Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 1

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

A. OSPF interface network types match.

B. OSPF router IDs are unique.

C. OSPF interface priority settings are unique.

D. Authentication settings match.

E. OSPF link costs match.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 2

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:      trans_id = KEY_IKE.
ike 0:624000:98:      encapsulation = IKE/none
ike 0:624000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:      trans_id = KEY_IKE.
ike 0:624000:98:      encapsulation = IKE/none
ike 0:624000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:      trans_id = KEY_IKE.
ike 0:624000:98:      encapsulation = IKE/none
iike 0:620000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:      trans_id = KEY_IKE.
ike 0:624000:98:      encapsulation = IKE/none
ike 0:624000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

The administrator does not have access to the remote gateway.

Based on the debug output, which configuration change can the administrator make to the local gateway to resolve the phase 1 negotiation error?

A. In the phase 1 network configuration, set the IKE version to 2.

B. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.

C. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.

D. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 3

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

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

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

```
# diagnose webfilter fortiguard statistics list
...
Cache Statistics:
=================
Maximum memory                  :            0
Memory usage                    :            0

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

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

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

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

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

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

A. set server-type rating under config system central-management

B. set webfilter-cache enable under config system fortiguard

C. set webfilter-force-off disable under config system fortiguard

D. set ngfw-mode policy-based under config system settings

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 4

Topic #: 1

[All NSE7_EFW-7.0 Questions]

Refer to the exhibits, which show the configuration on FortiGate and partial session information for internet traffic from a user on the internal network.

Configuration | Session

```
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
```

Configuration | Session

```
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
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

If the priority on route ID 2 were changed from 10 to 0, what would happen to traffic matching that user session?

A. The session would remain in the session table, but its traffic would now egress from both port1 and port2.

B. The session would remain in the session table, and its traffic would egress from port2.

C. The session would be deleted, and the client would need to start a new session.

D. The session would remain in the session table, and its traffic would egress from port1.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 5

Topic #: 1

[All NSE7_EFW-7.0 Questions]

Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.

Configuration | Session

```
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
```

Configuration | Session

```
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
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

An administrator would like to test session failover between the two service provider connections.

What changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

A. Configure set snat-route-change enable.

B. Change the priority of the port2 static route to 5.

C. Change the priority of the port1 static route to 11.

D. unset snat-route-change to return it to the default setting.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 6

Topic #: 1

[All NSE7_EFW-7.0 Questions]

What are two functions of automation stitches? (Choose two.)

A. Automation stitches can be configured on any FortiGate device in a Security Fabric environment.

B. An automation stitch configured to execute actions sequentially can take parameters from previous actions as input for the current action.

C. Automation stitches can be created to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.

D. An automation stitch configured to execute actions in parallel can be set to insert a specific delay between actions.

Show Suggested Answer

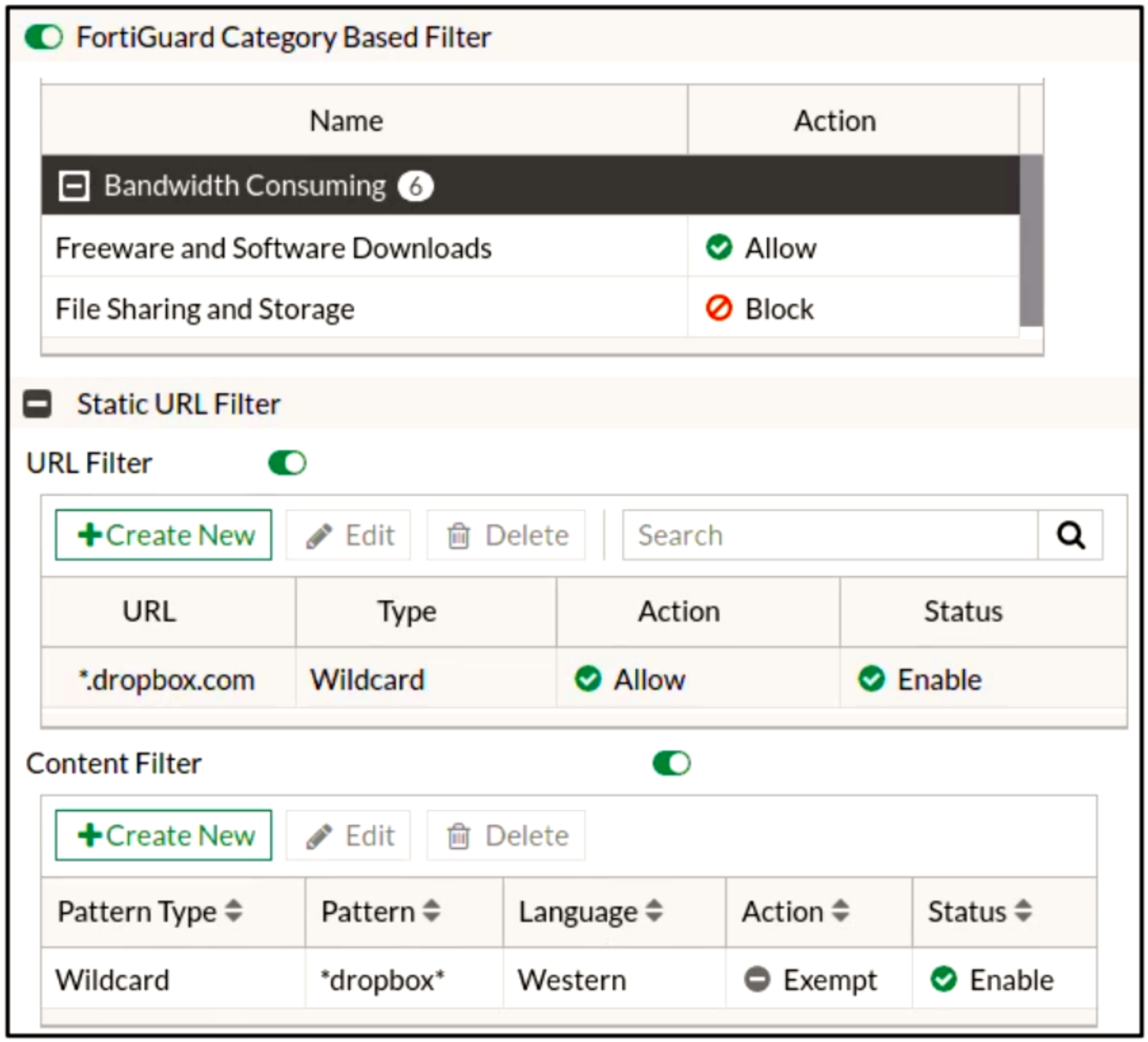
Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 7

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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



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

A. FortiGate will block the connection, based on the FortiGuard category based filter configuration.

B. FortiGate will block the connection as an invalid URL.

C. FortiGate will exempt the connection, based on the Web Content Filter configuration.

D. FortiGate will allow the connection, based onthe URL Filter configuration.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 8

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

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

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

A. The npu_flag for this tunnel is 03.

B. Different SPI values are a result of auto-negotiation being disabled for phase 2 selectors.

C. Anti-replay is enabled.

D. The npu_flag for this tunnel is 02.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 9

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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
orgin->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
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
```

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

A. FortiGate redirected the client to the captive portal to authenticate, so that a correct policy match could be made.

B. FortiGate forwarded this session without any inspection.

C. FortiGate is performing security profile inspection using the CPU.

D. FortiGate applied only IPS inspection to this session.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 10

Topic #: 1

[All NSE7_EFW-7.0 Questions]

Refer to the exhibits, which contain the partial configurations of two VPNs on FortiGate.

```
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
```

```
config vpn ipsec phase1-interface
 edit "user-2"
  set type dynamic
  set interface "port1"
  set mode main
  set xauthtype auto
  set authusrgrp "Users-2"
  set peertype any
  set dhgrp 14 15 19
  set proposal aes128-sha256 aes256-sha384
  set psksecret <encrypted_password>
next
```

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

A. Use different pre-shared keys on both VPNs.

B. Enable XAuth on both VPNs.

C. Set up specific peer IDs on both VPNs.

D. Change to aggressive mode on both VPNs.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 11

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

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

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

A. Set the priority of the static default route using port1 to 10.

B. Set the priority of the static default route using port2 to 1.

C. Set preserve-session-route to enable.

D. Set snat-route-change to enable.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 12

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

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

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

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

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

A. Configure route leaking between VRF 12 and VRF 21.

B. Disable auto-asic-offload as this is not supported between VRF instances.

C. Configure RIPv2 to exchange route information between the VRF instances.

D. Configure route leaking between port3 and port4.

E. Enable SNAT on the relevant firewall policies to prevent RPF check drops.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 13

Topic #: 1

[All NSE7_EFW-7.0 Questions]

What is the diagnose test application ipsmenitor 5 command used for?

A. To enable IPS bypass mode

B. To disable the IPS engine

C. To restart all IPS engines and monitors

D. To provide information regarding IPS sessions

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0
Question #: 14
Topic #: 1
[All NSE7_EFW-7.0 Questions]

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.
What can the administrator do to fix this problem?

A. Configure remote link monitoring to detect an issue in the forwarding path.

B. Configure set send-garp-on-failover enable under config system ha on both cluster members.

C. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports.

D. Configure set link-failed-signal enable under config system ha on both cluster members.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 15

Topic #: 1

[All NSE7_EFW-7.0 Questions]

Which statement about IKE and IKE NAT-T is true?

A. IKE is used to encapsulate ESP traffic in some situations, and IKE NAT-T is used only when the local FortiGate is using NAT on the IPsec interface.

B. IKE is the standard implementation for IKEv1 and IKE NAT-T is an extension added in IKEv2.

C. They both use UDP as their transport protocol and the port number is configurable.

D. They each use their own IP protocol number.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 16

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

```
Spoke-2 # diagnose 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 tun_id=10.200.4.1 dst_mtu=1500 dpd-
link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0 options[0210]=create_dev
frag-rfc  accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=10 olast=551 ad=/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=2
  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=10202 type=00 soft=0 mtu=1438 expire=42897/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42900/43200
  dec: spi=5ed4aaf8 esp=aes key=16 20d624b494b1c9bfe61ba9b7522448db
       ah=sha1 key=20 891cd9ba81f0e382de0d44127152cb5dba6c62d1
  enc: spi=3b574759 esp=aes key=16 3abf4e04edc09e4e88709750df9c117d
       ah=sha1 key=20 2d2618e867839866a279af5af70a64fa63a7bb52
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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

A. The remote gateway has quick mode selectors containing a destination subnet of 10.1.2.0/24.

B. The remote gateway IP is 10.200.5.1.

C. DPD is disabled.

D. Anti-replay is enabled.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 17

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

A. Only the DR receives link state information from non-DR routers.

B. Non-DR and non-BDR routers form full adjacencies to DR only.

C. Non-DR and non-BDR routers send link state updates and acknowledgements to 224.0.0.6.

D. FortiGate first checks the OSPF ID to elect a DR.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0
Question #: 18
Topic #: 1
[All NSE7_EFW-7.0 Questions]

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

A. Create a footer policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this footer policy to all other ADOMs.

B. Create a header policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this header policy to all other ADOMs.

C. Move the FortiGate devices into a single globally scoped ADOM, and merge policy packages, inserting the new firewall policies at the top.

D. Use a CLI script from the root ADOM on FortiManager to push these new policies to all FortiGate devices, through the FGFM tunnel.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 19

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

A. route-reflector enable

B. route-reflector-server enable

C. route-reflector-client enable

D. route-reflector-peer enable

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 20

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

```
FGT # get router info ospf neighbor

OSPF process 0:
Neighbor ID     Pri   State           Dead Time     Address         Interface
0.0.0.69          1   Full/DR         00:00:32      10.126.0.69     wan1
0.0.0.117         1   Full/DROther    00:00:34      10.126.0.117    wan2
0.0.0.2           1   Full/ -         00:00:38      172.16.1.2      ToRemote
```

What can be concluded from the debug command output?

A. The OSPF router with the ID 0.0.0.69 has its OSPF priority set to 0.

B. The local FortiGate has a different MTU value from the OSPF router with ID 0.0.0.2, based on the state information.

C. There are more than two OSPF routers on the wan2 network.

D. The interface ToRemote is a broadcast OSPF network.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 21

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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 do to fix the issue?

A. Increase webfilter-timeout.

B. Change protocol to TCP.

C. Enable fortiguard-anycast.

D. Disable webfilter-force-off.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 22

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

A. set av-failopen off

B. set av-failopen pass

C. set fail-open enable

D. set ips fail-open disable

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 23

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

```
# diagnose sys session list expectation

session info: proto=6 proto_state=00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=1 tunnel=/
state=new complex
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=2->4/4->2 gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0->10.200.1.1:60426(10.0.1.10:50365)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

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

A. This is a pinhole session created to allow traffic for a protocol that requires additional sessions to operate through FortiGate.

B. This is an expected session created by the IPS engine.

C. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.200.1.1.

D. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.0.1.10.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0
Question #: 24
Topic #: 1
[All NSE7_EFW-7.0 Questions]

You have configured FortiManager as a local FDS to provide FortiGate AV and IPS updates, but FortiGate devices are not receiving updates to their AV signature databases, IPS engines, or IPS signature databases.
Which two settings need to be verified for these features to function? (Choose two.)

A. FortiGate needs to have the server list entry for FortiManager set to server-type update under config system central-management.

B. FortiManager needs to be the license validation server for FortiGate devices trying to retrieve updated AV and IPS packages.

C. Service access needs to be enabled on FortiManager under System Settings > Network.

D. FortiGate needs to have include-default-servers disabled under config system central-management.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 25

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

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

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

A. In the network connected to port 4, two OSPF routers are down.

B. Based on the network type of port 4, OSPF hello packets will be sent to 224.0.0.5.

C. Based on the network type of port 4, OSPF hello packets will be sent to 224.0.0.6.

D. There are a total of 5 OSPF routers attached to the Port4 network segment.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 26

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

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

Routing table for VRF=0
S       0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S    *> 0.0.0.0/0 [10/0] via 100.64.1.254, port1

FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.64.1.254, port1
```

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

A. The port2 interface is disabled in the FortiGate configuration.

B. The port1 default route has a lower distance than the default route using port2.

C. The port1 default route has a higher priority value than the default route using port2.

D. The port1 default route has a lower priority value than the default route using port2.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 27

Topic #: 1

[All NSE7_EFW-7.0 Questions]

In which two ways does FortiManager function when it is deployed as a local FDS? (Choose two.)

A. It provides VM license validation services.

B. It supports rating requests from non-FortiGate devices.

C. It caches available firmware updates for unmanaged devices.

D. It can be configured as an update server, a rating server, or both.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 28

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

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

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

A. FortiGate is currently blocking all new sessions regardless of the content inspection requirements or configuration settings due to high memory use.

B. FortiGate is currently allowing new sessions that require flow-based or proxy-based content inspection but is not performing inspection on those sessions.

C. FortiGate is currently blocking new sessions that require flow-based or proxy-based content inspection.

D. FortiGate is currently allowing new sessions that require flow-based content inspection and blocking sessions that require proxy-based content inspection.

Show Suggested Answer

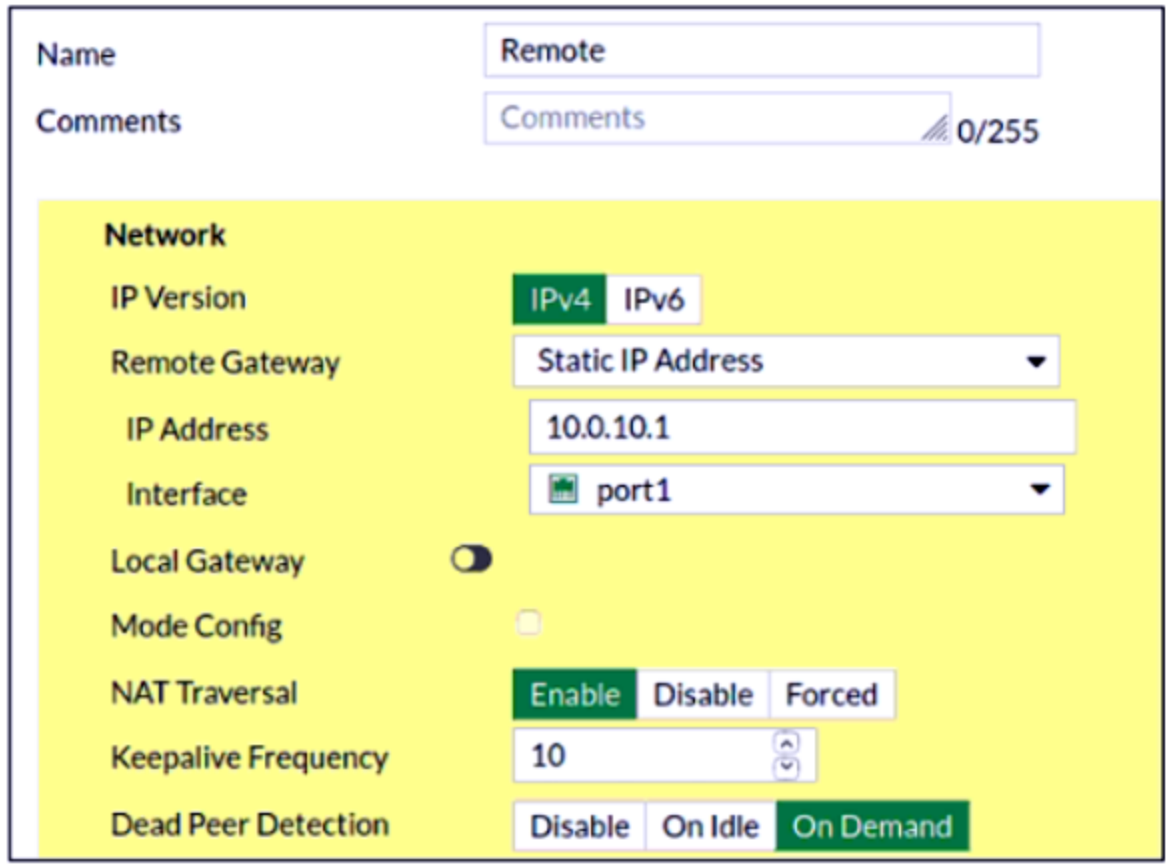
Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 29

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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



The VPN is not up. To diagnose the issue, the administrator enters the following CLI commands to an SSH session on FortiGate: diagnose vpn ike log-filter dst-addr4 10.0.10.1 diagnose debug application ike -1

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

A. The administrator must also run the command diagnose debug enable.

B. The administrator must enable the following real-time debug: diagnose debug application ipsec -1.

C. The log-filter setting is incorrect. The VPN traffic does not match this filter.

D. The debug shows only error messages. If there is no output, then the phase 1 and phase 2 configurations match.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 30

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500,ifindex=7....
ike 0: IKEv1 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=426
ike 0:Remotesite:3: initiator: aggressive mode get 1st response...
ike 0:Remotesite:3: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:Remotesite:3: DPD negotiated
ike 0:Remotesite:3: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:Remotesite:3: peer is FortiGate/FortiOS (v0 b0)
ike 0:Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:Remotesite:3: received peer identifier FQDN 'remote'
ike 0:Remotesite:3: negotiation result
ike 0:Remotesite:3: proposal id = 1:
ike 0:Remotesite:3:   protocol id = ISAKMP:
ike 0:Remotesite:3:     trans_id = KEY_IKE.
ike 0:Remotesite:3:     encapsulation = IKE/none
ike 0:Remotesite:3:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:Remotesite:3:       type=OAKLEY_HASH_ALG, val=SHA.
ike 0:Remotesite:3:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:Remotesite:3:       type=OAKLEY_GROUP, val=MODP1024.
ike 0:Remotesite:3: ISAKMP SA lifetime=86400
ike 0:Remotesite:3: NAT-T unavailable
ike 0:Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key 16:39915120ED73E520787C801DE3678916
ike 0:Remotesite:3: PSK authentication succeeded
ike 0:Remotesite:3: authentication OK
ike 0:Remotesite:3: add INITIAL-CONTACT
ike 0:Remotesite:3: enc A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A078E09026CA8B2
ike 0:Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF68208100401000000000000005C64D5CBA90B873F150CB8B5CC2A
ike 0:Remotesite:3: sent IKE msg (agg_i2send): 10.0.0.1:500->10.0.0.2:500, len=140, id=a2fbd6bb6394401a/
ike 0:Remotesite:3: established IKE SA a2fbd6bb6394401a/06b89c022d4df682
```

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

A. The initiator provided remote as its IPsec peer ID.

B. It shows a phase 2 negotiation.

C. Perfect Forward Secrecy (PFS) is enabled in the configuration.

D. The local gateway IP address is 10.0.0.1.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 31

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

A. With the auxiliary session setting disabled, only auxiliary sessions are offloaded.

B. With the auxiliary session setting enabled, two sessions are created in case of routing change.

C. With the auxiliary session setting enabled, ECMP traffic is accelerated to the NP6 processor.

D. With the auxiliary session setting disabled, for each traffic path, FortiGate uses the same auxiliary session.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 32

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

A. Set protected network to all

B. Enable AD-VPN in IPsec phase 1

C. Configure IP addresses on IPsec virtual interfaces

D. Disable add-route on hub

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 33

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

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

What can you conclude from the RTT value?

A. Its value represents the time it takes to receive a response after a rating request is sent to a particular server.

B. Its value is incremented with each packet lost.

C. It determines which FortiGuard server is used for license validation.

D. Its initial value is statically set to 10.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 34

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

A. FortiGate uses the CN information from the Subject field in the server certificate.

B. FortiGate uses the first entry listed in the SAN field in the server certificate.

C. FortiGate uses the SNI from the user's web browser.

D. FortiGate closes the connection because this represents an invalid SSL/TLS configuration.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 35

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

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

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

Total number of neighbors 3
```

What can be concluded about the router in this scenario?

A. The router 100.64.3.1 needs to update the local AS number in its BGP configuration in order to bring up the BGP session with the local router.

B. The State/PfxRcd for neighbor 100.64.3.1 will not change until an administrator on the local router adjusts the inbound route filtering so that prefixes received can be added to the RIB.

C. All of the neighbors displayed are part of a single BGP configuration on the local router with the neighbor-range set to a value of 4.

D. The BGP session with peer 10.127.0.75 is up.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 36

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

A. When run on the All FortiGate in ADOM, changes are automatically installed without the creation of a new revision history.

B. When run on the Device Database, changes are applied directly to the managed FortiGate device.

C. When run on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

D. When run on the Policy Package, ADOM database, you must use the installation wizard to apply the changes to the managed FortiGate device.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 37

Topic #: 1

[All NSE7_EFW-7.0 Questions]

Which two tasks are automated using the Import Configuration wizard on FortiManager? (Choose two.)

A. Importing firewall address objects from managed devices

B. Importing interface mappings from managed devices

C. Importing static and dynamic route configurations from managed devices

D. Importing devices to FortiManager

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 38

Topic #: 1

[All NSE7_EFW-7.0 Questions]

Which statement about protocol options is true?

A. Protocol options allows administrators a streamlined method to instruct FortiGate to block all sessions corresponding to disabled protocols.

B. Protocol options allows administrators the ability to configure the Any setting for all enabled protocols which provides the most efficient use of system resources.

C. Protocol options allow administrators to configure a maximum number of sessions for each configured protocol.

D. Protocol options allows administrators to configure which Layer 4 port numbers map to upper-layer protocols, such as HTTP, SMTP, FTP, and so on.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0
Question #: 39
Topic #: 1
[All NSE7_EFW-7.0 Questions]

An administrator has created a VPN community within VPN Manager on FortiManager. They also added gateways to the VPN community and are now trying to create firewall policies to permit traffic over the tunnel; however, the VPN interfaces are not listed as available options.
What step must the administrator take to resolve this issue?

A. Install the VPN community and gateway configuration to the FortiGate devices, in order for the interfaces to be displayed within Policy & Objects on FortiManager

B. Set up all of the phase 1 settings in the VPN community that they neglected to set up initially. The interfaces will be automatically generated after the administrator configures all of the required settings.

C. Refresh the device status from the Device Manager so that FortiGate will populate the IPsec interfaces.

D. Create interface mappings for the IPsec VPN interfaces, before they can be used in a policy.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-7.0

Question #: 40

Topic #: 1

[All NSE7_EFW-7.0 Questions]

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

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

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

A. Servers with a negative TZ value are less preferred for rating requests.

B. There is a natural correlation between the value in the Packets field and the value in the Weight field.

C. FortiGate used 64.26.151.37 as the initial server to validate its contract.

D. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.

Show Suggested Answer