

Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

https://www.2passeasy.com/dumps/NSE7_EFW-7.0/



NEW QUESTION 1

Which two statements about bulk configuration changes made using FortiManager CLI scripts are correct? (Choose two.)

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

Answer: AB

NEW QUESTION 2

Examine the following partial outputs from two routing debug commands; then answer the question below.

```
# get router info kernel
```

```
tab=254 vf=0 scope=0type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.1.254 dev=2(port1)
```

```
tab=254 vf=0 scope=0type=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=10.200.2.254 dev=3(port2)
```

```
tab=254 vf=0 scope=253type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/->10.0.1.0/24 pref=10.0.1.254
```

```
gwy=0.0.0.0 dev=4(port3)
```

```
# get router info routing-table all s*0.0.0.0/0 [10/0] via 10.200.1.254, port1 [10/0] via 10.200.2.254, port2, [10/0] d0.0.1.0/24 is directly connected, port3  
d0.200.1.0/24 is directly connected, port1 d0.200.2.0/24 is directly connected, port2
```

Which outbound interface or interfaces will be used by this FortiGate to route web traffic from internal users to the Internet?

- A. port1
- B. port2.
- C. Both port1 and port2.
- D. port3.

Answer: B

NEW QUESTION 3

Refer to the exhibit, which shows a session table entry.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=11 duration=35 expire=265 timeout=300 flags=00000000
sockflag=00000000 sockport=0 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=redir local may_dirty none app_ntf
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
origin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545(192.167.1.100:49545)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:6c:7b:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 tos=ff/ff app_list=0 app=0 url_cat=41
rpd_b_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=00000000
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
```

Which statement about FortiGate behavior relating to this session is true?

- A. FortiGate redirected the client to the captive portal to authenticate, so that a correct policy match could be made.
- B. FortiGate forwarded this session without any inspection.
- C. FortiGate is performing security profile inspection using the CP
- D. FortiGate applied only IPS inspection to this session.

Answer: C

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 91, 92 First digit of "proto_state" value at 1 and considering all counters are at 0 for HW acceleration means CPU usage

NEW QUESTION 4

Refer to the exhibit, which shows 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 device is 0, what will happen if the primary fails and the secondary becomes the primary?

- A. Traffic for this session continues to be permitted on the new primary device after failover, without requiring the client to restart the session with the server.
- B. The secondary device has this session synchronized; however, because application control is applied, the session will be marked dirty and have to be re-evaluated after failover.
- C. The session state will be preserved but the kernel will need to re-evaluate the session due to NAT being applied.
- D. The session will be removed from the session table of the secondary device due to the presence of allowed error packets, which will force the client to restart the session with the server.

Answer: A

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-see-if-a-session-is-synced-in-HA/ta-p/1941>

NEW QUESTION 5

Four FortiGate devices configured for OSPF connected to the same broadcast domain. The first unit is elected as the designated router The second unit is elected as the backup designated router Under normal operation, how many OSPF full adjacencies are formed to each of the other two units?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: B

NEW QUESTION 6

How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

- A. FortiManager can download and maintain local copies of FortiGuard databases.
- B. FortiManager supports only FortiGuard push to managed devices.
- C. FortiManager will respond to update requests only if they originate from a managed device.
- D. FortiManager does not support rating requests.

Answer: A

NEW QUESTION 7

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 8

View the exhibit, which contains a partial web filter profile configuration, and then answer the question below.

Name: default

Comments: Default web filtering. 22/255

FortiGuard category based filter

Show Allow

- Bandwidth Consuming
- File Sharing and Storage

Status URL Filter

Block invalid URLs

URL Filter

URL	Type	Action	Status
*dropbox.com	Wildcard	<input checked="" type="checkbox"/> Block	Enable

Web content filter

Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	<input checked="" type="checkbox"/> Exempt	Enable

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

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

Answer: B

Explanation:

fortigate does it in order Static URL -> FortiGuard -> Content -> Advanced (java, cookie removal..)so block it in first step

NEW QUESTION 9

View the exhibit, which contains a session entry, and then answer the question below.

```

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
origin->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(10.200.1.254/10.1.0.1
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 is correct regarding this session?

- A. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
- B. It is an ICMP session from 10.1.10.10 to 10.200.5.1.
- C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.
- D. It is a TCP session in CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.

Answer: B

NEW QUESTION 10

Examine the output of the 'get router info ospf interface' command shown in the exhibit; then answer the question below.

```

# get router info ospf interface port4
port4 is up, line protocol is up
  Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
  Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROther, Priority 1
  Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
  Backup Designated Router (ID) 0.0.0.1, Interface Address
  172.20.121.239
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit
  5
    Hello due in 00:00:05
    Neighbor Count is 4, Adjacent neighbor count is 2
    Crypt Sequence Number is 411
    Hello received 106, sent 27, DD received 7 sent 9
    LS-Req received 2 sent 2, LS-Upd received 7 sent 5
    LS-Ack received 4 sent 3, Discarded 1

```

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

- A. The port4 interface is connected to the OSPF backbone area.
- B. The local FortiGate has been elected as the OSPF backup designated router.
- C. There are at least 5 OSPF routers connected to the port4 network.
- D. Two OSPF routers are down in the port4 network.

Answer: AC

Explanation:

on BROADCAST network there are 4 neighbors, among which 1*DR +1*BDR. So our FG has 4 neighbors, but create adjacency only with 2 (with DR and BDR). 2 neighbors DROther (not down).

NEW QUESTION 10

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

```
#dia hardware sysinfo shm
SHM counter:          150
SHM allocated:        0
SHM total:            625057792
conserve mode: on - mem
system last entered: Mon Apr 24 16:36:37 2017
sys fd last entered: n/a
SHM FS total:        641236992
SHM FS free:         641208320
SHM FS avail:        641208320
SHM FS alloc:        28672
```

What statement is correct about this FortiGate?

- A. It is currently in system conserve mode because of high CPU usage.
- B. It is currently in FD conserve mode.
- C. It is currently in kernel conserve mode because of high memory usage.
- D. It is currently in system conserve mode because of high memory usage.

Answer: D

NEW QUESTION 14

Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command.

```
Hub # get vpn ipsec tunnel details
gateway
  name: 'Hub2Spoke1'
  type: route-based
  local-gateway: 10.10.1.1:0 (static)
  remote-gateway: 10.10.2.2:0 (static)
  mode: ike-v1
  interface: 'wan2' (6)
  rx packets: 1025 bytes: 524402 errors: 0
  tx packets: 641 bytes: 93 errors: 0
  dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
  selectors
    name: 'Hub2Spoke1'
    auto-negotiate: disable
    mode: tunnel
    src: 0:192.168.1.0/0.0.0.0:0
    dst: 0:10.10.20.0/0.0.0.0:0
  SA
    lifetime/rekey: 43200/32137
    mtu: 1438
    tx-esp-seq: 2ce
    replay: enabled
  inbound
    spi: 01e54b14
    enc: aes-cb 914dc5d092667ed436ea7f6efb867976
    auth: sha1 a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
  outbound
    spi: 3dd3545f
    enc: aes-cb 017b8ff6c4ba21eac99b22380b7de74d
    auth: sha1 edd8141f4956140eef703d9042621d3dbf5cd961
  NPU acceleration: encryption(outbound) decryption(inbound)
```

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

- A. The npu_flag for this tunnel is 03.
- B. Different SPI values are a result of auto-negotiation being disabled for phase 2 selectors.
- C. Anti-replay is enabled.
- D. The npu_flag for this tunnel is 02.

Answer: AC

NEW QUESTION 18

Refer to the exhibit, which shows a session entry. Which statement about this session is true?

```

session info: proto=1 proto_state=00 duration=1 expire=59 timeout
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 tup
tx speed(Bps/kbps): 97/0 rx speed(Bps/kbps): 97/0
origin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.1
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

```

- A. It is an ICMP session from 10.1.10.10 to 10.200.5.1.
- B. It is a TCP session in close_wait state, from 10.
- C. 10.10 to 10.200.1.1.
- D. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
- E. It is a TCP session in the established state, from 10.1.10.10 to 10.200.5.1.

Answer: A

Explanation:

<https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGate-session-table-information/ta-p/1969>

NEW QUESTION 21

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

```

FGT # get router info ospf interface port4
port4 is up, line protocol is up
  Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
  Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROther, Priority 1
  Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
  Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:05
  Neighbor Count is 4, Adjacent neighbor count is 2
  Crypt Sequence Number is 411
  Hello received 106 sent 27, DD received 6 sent 3
  LS-Req received 2 sent 2, LS-Upd received 7 sent 17
  LS-Ack received 4 sent 3, Discarded 1

```

Which two statements about the output are true? (Choose two.)

- A. In the network connected to port 4, two OSPF routers are down.
- B. Based on the network type of port 4, OSPF hello packets will be sent to 224.0.0.5.
- C. Based on the network type of port 4, OSPF hello packets will be sent to 224.0.0.6.
- D. There are a total of 5 OSPF routers attached to the Port4 network segment.

Answer: BD

NEW QUESTION 24

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

```

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

```

What does the log mean?

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

Answer: B

NEW QUESTION 28

Which statement is true regarding File description (FD) conserve mode?

- A. IPS inspection is affected when FortiGate enters FD conserve mode.
- B. A FortiGate enters FD conserve mode when the amount of available description is less than 5%.
- C. FD conserve mode affects all daemons running on the device.
- D. Restarting the WAD process is required to leave FD conserve mode.

Answer: B

NEW QUESTION 32

View the exhibit, which contains a partial routing table, and then answer the question below.

```
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, which of the following pings will FortiGate route? (Choose two.)

- A. Source IP address 10.1.0.24, Destination IP address 10.72.3.20.
- B. Source IP address 10.72.3.27, Destination IP address 10.1.0.52.
- C. Source IP address 10.72.3.52, Destination IP address 10.1.0.254.
- D. Source IP address 10.73.9.10, Destination IP address 10.72.3.15.

Answer: BC

NEW QUESTION 36

Which the following events can trigger the election of a new primary unit in a HA cluster? (Choose two.)

- A. Primary unit stops sending HA heartbeat keepalives.
- B. The FortiGuard license for the primary unit is updated.
- C. One of the monitored interfaces in the primary unit is disconnected.
- D. A secondary unit is removed from the HA cluster.

Answer: AC

NEW QUESTION 40

Two independent FortiGate HA clusters are connected to the same broadcast domain. The administrator has reported that both clusters are using the same HA virtual MAC address. This creates a duplicated MAC address problem in the network. What HA setting must be changed in one of the HA clusters to fix the problem?

- A. Group ID.
- B. Group name.
- C. Session pickup.
- D. Gratuitous ARPs.

Answer: A

Explanation:

https://help.fortinet.com/fo50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverVMAC.htm

NEW QUESTION 44

Which two statements about conserve mode are true? (Choose two.)

- A. FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.
- B. FortiGate starts dropping all new sessions when the system memory reaches the configured redthreshold.
- C. FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.
- D. FortiGate exits conserve mode when the system memory goes below the configured green threshold.

Answer: AD

NEW QUESTION 49

Which real time debug should an administrator enable to troubleshoot RADIUS authentication problems?

- A. Diagnose debug application radius -1.
- B. Diagnose debug application fnbamd -1.
- C. Diagnose authd console -log enable.
- D. Diagnose radius console -log enable.

Answer: B

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD32838>

NEW QUESTION 50

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=statistic/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refernt=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
  dat: 0:10.1.1.0/255.255.255.0:0
  SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/OB replaywin=204B seqno=1
esn=replaywin_lastseq=00000000
  life: type=01 bytes=0/0 timeout=43177/43200
  dec: spi=ccclf66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
      ah=shal key=20 c68091d68753578785de6a7a6b276b506e527
```

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

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

Answer: AC

NEW QUESTION 51

What configuration changes can reduce the memory utilization in a FortiGate? (Choose two.)

- A. Reduce the session time to live.
- B. Increase the TCP session timers.
- C. Increase the FortiGuard cache time to live.
- D. Reduce the maximum file size to inspect.

Answer: AD

NEW QUESTION 52

Refer to the exhibit, which contains a TCL script configuration on FortiManager.

Type	TCL Script
Run script on	Remote FortiGate ...
Script details	<pre>#!/ proc do_cmd {cmd} { puts [exec "\$cmd\n" "# " 10] } run_cmd "config system interface " run_cmd "edit port1" run_cmd "set ip 10.0.1.10 255.255.255.0" run_cmd "next" run_cmd "end"</pre>

An administrator has configured the TCL script on FortiManager, but failed to apply any changes to the managed device after being executed. Why did the TCL script fail to make any changes to the managed device?

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

Answer: D

NEW QUESTION 53

The logs in a FSSO collector agent (CA) are showing the following error: failed to connect to registry: PIKA1026 (192.168.12.232) What can be the reason for this error?

- A. The CA cannot resolve the name of the workstation.
- B. The FortiGate cannot resolve the name of the workstation.
- C. The remote registry service is not running in the workstation 192.168.12.232.
- D. The CA cannot reach the FortiGate with the IP address 192.168.12.232.

Answer: C

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD30548>

NEW QUESTION 57

A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the 'diagnose debug authd fssolist' command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems. What should the administrator check? (Choose two.)

- A. The user student must not be listed in the CA's ignore user list.
- B. The user student must belong to one or more of the monitored user groups.
- C. The student workstation's IP subnet must be listed in the CA's trusted list.
- D. At least one of the student's user groups must be allowed by a FortiGate firewall policy.

Answer: AD

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828>

NEW QUESTION 59

Which two configuration commands change the default behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

- A. set av-failopen off
- B. set av-failopen pass
- C. set fail-open enable
- D. set ips fail-open disable

Answer: AC

Explanation:

<https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/194558/conserve-mode>

NEW QUESTION 60

What events are recorded in the crashlogs of a FortiGate device? (Choose two.)

- A. A process crash.
- B. Configuration changes.
- C. Changes in the status of any of the FortiGuard licenses.
- D. System entering to and leaving from the proxy conserve mode.

Answer: AD

Explanation:

diagnose debug crashlog read 275: 2014-08-05 13:03:53 proxy=acceptor service=imap session fail mode=activated276: 2014-08-05 13:03:53 proxy=acceptor service=ftp session fail mode=activated277: 2014-08-05 13:03:53 proxy=acceptor service=nntp session fail mode=activated278: 2014-08-06 11:05:47 service=kernel conserve=on free="45034 pages" red="45874 pages" msg="Kernel279: 2014-08-06 11:05:47 enters conserve mode"280: 2014-08-06 13:07:16 service=kernel conserve=exit free="86704 pages" green="68811 pages"281: 2014-08-06 13:07:16 msg="Kernel leaves conserve mode"282: 2014-08-06 13:07:16 proxy=imd sysconserve=exited total=1008 free=349 marginenter=201283: 2014-08-06 13:07:16 marginexit=302

NEW QUESTION 65

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 68

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 72

Which statement about memory conserve mode is true?

- A. A FortiGate exits conserve mode when the configured memory use threshold reaches yellow.
- B. A FortiGate starts dropping all the new and old sessions when the configured memory use threshold reaches extreme.
- C. A FortiGate starts dropping new sessions when the configured memory use threshold reaches red
- D. A FortiGate enters conserve mode when the configured memory use threshold reaches red

Answer: D

NEW QUESTION 75

View the exhibit, which contains a screenshot of some phase-1 settings, and then answer the question below.

The screenshot shows the configuration page for a phase-1 VPN tunnel. The 'Name' field is set to 'Remote' and the 'Comments' field is empty. Under the 'Network' section, 'IP Version' is set to 'IPv4'. 'Remote Gateway' is set to 'Static IP address'. 'IP Address' is set to '10.0.10.1'. 'Interface' is set to 'port1'. 'Mode Config' is unchecked, 'NAT Traversal' is checked, and 'Keepalive Frequency' is set to '10'. 'Dead Peer Detection' is also checked.

The VPN is up, and DPD packets are being exchanged between both IPsec gateways; however, traffic cannot pass through the tunnel. To diagnose, the administrator enters these CLI commands:

```
diagnose vpn ike log-filter src-add4 10.0.10.1
diagnose debug application ike-1
diagnose debug enable
```

However, the IKE real time debug does not show any output. Why?

- A. The debug output shows phases 1 and 2 negotiations onl
- B. Once the tunnel is up, it does not show any more output.
- C. The log-filter setting was set incorrectl
- D. The VPN's traffic does not match this filter.
- E. The debug shows only error message
- F. If there is no output, then the tunnel is operating normally.
- G. The debug output shows phase 1 negotiation onl
- H. After that, the administrator must enable the following real time debug: diagnose debug application ipsec -1.

Answer: B

NEW QUESTION 80

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

```
# diagnose sys session list expectation

session info: proto=6 proto_state=00 duration=3 expire=26 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=1 tunnel=/
state=new complex
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
origin->sink: org pre->post, reply pre->post dev=2->4/4->2 gw=10.0.1.10/10.200.1.254
hook-pre dir=org act=dnat 10.171.121.38:0->10.200.1.1:60426(10.0.1.10:50365)
hook-pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What can you conclude from the output shown in the exhibit? (Choose two.)

- A. This is a pinhole session created to allow traffic for a protocol that requires additional sessions to operate through FortiGate.
- B. This is an expected session created by the IPS engine.
- C. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.200.1.1.
- D. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to thenext-hop IP address 10.0.1.10.

Answer: AD

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 110, 111, 115

NEW QUESTION 82

Refer to the exhibits.

```
config vpn ipsec phase1-interface
edit "user-1"
set type dynamic
set interface "port1"
set mode main
set xauthtype auto
set authusrgrp "Users-1"
set peertype any
set dhgrp 14 15 19
set proposal aes128-sha256 aes256-sha384
set psksecret <encrypted_password>
next
```

Which contain the partial configurations of two VPNs on FortiGate.

An administrator has configured two VPNs for two different user groups. Users who are in the Users-2 group are not able to connect to the VPN. After running a diagnostics command, the administrator discovered that FortiGate is not matching the user-2 VPN for members of the Users-2 group.

Which two changes must administrator make to fix the issue? (Choose two.)

- A. Use different pre-shared keys on both VPNs
- B. Enable Mode Config on both VPNs.
- C. Set up specific peer IDs on both VPNs.
- D. Change to aggressive mode on both VPNs.

Answer: CD

Explanation:

To set peer-id, the VPN must be set in aggressive mode - <https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-use-Peer-IDs-to-select-an-IPSec-dialup/ta-p>

NEW QUESTION 86

An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link-failed-signal to fix the problem. Which statement is correct regarding this command?

- A. Forces the former primary device to shut down all its non-heartbeat interfaces for one second while the failover occurs.
- B. Sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.
- C. Sends a link failed signal to all connected devices.
- D. Disables all the non-heartbeat interfaces in all the HA members for two seconds after a failover.

Answer: A

NEW QUESTION 87

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

- A. Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer.
- B. Only the root FortiGate sends logs to FortiAnalyzer.
- C. Only FortiGate devices with fabric-object-unification set to default will receive and synchronize global CMDB objects sent by the root FortiGate.
- D. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.

Answer: AC

Explanation:

FortiGate's to Root uses FortiTelemetry (TCP-8013) FortiTelemetry is also used for FortiClient communication Root Fortigate to FortiAnalyzer uses API (TCP-443)

NEW QUESTION 92

View the exhibit, which contains an entry in the session table, and then answer the question below.

```
session info: proto=6 proto_state=11 duration=53 expire=265 timeout=300 flags=00000000
sockflag=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=AALI state=redir log local may_dirty npu nlb none acct-ext
statistic (bytes/packets/allow_err): org=2651/17/1 reply=19130/28/1 tuples=3
tx speed (Bps/kbps): 75/0 rx speed (Bps/kbps): 542/4
origin->sink: org pre->post, reply pre->post dev=7->6/6->7 gw=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443 (172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545 (192.167.1.100:49545)
hook=post dir=reply act=noop 216.58.216.238:443->192.167.1.100:49545 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:6c:7b:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 tos=ff/ff app_list=0 app=0 url_cat=41
dd_type=0 dd_mode=0
npu_state=00000000
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
```

Which one of the following statements is true regarding FortiGate's inspection of this session?

- A. FortiGate applied proxy-based inspection.
- B. FortiGate forwarded this session without any inspection.
- C. FortiGate applied flow-based inspection.
- D. FortiGate applied explicit proxy-based inspection.

Answer: A

Explanation:

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

NEW QUESTION 94

You have configured FortiManager as a local FDS to provide FortiGate AV and IPS updates, but FortiGate devices are not receiving updates to their AV signature databases, IPS engines, or IPS signature databases.

Which two settings need to be verified for these features to function? (Choose two.)

- A. FortiGate needs to have the server list entry for FortiManager set to server-type update under config system central-management.
- B. FortiManager needs to be the license validation server for FortiGate devices trying to retrieve updated AV and IPS packages.
- C. Service access needs to be enabled on FortiManager under System Settings > Network.
- D. FortiGate needs to have include-default-servers disabled under config system central-management.

Answer: AC

Explanation:

NSE 7.0 Guide page 184-185

NEW QUESTION 98

An administrator has been assigned the task of creating a set of firewall policies which must be evaluated before any custom policies defined within the policy packages of managed FortiGate devices, across all 25 ADOMs in FortiManager.

How should the administrator accomplish this task?

- A. Create a footer policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this footer policy to all other ADOMs.
- B. Create a header policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this header policy to all other ADOMs.
- C. Move the FortiGate devices into a single globally scoped ADOM, and merge policy packages, inserting the new firewall policies at the top.
- D. Use a CLI script from the root ADOM on FortiManager to push these new policies to all FortiGate devices, through the FGFM tunnel.

Answer: B

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 244

NEW QUESTION 103

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 107

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 112

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

```
# diagnose hardware sysinfo conserve
memory conserve mode:          on
total RAM:                     3040 MB
memory used:                   2706 MB 89% of total RAM
Memory freeable:              334 MB 11% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red:    2675 MB 88% of total RAM
memory used threshold green:  2492 MB 82% of total RAM
```

If the default settings are in place, what can be concluded about the conserve mode shown in the exhibit?

- A. FortiGate is currently blocking all new sessions regardless of the content inspection requirements or configuration settings due to high memory use.
- B. FortiGate is currently allowing new sessions that require flow-based or proxy-based content inspection but is not performing inspection on those sessions.
- C. FortiGate is currently blocking new sessions that require flow-based or proxy-based content inspection.
- D. FortiGate is currently allowing new sessions that require flow-based content inspection and blocking sessions that require proxy-based content inspection.

Answer: C

NEW QUESTION 117

Examine the following routing table and BGP configuration; then answer the question below.

```
#get router info routing-table all
*0.0.0.0/0 [10/0] via 10.200.1.254, port1
C10.200.1.0/24 is directly connected, port1
S192.168.0.0/16 [10/0] via 10.200.1.254, port1
# show router bgp
config router bgp
set as 65500
set router-id 10.200.1.1
set network-import-check enable
set ebgp-multipath disable
config neighbor
edit "10.200.3.1"
set remote-as 65501
next
end
config network
edit1
```

The BGP connection is up, but the local peer is NOT advertising the prefix 192.168.1.0/24. Which configuration change will make the local peer advertise this prefix?

- A. Enable the redistribution of connected routers into BGP.
- B. Enable the redistribution of static routes into BGP.
- C. Disable the setting network-import-check.
- D. Enable the setting ebgp-multipath.

Answer: C

NEW QUESTION 118

A FortiGate is configured as an explicit web proxy. Clients using this web proxy are reporting DNS errors when accessing any website. The administrator executes the following debug commands and observes that the n-d ns-timeout counter is increasing:

```
#diagnose test application wad 2200
#diagnose test application wad 104
DNS Stats:
n_dns_reqs=878 n_dns_fails= 2 n_dns_timeout=875
n_dns_success=0

n_snd_retries=0 n_snd_fails=0 n_snd_success=0 n_dns_overflow=0
n_build_fails=0
```

What should the administrator check to fix the problem?

- A. The connectivity between the FortiGate unit and the DNS server.
- B. The connectivity between the client workstations and the DNS server.
- C. That DNS traffic from client workstations is allowed by the explicit web proxy policies.
- D. That DNS service is enabled in the explicit web proxy interface.

Answer: A

NEW QUESTION 120

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 filter 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 121

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 122

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     -5   262432  0          846
64.26.151.35  10      46    -5     -5   329072  0          6806
66.117.56.37  10      75    -5     -5   71638   0          275
66.210.95.240 20      71    -8     -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      0    33728   0          120
80.85.69.41   71      226   1      1    33797   0          192
62.209.40.74  150     97    9      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 123

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_EFW-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_EFW-7.0 Product From:

https://www.2passeasy.com/dumps/NSE7_EFW-7.0/

Money Back Guarantee

NSE7_EFW-7.0 Practice Exam Features:

- * NSE7_EFW-7.0 Questions and Answers Updated Frequently
- * NSE7_EFW-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_EFW-7.0 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * NSE7_EFW-7.0 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year