

NSE7_EFW-6.4.pre.exam.35q - DEMO

Number: 000-000
Passing Score: 800
Time Limit: 120 min



NSE7_EFW-6.4

Fortinet NSE 7 - Enterprise Firewall 6.4



Exam A

QUESTION 1

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

- A. Installing configuration changes to managed devices
- B. Importing interface mappings from managed devices
- C. Adding devices to FortiManager
- D. Previewing pending configuration changes for managed devices

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

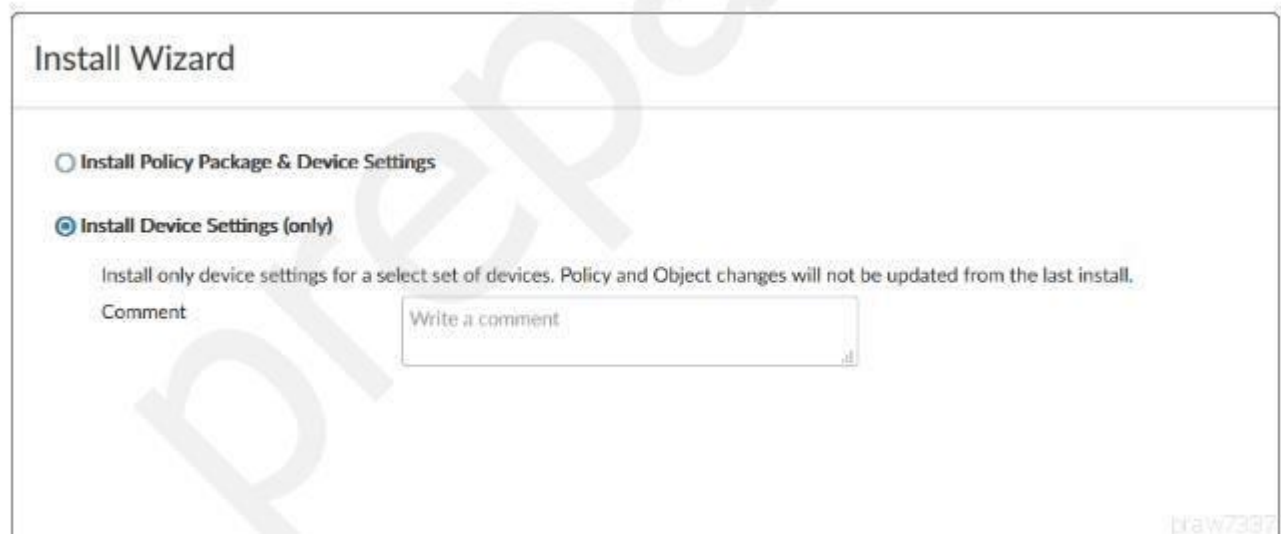
Reference: <https://docs.fortinet.com/document/fortimanager/6.2.0/administration-guide/668612/using-the-install-wizard-to-install-device-settings-only>

Using the Install Wizard to install device settings only

You can use the *Install Wizard* to install device settings only to one or more FortiGate devices. The *Install Wizard* includes a preview feature.

To use the Install Wizard to install device settings only:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. In the toolbar, select *Install Wizard* or *Install > Install Wizard*.
3. Select *Install Device Settings (only)* and if you want, type a comment. Click *Next*.



Install Wizard

☐ Install Policy Package & Device Settings

☒ Install Device Settings (only)

Install only device settings for a select set of devices. Policy and Object changes will not be updated from the last install.

Comment

QUESTION 2

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

```

VCEup

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

- A. Phase 2 authentication is set to sha1 on both sides.
- B. Anti-replay is disabled.
- C. Hub2Spoke1 is a policy-based VPN.
- D. Hub2Spoke1 is configured on interface wan2.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

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 send 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
```

praw733771

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

- A. The local FortiGate OSPF router ID is 0.0.0.4.
- B. Port4 is connected to the OSPF backbone area.
- C. In the network connected to port4, two OSPF routers are down.
- D. The local FortiGate is the backup designated router.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Area 0.0.0.0 is the backbone area.

QUESTION 4

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=ccclf66d 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

```

raw733771

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.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

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: IKEv2 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
16:39915120ED73ED73E520787C801DE3678916
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
A2FBD6BB6394401A06B89C022D4DF682081004010000000000000500B000018882A07BE09026CA8B2
ike 0: Remotesite:3: out
A2FBD6BB6394401A06B89C022D4DF6820810040100000000000005C64D5CBA90B873F150CB8B5CC2A
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 remote gateway IP address is 10.0.0.1.
- B. The initiator provided `remote` as its IPsec peer ID.
- C. It shows a phase 1 negotiation.
- D. The negotiation is using AES128 encryption with CBC hash.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

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

```

Which statement about the exhibit is true?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Active means it is actively trying to establish a TCP connection using port 179, but has not yet actually established one.

QUESTION 7

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 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 script must start with #include <>.
- B. The TCL command run_cmd has not been created.

- C. Changes to an interface configuration can be made only by a CLI script.
- D. Incomplete commands are ignored in TCL scripts.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

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
      |- 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
raw733771
```

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.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortimanager/7.0.0/upgrade-guide/959309/cli-example-of-diagnose-dvm-device-list>

Following is an example of the CLI output for the `diagnose dvm device list` command:

```
# diagnose dvm device list
--- There are currently 16 devices/vdoms managed ---
TYPE          OID SN          HA IP          NAME    ADOM    IPS
...
...
fmg/faz enabled 448 FGVM020000058807 - 10.3.121.82 FGVM82 54-VPN 6.00741 (regular)
|- STATUS: db: modified; conf: in sync; cond: OK; dm: retrieved; conn: up
|- vdom:[3]root flags:0 adom:54-VPN pkg:[modified]pp_vpn_v1
fmg/faz enabled 317 FGVM02Q105060033 - 10.3.121.92 FGVM92 54-ADOM 6.00741 (regular)
|- STATUS: db: not modified; conf: out of sync; cond: unknown; dm: autoupdated; conn: down
|- vdom:[3]root flags:1 adom:54-ADOM pkg:[unknown]VM92_root
...
...
--- End device list ---
```

This command shows the total number of devices or VDOMs, the configuration status of devices and policy packages, and the connection status. The number of managed devices or VDOMs should be the same before and after the upgrade.

- If the device configuration or policy package status (db) is modified, we recommend installing the changes before upgrading.
- The policy package status (pkg) shows if there is any pending package change on a policy package that has been linked to a device or VDOM. This status can be modified, never-installed, or unknown.
- The connection status (conn) is either up or down.

paw733771

QUESTION 9

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
```

praw733771

VCEUp

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`.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.4.5/cli-reference/109620/config-system-fortiguard>

config system fortiguard

Parameter	Description	Type	Size	Default
fortiguard-anycast	Enable/disable use of FortiGuard's anycast network.	option	-	enable

Option	Description
<i>enable</i>	Enable use of FortiGuard's anycast network.
<i>disable</i>	Disable use of FortiGuard's anycast network.

QUESTION 10

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://checkthefirewall.com/blogs/fortinet/ssl-inspection>

SSL certificate inspection

FortiGate identifies the SSL server name by inspecting the SSL handshake, specifically the client hello and server hello messages, both of which are exchanged in clear-text. In the client hello, FortiGate checks the SNI extension, while on the server hello, FortiGate looks at the CN and SAN. By looking at the SNI, CN and SAN values, FortiGate can identify the hostname of the SSL server. The hostname is then checked against the web filtering profile enabled in the matching policy to determine whether the website must be allowed or blocked. If the website must be allowed, FortiGate let the client and server complete the SSL handshake and exchange data through the SSL connection. However, if the website must be blocked, FortiGate performs MITM and presents the client a replacement message instead of the original website. The replacement message informs the user that the website has been blocked by web filtering. The following is an example of a replacement message:

QUESTION 11

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.

```

gaw733771

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/320160/example-advpn-configuration>

The New York hub would have a dynamic phase 1 for its spoke connections, and two static phase 1s for its connections to the other hubs:

```
config vpn ipsec phase1-interface
  edit "Spokes"
    set type dynamic
    set interface wan1
    set psk <New-York-PSK>
    set auto-discovery-sender enable
    set auto-discovery-psk enable
    set add-route disable
  next
  edit "London"
    set type static
    set interface wan1
    set psk <New-York-London-PSK>
    set auto-discovery-forwarder enable
  next
  edit "Shanghai"
    set type static
    set interface wan1
    set psk <New-York-Shanghai-PSK>
    set auto-discovery-forwarder enable
  next
end
```

The 'Spokes' connection has `set auto-discovery-sender enable` to indicate that when IPsec traffic transits the hub it should optionally generate a message to the initiator of the traffic to indicate that it could perhaps establish a more direct connection.

QUESTION 12 Which two statements about OCVPN are true? (Choose two.)

- A. Only root vdom supports OCVPN.
- B. OCVPN supports static and dynamic IPs in WAN interface.
- C. OCVPN offers only Hub-Spoke VPNs.
- D. FortiGate devices under different FortiCare accounts can be used to form OCVPN.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/977344/one-click-vpn-ocvpn> <https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/496884/overlay-controller-vpn-ocvpn>

Overlay Controller VPN (OCVPN)

Overlay Controller VPN (OCVPN) is a cloud based solution to simplify IPsec VPN setup. When OCVPN is enabled, IPsec phase1-interfaces, phase2-interfaces, static routes, and firewall policies are generated automatically on all FortiGates that belong to the same community network. A community network is defined as all FortiGates registered to FortiCare using the same FortiCare account.

If the network topology changes on any FortiGates in the community (such as changing a public IP address in DHCP mode, adding or removing protected subnets, failing over in dual WAN), the IPsec-related configuration for all devices is updated with Cloud assistance in self-learning mode. No intervention is required.

QUESTION 13

Refer to the exhibit, which shows a central management configuration.

```
config system central-management
  set type fortimanager
  set fmg "10.0.1.242"
  config server-list
    edit 1
      set server-type rating
      set addr-type ipv4
      set server-address 10.0.1.240
    next
    edit 2
      set server-type update
      set addr-type ipv4
      set server-address 10.0.1.243
    next
    edit 3
      set server-type rating
      set addr-type ipv4
      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. 10.0.1.242
- B. Public FortiGuard servers
- C. 10.0.1.240

D. 10.0.1.244

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD38219>

Purpose

This article describes how to over-ride FortiGate central-management setting to get updates from FortiManager.

Expectations, Requirements

FortiGate will receive updates from FortiManager other than FortiGuard servers.

Configuration

If FortiGate is setup to get updates from FortiGuard server, following is the configuration:

```
config system central-management
  set type fortimanager
  set fmg "x.x.x.x"
  set include-default-servers enable
end
```

<----- This setting will ensure FortiGate is getting update from FortiGuard default servers.

QUESTION 14 Which two statements about application layer test commands are true? (Choose two.)

- A. They display real-time application debugs.
- B. They are used to filter real-time debugs.
- C. Some of them can be used to restart an application.
- D. Some of them display statistics and configuration information about a feature or process.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15 Which two configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/681934/conservemode>

Antivirus conserve mode effects

You can use the following command to configure how antivirus processing acts when conserve mode is reached:

```
config system global
    set av-failopen {pass | off | one-shot}
end
```

What happens when the FortiGate unit enters conserve mode depends on how you have av-failopen configured.

There are four options:

off

The off setting forces the FortiGate unit to stop all traffic that is configured for content inspection by Security Profiles features that use the AV proxy. New sessions are not allowed but current sessions continue to be processed normally unless they request more memory. Sessions requesting more memory are terminated.

For example, if a security policy is configured to use antivirus scanning, the traffic it permits is blocked while in conserve mode. A policy with IPS scanning enabled continues as normal. A policy with both IPS and antivirus scanning is blocked because antivirus scanning requires the AV proxy.

Use the off setting when security is more important than a loss of access while the problem is rectified.

QUESTION 16

An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device. The administrator decides to enable the setting `link-failed-signal` to fix the problem.

Which statement about this setting is true?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://kb.fortinet.com/kb/viewContent.do?externalId=FD40860&sliceId=1>

Reference

Refer to the [High Availability](#) section of the OnLine Help guide.

When a FortiGate HA cluster is operating and a monitored interface fails on the primary unit, the primary unit becomes a subordinate unit and another cluster unit becomes the primary unit.

Normally, after a link failover, the new primary unit sends Gratuitous ARP (GARP) packets to refresh the MAC forwarding tables of the switches connected to the cluster.

In some instances switches ignore the GARP packets and continue to reference the MAC address for the port the on the failed FortiGate and will keep sending packets.

You can use the following command to cause a cluster unit with a monitored interface link failure to briefly shut down all of its interfaces (except the heartbeat interfaces and HA mgmt Interface) after the failover occurs:

```
config system ha
set link-failed-signal enable
end
```

praw733771

QUESTION 17

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 10:42:32 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
65.210.95.240  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 two statements about the output in the exhibit are true? (Choose two.)

- A. FortiGate will probe 121.111.236.179 every fifteen minutes for a response.
- B. Servers with a negative TZ value are experiencing a service outage.

- C. Servers with the D flag are considered to be down.
- D. FortiGate used 209.222.147.36 as the initial server to validate its contract.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

15 minutes is the default probing time, where the F flag is for failed connection. Flag I represents the Initial request on 209.222.147.36.

QUESTION 18

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 inspection of this session is true?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

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.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortimanager/6.2.1/administration-guide/71780/cli-scripts>

CLI scripts

CLI scripts include only FortiOS CLI commands as they are entered at the command line prompt on a FortiGate device. 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.

CLI scripts are useful for specific tasks such as configuring a routing table, adding new firewall policies, or getting system information. These example tasks easily apply to any or all FortiGate devices connected to the FortiManager system.

However, the more complex a CLI script becomes the less it can be used with all FortiGate devices - it quickly becomes tied to one particular device or configuration. One example of this is any script that includes the specific IP address of a FortiGate device's interfaces cannot be executed on a different FortiGate device.

Samples of CLI scripts have been included to help get you started writing your own scripts for your network administration tasks.

Error messages will help you determine the causes of any CLI scripting problems, and fix them. For more information, see [Error Messages](#).

The troubleshooting tips section provides some suggestions on how to quickly locate and fix problems in your CLI scripts. For more information, see [Troubleshooting Tips](#).

paaw733771

QUESTION 20

Refer to the exhibits, which show the configuration on FortiGate and partial session information.


```

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

```

```

FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 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=log may_dirty npu f00
statistic (bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
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)
src_mac=b4:f7a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:

```

All traffic to the Internet currently egresses from `port1`. The exhibit shows partial session information for Internet traffic from a user on the internal network.

If the priority on route ID 1 were changes from 5 to 20, what would happen to traffic matching that user session?

- A. The session would remain in the session table, and its traffic would still egress from `port1`.
- B. The session would be deleted, and the client would need to start a new session.

- C. The session would remain in the session table, and its traffic would start to egress from port2.
 D. The session would remain in the session table, but its traffic would now egress from both port1 and port2.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD40943>

Description

This article provides detail about Routing Changes with existing SNAT sessions on a FortiGate.

When troubleshooting if after a routing change (For instance, setting up a VPN with corresponding added routes) a session for a particular communication goes via the wrong interface and/or firewall policy, it is probably due to keepalive traffic. The result is that sessions do not expire and by default the FortiGate does not flush routing information for those sessions.

Solution

1. Routing Changes without Source NAT (SNAT)

After a routing change, routing information is flushed from the affected sessions where source NAT (SNAT) is not applied.

- Routing lookups are done again for the next packets.
- Route cache entries are removed.
- RPF check is done again for the first packet in the original direction.
- Session is flagged as dirty.

QUESTION 21

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 scokflag=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
origin-> sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=poat 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, which statement about the output is true? A.

This session cannot be synced with the secondary device.

- B. This session is for HA talk traffic.
- C. The inspection of this session has been offloaded to the secondary device.
- D. The master unit is processing this traffic

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

Refer to the exhibit, which shows the output of `diagnose sys session stat`.

```
NGFW-1 # diagnose sys session stat
misc info:      session_count=591 setup_rate=0 exp_count=0 clash=
memory_tension_drop=0 ephemeral=0/65536 removable=0
delete=0, flush=0, dev_down=0/0
TCP session:
  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
praw733771
```

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

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

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
. . .
prw733771
```

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

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Only the source/destination pairs within the same VRF will be able to ping each other.

QUESTION 24

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


```

ike 0:253000:27: responder: main mode get 1st message
ike 0:253000:27: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:253000:27: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:253000:27: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:253000:27: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:253000:27: incoming proposal:
ike 0:253000:27: proposal id = 0:
ike 0:253000:27:   protocol id = ISAKMP:
ike 0:253000:27:   trans_id = KEY_IKE.
ike 0:253000:27:   encapsulation = IKE/none
ike 0:253000:27:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:253000:27:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:253000:27:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:253000:27:   type=OAKLEY_GROUP, val=MODP1536.
ike 0:253000:27: ISAKMP SA lifetime=86400
ike 0:253000:27: my proposal, gw Remotesite:
ike 0:253000:27: proposal id = 1:
ike 0:253000:27:   protocol id = ISAKMP:
ike 0:253000:27:   trans_id = KEY_IKE.
ike 0:253000:27:   encapsulation = IKE/none
ike 0:253000:27:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:253000:27:   type=OAKLEY_HASH_ALG, val=SHA.
ike 0:253000:27:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:253000:27:   type=OAKLEY_GROUP, val=MODP1536.
ike 0:253000:27: ISAKMP SA lifetime=86400
ike 0:253000:27: negotiation failure
ike Negot:253a8cbe6335e6fd/0000000000000000:27: no SA proposal chosen

```

Why did the tunnel *not* come up?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

ISAKMP negotiation failed, which is a phase 1 function.

QUESTION 25 How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortimanager/6.0.6/cli-reference/330471/fds-setting#fds-setting>

fds-setting

Use this command to set FDS settings.

Syntax

```
config fmupdate fds-setting
  set fds-clt-ssl-protocol {sslsv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}
  set fds-ssl-protocol {sslsv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}
  set fmtr-log {alert | critical | debug | disable | emergency | error |
    info | notice | warn}
  set linkd-log {alert | critical | debug | disable | emergency | error |
    info | notice | warn}
  set max-av-ips-version <integer>
  set max-work <integer>
  set send_report {enable | disable}
  set send_setup {enable | disable}
  set system-support-faz {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
  set system-support-fct {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
  set system-support-fgt {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
  set system-support-fml {4.x | 5.x}
  set system-support-fsa {1.x | 2.x}
  set system-support-fsw {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
  set umsvc-log {alert | critical | debug | disable | emergency | error |
    info | notice | warn}
  set unreg-dev-option {add-service | ignore | svc-only}
  set User-Agent <text>
end
```

QUESTION 26

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
Request 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
. . .

Cache Statistics:
=====
Maximum memory      :
Memory usage       :
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%
```

VCEUp

Which statement explains why the cache statistics are all zeros?

- A. The FortiGuard web filter cache is disabled in the FortiGate configuration.
- B. There are no users making web requests.
- C. FortiGate is using flow-based inspection, which does not use the cache.
- D. The administrator has reallocated the cache memory to a separate process.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/406127/filtering>

Web Filter Cache	Enable/disable web filter cache, and set the amount of time that the FortiGate will store a blocked IP address or URL locally. After the time expires, the FortiGate contacts the FDN to verify the address.
Anti-Spam Cache	Enable/disable email filter cache, and set the amount of time that the FortiGate will store an email address locally.
FortiGuard Filtering Protocol	Select the protocol for contacting the FortiGuard servers.
FortiGuard Filtering Port	Select the port assignments for contacting the FortiGuard servers.
Filtering Service Availability	The status of the filtering service. Click <i>Check Again</i> if the filtering service is not available.
Request re-evaluation of a URL's category	Click to re-evaluate a URL category rating on the FortiGuard web filter service.

praw733771

QUESTION 27 What does the `dirty` flag mean in a FortiGate session?

- A. The next packet must be re-evaluated against the firewall policies.
- B. Traffic has been identified as coming from an application that is not allowed.
- C. Traffic has been blocked by the antivirus inspection.
- D. The session must be removed from the former primary unit after an HA failover.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://kb.fortinet.com/kb/viewContent.do?externalId=FD40119&sliceId=1>

Solution

Firewall-session-dirty is a mechanism to make sure that active sessions always stay relevant. There are two distinct behaviors that would cause an active session to be validate in totally difference ways.

Available options

check-all: Flush all sessions and evaluate them anew. This is the default setting.

check-new: Keep existing sessions and check new connections only. This reduces CPU load and the possibility of packet loss.

check-policy-option: Use the option selected in the firewall-session-dirty field of the firewall policy.

Configuration

```
config system settings
set firewall-session-dirty { check-all | check-new | check-policy-option }
end
```

praw733771

QUESTION 28 An administrator wants to capture ESP traffic between two Fortigate devices using the built-in sniffer.

If the administrator knows that there is no NAT device located between both FortiGate devices, which command should the administrator run?

- A. diagnose sniffer packet any 'esp'
- B. diagnose sniffer packet any 'udp port 4500'
- C. diagnose sniffer packet any 'tcp port 500 or tcp port 4500'
- D. diagnose sniffer packet any 'udp port 500'

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortiad/6.0.1/cli-reference/395933/diagnose-sniffer-packet>

Syntax

```
diagnose sniffer packet [{any | <interface_name>} [{none |
    '<filter_str>'} [{1 | 2 | 3} [<packets_int>]]}]
```

{any <interface_name>}	Type the name of a network interface whose packets you want to capture, such as port1, or type any to capture packets on all network interfaces. If you omit this and the following parameters for the command, the command captures all packets on all network interfaces.
{none '<filter_str>'}	Type either none to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as 'tcp port 25'. Surround the filter string in quotes (').

QUESTION 29 Which three conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

- A. OSPF peer IDs match
- B. IP addresses are in the same subnet
- C. Hello and dead intervals match
- D. OSPF IP MTUs match
- E. OSPF costs match

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

Reference: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-advanced-routing-54/Routing_OSPF/OSPF_Background_Concepts.htm#Adjacenc

For two OSPF routers to become neighbors, the following conditions must be met.

- The subnet mask used on both routers must be the same subnet.
- The subnet number derived using the subnet mask and each router's interface IP address must match.
- The Hello interval & The Dead interval must match.
- The routers must have the same OSPF area ID. If they are in different areas, they are not neighbors.
- If authentication is used, they must pass authentication checks.

If any of these parameters are different between the two routers, the routers do not become OSPF neighbors and cannot be adjacent. If the routers become neighbors, they are adjacent.

QUESTION 30

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
Memory freeable:              334 MB 11% of total
memory used + freeable threshold extreme: 2887 MB 95% of total
memory used threshold red:     2675 MB 88% of total
memory used threshold green:   2492 MB 82% of total
```

What can be concluded about the conserve mode shown in the exhibit?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.fortinetguru.com/2017/09/fortigate-conserve-mode-changes-242562-386503/>

FortiGate conserve mode changes (242562, 386503)

FortiGate conserve mode changes (242562, 386503)

The following changes were made to rework **conserve mode** and facilitate its implementation:

- Implemented CLI commands to configure **extreme**, **red**, and **green** memory usage thresholds in percentages of total RAM. Memory used is the criteria for these thresholds, and set at 95% (extreme), 88% (red) and 82% (green).
- Removed structure `av_conserve_mode`, other changes in kernel to obtain and set memory usage thresholds from the kernel
- Added conserve mode diagnostic command `diag hardware sysinfo conserve`, which displays information about memory conserve mode.
- Fixed conserve mode logs in the kernel
- Added conserve mode stats to the proxy daemon through command `diag sys proxy stats all | grep conserve_mode`

QUESTION 31 Which two conditions must be met for a static route to be active in the routing table?
(Choose two.)

- A. The link health monitor (if configured) is up.
B. The next-hop IP address is up.

- C. The outgoing interface is up.
- D. There is no other route to the same destination, with a higher distance.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/370572/configuring-link-health-monitoring>

Configuring link health monitoring

Link health monitoring measures the health of links that are connected to SD-WAN member interfaces. The FortiGate checks the status of each SD-WAN member interface that you include in a Performance SLA, by sending probing signals through each member link to a server and measuring the link quality based on latency, jitter, and packet loss.

You can configure up to two servers to test the health of SD-WAN member interfaces. This helps to ensure that if the health checks identify connectivity issues, the interface is at fault and not the server. If either server meets the link status criteria, the link is good. The FortiGate removes an interface from an SD-WAN link load balancing group if its connectivity is down.

QUESTION 32

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

```
FortiGate # get router info kernel

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

FortiGate # get router info routing-table all

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

Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-advanced-routing-54/Routing_Advanced_Static/Routing_Concepts.htm#Viewing2

Viewing the routing table in the CLI

In the CLI, you can easily view the static routing table just as in the web-based manager or you can view the full routing table.

When viewing the list of static routes using the CLI command `get router static`, it is the configured static routes that are displayed. When viewing the routing table using the CLI command `get router info routing-table all`, it is the entire routing table information that is displayed including configured and learned routes of all types. The two are different information in different formats.



If VDOMs are enabled on your FortiGate unit, all routing related CLI commands must be performed within a VDOM and not in the global context.

14W/33771

QUESTION 33

What is the `diagnose test application ipsmonitor99` command used for?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://vi4nn4network.blogspot.com/2017/11/fortigate-troubleshooting-ips-engine.html>

`#diag test application ipsmonitor`

IPS Engine Test Usage:

- 1: Display IPS engine information
- 2: Toggle IPS engine enable/disable status
- 3: Display restart log
- 4: Clear restart log
- 5: Toggle bypass status
- 6: Submit attack characteristics now
- 97: Start all IPS engines
- 98: Stop all IPS engines
- 99: Restart all IPS engines and monitor

14W/33771

QUESTION 34 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.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/327890/deploying-security-fabric>

Deploying Security Fabric

This recipe provides an example of deploying Security Fabric with three downstream FortiGates connecting to one root FortiGate. To deploy Security Fabric, you need a FortiAnalyzer running firmware version 6.2 or later.

The following shows a sample network topology of three downstream FortiGates (Accounting, Marketing, and Sales) connected to the root FortiGate (Edge).



QUESTION 35 Which two statements about an auxiliary session are true? (Choose two.)

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

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/7.0.1/administration-guide/14295/controlling-return-path-with-auxiliary-session>

Scenario 1 - Return traffic returns on the original outgoing interface

In this scenario, a session is established between port1 and port3. When the return traffic hits port3:

Auxiliary sessions disabled:

The reply to the client egresses on the original incoming interface, port1. If policy routes or SD-WAN rules are configured, the next hop gateway is applied if the output device is the same as the original incoming interface.

prw733771