

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

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 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)
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 2

When using the SSL certificate inspection method to inspect HTTPS traffic, how does FortiGate filter web requests when the client browser does not provide the server name indication (SNI) extension?

- A. FortiGate uses the requested URL from the user's web browser.
- B. FortiGate uses the CN information from the Subject field in the server certificate.
- C. FortiGate blocks the request without any further inspection.
- D. FortiGate switches to the full SSL inspection method to decrypt the data.

Answer: B

NEW QUESTION 3

Refer to the exhibit, which contains the output of get system ha status. Which two statements about the output are true? (Choose two.)

```
NGFW-1 # get system ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 2
Debug: 0
Cluster Uptime: 0 days 4:23:19
Cluster state change time: 2019-01-25 10:19:46
Master selected using:
  <2019/01/25 10:19:46> FGVM010000077649 is selected as the master because it has the largest value
of override priority.
  <2019/01/25 10:19:40> FGVM010000077649 is selected as the master because it's the only member in
the cluster.
ses_pickup: disable
override: enable
Configuration Status:
  FGVM010000077649 (updated 1 seconds ago): in-sync
  FGVM010000077650 (updated 0 seconds ago): out-of-sync
System Usage stats:
  FGVM010000077649 (updated 1 seconds ago):
    sessions=27, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=56%
  FGVM010000077650 (updated 0 seconds ago):
    sessions=2, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=57%
HBDEV stats:
  FGVM010000077649 (updated 1 seconds ago):
    port7: physical/10000full, up, rx-bytes/packets/dropped/errors=63817615/202024/0/0, tx=
71110281/121109/0/0
  FGVM010000077650 (updated 0 seconds ago):
    port7: physical/10000full, up, rx-bytes/packets/dropped/errors=79469596/122024/0/0, tx=
30877890/107878/0/0
Master: NGFW-1      , FGVM010000077649, cluster index = 1
Slave : NGFW-2      , FGVM010000077650, cluster index = 0
number of voluster: 1
voluster 1: work 169.254.0.2
Master: FGVM010000077649, operating cluster index = 0
Slave : FGVM010000077650, operating cluster index = 1
```

- A. The slave configuration is synchronized with the master.
- B. port7 is used as the HA heartbeat on all devices in the cluster.
- C. Primary is selected based on the priority configured under config system ha.
- D. The HA management IP is 169.254.0.2.

Answer: BC

NEW QUESTION 4

View the exhibit, which contains the output of diagnose sys session stat, and then answer the question below.

```
NGFW-1 # diagnose sys session stat
misc info:      session_count=591  setup_rate=0  exp_count=0
clash=162  memory_tension_drop=0  ephemeral=0/65536
removeable=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
  166 in NONE state
  1 in ESTABLISHED state
  3 in SYN_SENT state
  2 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000006
global: ses_limit=0  ses6_limit=0  rt_limit=0  rt6_limit=0
```

Which statements are correct regarding the output shown? (Choose two.)

- A. There are 0 ephemeral sessions.
- B. All the sessions in the session table are TCP sessions.
- C. No sessions have been deleted because of memory pages exhaustion.
- D. There are 166 TCP sessions waiting to complete the three-way handshake.

Answer: AC

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40578>

NEW QUESTION 5

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

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

Answer: BD

Explanation:

CLI scripts can be run in three different ways: Device Database: By default, a script is executed on the device database. It is recommended 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 6

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 7

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 8

An administrator cannot connect to the GUI of a FortiGate unit with the IP address 10.0.1.254. The administrator runs the debug flow while attempting the connection using HTTP. The output of the debug flow is shown in the exhibit:

```
# diagnose debug flow filter port 80
# diagnose debug flow trace start 5
# diagnose debug enable

id=20085 trace_id=5 msg="vd-root received a packet(proto=6,
10.0.1.10:57459->10.0.1.254:80) from port3. flag [S], seq 3190430861, ack
0, win 8192"
id=20085 trace_id=5 msg="allocate a new session-0000008c"
id=20085 trace_id=5 msg="iprope_in_check() check failed on policy 0, drop"
```

Based on the error displayed by the debug flow, which are valid reasons for this problem? (Choose two.)

- A. HTTP administrative access is disabled in the FortiGate interface with the IP address 10.0.1.254.
- B. Redirection of HTTP to HTTPS administrative access is disabled.
- C. HTTP administrative access is configured with a port number different than 80.
- D. The packet is denied because of reverse path forwarding check.

Answer: AC

NEW QUESTION 9

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 10

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 10

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 15

An administrator is running the following sniffer in a FortiGate: diagnose sniffer packet any "host 10.0.2.10" 2
 What information is included in the output of the sniffer? (Choose two.)

- A. Ethernet headers.
- B. IP payload.
- C. IP headers.
- D. Port names.

Answer: BC

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=11186>

NEW QUESTION 16

Which two tasks are automated using the Install Wizard on FortiManager? (Choose two.)

- A. Preview pending configuration changes for managed devices.
- B. Add devices to FortiManager.
- C. Import policy packages from managed devices.
- D. Install configuration changes to managed devices.
- E. Import interface mappings from managed devices.

Answer: AD

Explanation:

https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/1200_ins

There are 4 main wizards: Add Device: is used to add devices to central management and import their configurations.

Install: is used to install configuration changes from Device Manager or Policies & Objects to the managed devices. It allows you to preview the changes and, if the administrator doesn't agree with the changes, cancel and modify them.

Import policy: is used to import interface mapping, policy database, and objects associated with the managed devices into a policy package under the Policy & Object tab. It runs with the Add Device wizard by default and may be run at any time from the managed device list.

Re-install policy: is used to perform a quick install of the policy package. It doesn't give the ability to preview the changes that will be installed to the managed device.

NEW QUESTION 21

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: SHORTCUT-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 23

Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below:

```
# diagnose ip router bgp all enable
# diagnose ip router bgp level info
# diagnose debug enable
"BGP: 10.200.3.1-Outgoing [DECODE] KAlive: Received!"
"BGP: 10.200.3.1-Outgoing [FSM] State: OpenConfirm Event: 26"
"BGP: 10.200.3.1-Outgoing [DECODE] Msg-Hdr: type 2, length 56"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: Starting UPDATE decoding... Byt
(37), msg_size (37)"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: NLRI Len(13)"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 27"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 0.0.0.0/0"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.4.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.3.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.0.2.0/24"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
"BGP: 10.200.3.1-Outgoing [ENCODE] Msg-Hdr: Type 2"
"BGP: 10.200.3.1-Outgoing [ENCODE] Attr IP-Unicast: Tot-attr-len 20"
"BGP: 10.200.3.1-Outgoing [ENCODE] Update: Msg #5 Size 55"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
```

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

- A. BGP peers have successfully interchanged Open and Keepalive messages.
- B. Local BGP peer received a prefix for a default route.
- C. The state of the remote BGP peer is OpenConfirm.
- D. The state of the remote BGP peer will go to Connect after it confirms the received prefixes.

Answer: AB

NEW QUESTION 24

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

NEW QUESTION 26

A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

- A. Firewall monitor.
- B. Policy monitor.
- C. Logs.
- D. Crashlogs.

Answer: CD

NEW QUESTION 27

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 32

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


```
# 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
```

Which one of the following statements about this FortiGate is correct?

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

Answer: D

NEW QUESTION 37

When using the SSL certificate inspection method for HTTPS traffic, how does FortiGate filter web requests when the browser client does not provide the server name indication (SNI) extension?

- A. FortiGate uses CN information from the Subject field in the server's certificate.
- B. FortiGate switches to the full SSL inspection method to decrypt the data.
- C. FortiGate blocks the request without any further inspection.
- D. FortiGate uses the requested URL from the user's web browser.

Answer: A

NEW QUESTION 38

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 43

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

- A. av-failopen
- B. mem-failopen
- C. utm-failopen
- D. ips-failopen

Answer: A

Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Other_Profile_Consideratio

NEW QUESTION 44

Examine the following partial output from two system debug commands; then answer the question below.

```
# diagnose hardware sysinfo memory
MemTotal: 3092728 kB
MemFree: 1954204 kB
MemShared: 0 kB
Buffers: 284 kB
Cached: 143004 kB
SwapCached: 0 kB
Active: 34092 kB
Inactive: 109256 kB
HighTotal 1179648 kB
HighFree: 853516 kB
LowTotal: 1913080 kB
LowFree: 1100688 kB
SwapTotal: 0 kB
SwapFree: 0 kB
# diagnose hardware sysinfo shm
SHM counter: 285
SHM allocated: 6823936
SHM total: 623452160
concermode: 0
shm last entered: n/a
system last entered: n/a
SHM FS total: 639725568
SHM FS free: 632614912

SHM FS alloc: 7110656
```

Which of the following statements are true regarding the above outputs? (Choose two.)

- A. The unit is running a 32-bit FortiOS
- B. The unit is in kernel conserve mode
- C. The Cached value is always the Active value plus the Inactive value
- D. Kernel indirectly accesses the low memory (LowTotal) through memory paging

Answer: AC

NEW QUESTION 48

When does a RADIUS server send an Access-Challenge packet?

- A. The server does not have the user credentials yet.
- B. The server requires more information from the user, such as the token code for two-factor authentication.
- C. The user credentials are wrong.
- D. The user account is not found in the server.

Answer: B

NEW QUESTION 51

Which two conditions must be met for a statistic route to be active in the routing table? (Choose two.)

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

Answer: AC

NEW QUESTION 53

Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

- A. Neighbor range
- B. Route reflector
- C. Next-hop-self
- D. Neighbor group

Answer: B

Explanation:

Route reflectors help to reduce the number of IBGP sessions inside an AS. A route reflector forwards the routes learned from one peer to the other peers. If you configure route reflectors, you don't need to create a full mesh IBGP network. All clients in a cluster only talk to route reflector to get sync routing updates. Route reflectors pass the routing updates to other route reflectors and border routers within the AS.

NEW QUESTION 57

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 60

Refer to the exhibit, which shows a FortiGate configuration.

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

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

- A. The administrator must increase webfilter-timeout.
- B. The administrator must disable webfilter-force-off.
- C. The administrator must change protocol to TCP.
- D. The administrator must enable fortiguard-anycast.

Answer: D

NEW QUESTION 65

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 70

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 routers into BGP.
- C. Disable the setting network-import-check.
- D. Enable the setting ebgp-multipath.

Answer: C

NEW QUESTION 74

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

diagnose webfilter fortiguard statistics list

Raring Statistics:

```
=====
DNS filures      : 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 requests 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 one of the following statements explains why the cache statistics are all zeros?

- A. The administrator has reallocated the cache memory to a separate process.
- B. There are no users making web requests.
- C. The FortiGuard web filter cache is disabled in the FortiGate's configuration.
- D. FortiGate is using a flow-based web filter and the cache applies only to proxy-based inspection.

Answer: C

NEW QUESTION 75

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 76

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 80

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 83

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
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=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 86

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 identifier 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 87

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

- A. IPS failopen
- B. mem failopen
- C. AV failopen
- D. UTM failopen

Answer: AC

NEW QUESTION 92

.....

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 FirstTry
- * NSE7_EFW-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year