200.5.1:500->10.200.1.1:500,ifindex=3….
ike 0: IKEv1 exchange=Informational id=4134df8580d5bcdd/ce54851612c7432f:6266ee8c
len=196

ike 0:H2S_0_1:15: notify msg received: SHORTCUR-QUERY
ike 0:H2S_0_1: recv shortcut-query 16462343159772385317

ike 0:H2S_0_0:16:  senr IKE msg (SHORTCUT-QUERY): 10.200.1.1:500->10.200.3.1:500,
len=196, id=7c6b6cca6700a935/dba061eaf51b89f7:b326df2a
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=3….
ike 0: IKEv1 exchange=Informational id=7c6b6cca6700a935/dba061eaf51b89f7:1c1dbf39
len=188

ike 0:H2S_0_0:16: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0: recv shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64
ike 0:H2S_0_0: shortcut-reply route to 10.1.2.254 via H2S_0_1 29
ike 0:H2S: forward shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64 ttl 31
ike 0:H2S_0_1:15: enc
…
ike 0:H2S_0_1:15: sent IKE msg (SHORTCUT-REPLY): 10.200.1.1:500->10.200.5.1:500,
len=188, id=4134df8580d5bcdd/ce54851612c7432f:70ed6d2c
```

Based on the debug output, which phase-1 setting is enabled in the configuration of this VPN?

A. auto-discovery-sender
B. auto-discovery-forwarder
C. auto-discovery-shortcut
D. auto-discovery-receiver

Answer: B

NEW QUESTION 80
View the exhibit, which contains the output of diagnose sys session list, and then answer the question below.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
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=/
state=may_dirty synced none app_ntf
statistic (bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
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=snst 10.0.1.10:65464->54.192.15.182:80(10.200.1.1:65464
hook-pre dir=reply act=dnat 54.192.15.182:80->10.200.1.1:65464(10.0.1.10:65464)
pos/ (before, after) 0/(0/0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary unit is zero (0), which statement is correct regarding the output?

A. This session is for HA heartbeat traffic.
B. This session is synced with the slave unit.
C. The inspection of this session has been offloaded to the slave unit.
D. This session cannot be synced with the slave unit.

Answer: B

NEW QUESTION 83
An administrator has configured a dial-up IPsec VPN with one phase 2, extended authentication (XAuth) and IKE mode configuration. The administrator has also enabled the IKE real time debug:
diagnose debug application ike-1 diagnose debug enable
In which order is each step and phase displayed in the debug output each time a new dial-up user is connecting to the VPN?

A. Phase1; IKE mode configuration; XAuth; phase 2.
B. Phase1; XAuth; IKE mode configuration; phase2.
C. Phase1; XAuth; phase 2; IKE mode configuration.
D. Phase1; IKE mode configuration; phase 2; XAuth.

Answer: B

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/IKE_Packet

NEW QUESTION 87
An administrator has configured a FortiGate device with two VDOMs: root and internal. The administrator has also created and inter-VDOM link that connects both VDOMs. The objective is to have each VDOM advertise some routes to the other VDOM via OSPF through the inter-VDOM link. What OSPF configuration settings must match in both VDOMs to have the OSPF adjacency successfully forming? (Choose three.)

A. Router ID.
B. OSPF interface area.
C. OSPF interface cost.
D. OSPF interface MTU.
E. Interface subnet mask.

Answer: BDE

NEW QUESTION 88
Refer to the exhibit, which shows partial outputs from two routing debug commands.

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

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

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
```

Why is the port2 default route not in the second command output?

A. The port2 interface is disabled in the FortiGate configuration.
B. The port1 default route has a lower distance than the default route using port2.
C. The port1 default route has a higher priority value than the default route using port2.
D. The port1 default route has a lower priority value than the default route using port2.

Answer: B

NEW QUESTION 92
Refer to the exhibit, which shows the output of a BGP debug command.

```
FGT # get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS       MsgRcvd MsgSent   TblVer  InQ OutQ   Up/Down   State/PfxRcd
10.125.0.60     4 65060       1698    1756      103      0    0    03:02:49        1
10.127.0.75     4 65075       2206    2250      102      0    0    02:45:55        1
100.64.3.1      4 65501       101     115        0       0    0    never       Active

Total number of neighbors 3
```

What can be concluded about the router in this scenario?

A. The router 100.64.3.1 needs to update the local AS number in its BGP configuration in order to bring up the BGP session with the local router.
B. The State/PfxRcd for neighbor 100.64.3.1 will not change until an administrator on the local router adjusts the inbound route filtering so that prefixes received can be added to the RIB.
C. All of the neighbors displayed are part of a single BGP configuration on the local router with the neighbor-range set to a value of 4.
D. The BGP session with peer 10.127.0.75 is up.

Answer: D

NEW QUESTION 93
Refer to the exhibit, which shows the output of a diagnose command.

```
FGT # diagnose debug rating
Locale        : english
Service       : Web-filter
Status        : Enable
License       : Contract
Service       : Antispam
Status        : Disable
Service       : Virus Outbreak Prevention
Status        : Disable
 -=- Server List (Mon Apr 19 10:41:32 20xx) -=-
IP                   Weight  RTT    Flags   TZ   Packets   Curr Lost     Total Lost
64.26.151.37         10      45             -5    262432    0             846
64.26.151.35         10      46             -5    329072    0             6806
66.117.56.37         10      75             -5    71638     0             275
65.210.95.240        20      71             -8    36875     0             92
209.222.147.36       20      103     DI     -8    34784     0             1070
208.91.112.194       20      107     D      -8    35170     0             1533
96.45.33.65          60      144            0     33728     0             120
80.85.69.41          71      226            1     33797     0             192
62.209.40.74         150     97             9     33754     0             145
121.111.236.179      45      44      F      -5    26410     26226         26227
```

What can be concluded about the debug output in this scenario?

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

Answer: B

NEW QUESTION 94
View the central management configuration shown in the exhibit, and then answer the question below.

```
config system central-management
   set type fortimanager
   set fmg "10.0.1.242"
   config server-list
      edit 1
         set server-type rating
         set server-address 10.0.1.240
      next
      edit 2
         set server-type update
         set server-address 10.0.1.243
      next
      edit 3
         set server-type rating
         set server-address 10.0.1.244
      next
   end
   set include-default-servers enable
end
```

Which server will FortiGate choose for antivirus and IPS updates if 10.0.1.243 is experiencing an outage?

A. 10.0.1.240
B. One of the public FortiGuard distribution servers
C. 10.0.1.244
D. 10.0.1.242

Answer: B

NEW QUESTION 95
View the exhibit, which contains the output of a real-time debug, Which statement about this output is true?

```
FGT # diagnose debug application urlfilter -1
FGT # diagnose debug enable

msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:
d=training.fortinet.com:443, id=687, cat=255, vfname='root', vfid=0,
profile='default', type=0, client=10.1.10.1, url_source=1, url="/"
action=9(ftgd-allow) wf-act=5(ALLOW) user="N/A" src=10.1.10.1 sport=58334
dst=13.226.142.41 dport=443 service="https" cat=52 url_cat=52 ip_cat=0
hostname="training.fortinet.com" url="/"
```

Which of the following statements is true regarding this output?

A. The requested URL belongs to category ID 255.
B. The server hostname Is training, fortinet.com.
C. FortiGate found the requested URL in its local cache.
D. This web request was inspected using the ftgd-allow web filler profile.

Answer: C

Explanation:
Example log for no local cache case: #id=93000 msg="pid=57 urlfilter_main-723 in main.c received pkt:count=91 "IPS and WAD will only send request to urlfilter daemon when cache is missed. " So the WAD process by itself found the URL rating in the local cache and didn`t ask for help from the URL process as in the example.

NEW QUESTION 100
Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

A. FortiGate limits the number of simultaneous sessions per explicit web proxy use
B. This limit CANNOT be modified by the administrator.
C. FortiGate limits the total number of simultaneous explicit web proxy users.
D. FortiGate limits the number of simultaneous sessions per explicit web proxy user The limit CAN be modified by the administrator
E. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials.This limit CANNOT be modified by the administrator.

Answer: B

Explanation:
https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-WAN-opt-52/web_proxy.htm#Explicit2
The explicit proxy does not limit the number of active sessions for each user. As a result the actual explicit proxy session count is usually much higher than the number of explicit web proxy users. If an excessive number of explicit web proxy sessions is compromising system performance you can limit the amount of users if the FortiGate unit is operating with multiple VDOMs.

NEW QUESTION 103
View the exhibit, which contains the output of a diagnose command, and the answer the question below.

```
# diagnose debug rating
Locale       : English
License      : Contract
Expiration   : Thu Sep 28 17:00:00 20XX
-=- Server List (Thu APR 19 10:41:32 20XX) -=-
IP               Weight   RTT   Flags   TZ   Packets  Curr Lost  Total Lost
64.26.151.37     10       45            -5    262432  0          846
64.26.151.35     10       46            -5    329072  0          6806
66.117.56.37     10       75            -5    71638   0          275
66.210.95.240    20       71            -8    36875   0          92
209.222.147.36   20       103   DI      -8    34784   0          1070
208.91.112.194   20       107   D       -8    35170   0          1533
96.45.33.65      60       144           0     33728   0          120
80.85.69.41      71       226           1     33797   0          192
62.209.40.74     150      97            9     33754   0          145
121.111.236.179  45       44    F       -5    26410   26226      26227
```

Which statements are true regarding the Weight value?

A. Its initial value is calculated based on the round trip delay (RTT).
B. Its initial value is statically set to 10.
C. Its value is incremented with each packet lost.
D. It determines which FortiGuard server is used for license validation.

Answer: C

NEW QUESTION 105
.....

Relate Links

100% Pass Your NSE7_EFW-7.0 Exam with Exambible Prep Materials

https://www.exambible.com/NSE7_EFW-7.0-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/