Fortinet

Exam Questions NSE7_EFW-7.2

Fortinet NSE 7 - Enterprise Firewall 7.2

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

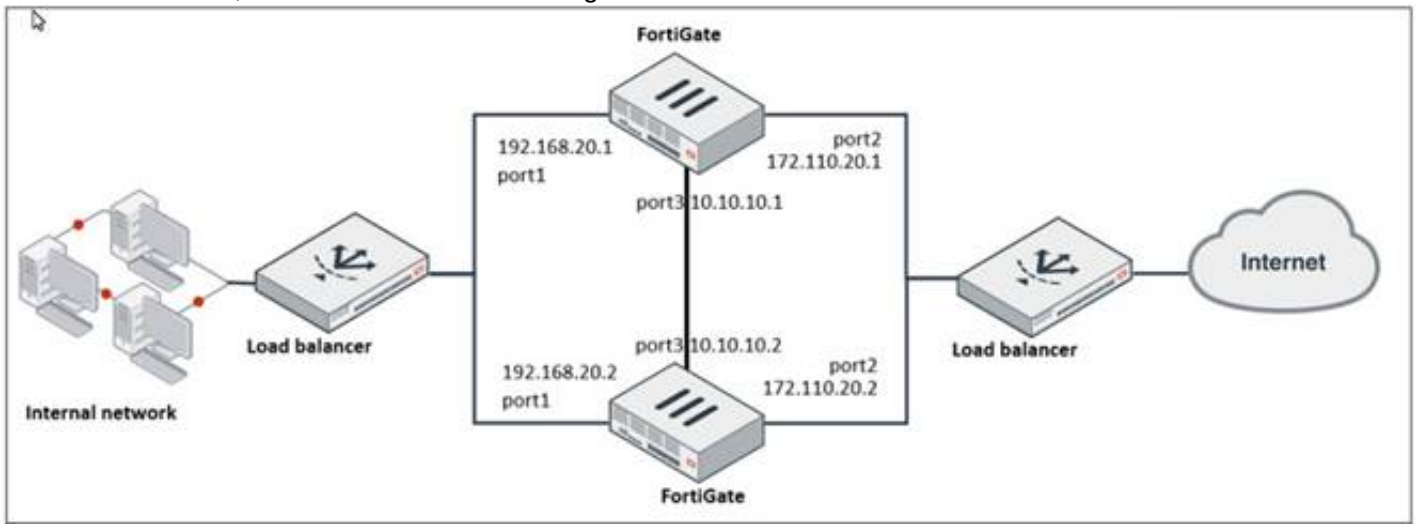
* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Refer to the exhibit, which shows a network diagram.



Which protocol should you use to configure the FortiGate cluster?

A. FGCP in active-passive mode
B. OFGSP
C. VRRP
D. FGCP in active-active mode

Answer: A

Explanation:
Given the network diagram and the presence of two FortiGate devices, the Fortinet Gate Clustering Protocol (FGCP) in active-passive mode is the most appropriate for setting up a FortiGate cluster. FGCP supports high availability configurations and is designed to allow one FortiGate to seamlessly take over if the other fails, providing continuous network availability. This is supported by Fortinet documentation for high availability configurations using FGCP.

NEW QUESTION 2
Exhibit.

```
Routing table for VRF=0
S*      0.0.0.0/0 [20/0] via 100.64.1.254 (recursive is directly connected, port1), 00:03:58, [1/0]
C       10.1.0.0/24 is directly connected, port3
S       10.1.1.0/24 [200/0] via 172.16.1.2 (recursive is directly connected, tunnel_0), 00:03:25, [1/0]
S       10.1.2.0/24 [200/0] via 172.16.1.3 (recursive is directly connected, tunnel_1), 00:03:21, [1/0]
O       10.1.4.0/24 [110/2] via 10.1.0.100, port3, 00:04:56, [1/0]
O       10.1.10.0/24 [110/2] via 10.1.0.1, port3, 00:04:56, [1/0]
C       100.64.1.0/24 is directly connected, port1
C       100.64.2.0/24 is directly connected, port2
C       172.16.1.1/32 is directly connected, tunnel_0
                      is directly connected, tunnel_1
C       172.16.1.2/32 is directly connected, tunnel_0
C       172.16.1.3/32 is directly connected, tunnel_1
C       172.16.100.0/24 is directly connected, port8
```

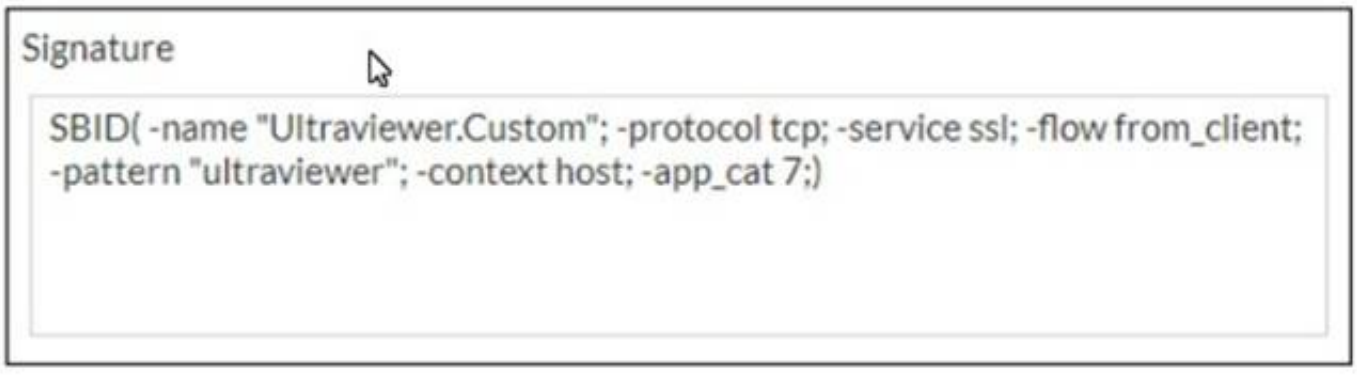
Refer to the exhibit, which shows a partial touting table
What two concisions can you draw from the corresponding FortiGate configuration? (Choose two.)

A. IPSec Tunnel aggregation is configured
B. net-device is enabled in the tunnel IPSec phase 1 configuration
C. OSPI is configured to run over IPSec.
D. add-route is disabled in the tunnel IPSec phase 1 configuration.

Answer: BD

Explanation:
? Option B is correct because the routing table shows that the tunnel interfaces have a netmask of 255.255.255.255, which indicates that net-device is enabled in the phase 1 configuration. This option allows the FortiGate to use the tunnel interface as a next-hop for routing, without adding a route to the phase 2 destination1.
? Option D is correct because the routing table does not show any routes to the phase 2 destination networks, which indicates that add-route is disabled in the phase 1 configuration. This option controls whether the FortiGate adds a static route to the phase 2 destination network using the tunnel interface as the gateway2.
? Option A is incorrect because IPSec tunnel aggregation is a feature that allows multiple phase 2 selectors to share a single phase 1 tunnel, reducing the number of tunnels and improving performance3. This feature is not related to the routing table or the phase 1 configuration.
? Option C is incorrect because OSPF is a dynamic routing protocol that can run over IPSec tunnels, but it requires additional configuration on the FortiGate and the peer device4. This option is not related to the routing table or the phase 1 configuration. References: =
? 1: Technical Tip: ‘set net-device’ new route-based IPsec logic2
? 2: Adding a static route5
? 3: IPSec VPN concepts6
? 4: Dynamic routing over IPsec VPN7

NEW QUESTION 3
Refer to the exhibit, which shows a custom signature.



Which two modifications must you apply to the configuration of this custom signature so that you can save it on FortiGate? (Choose two.)

A. Add severity.
B. Add attack_id.
C. Ensure that the header syntax is F-SBID.
D. Start options with --.

Answer: AB

Explanation:
For a custom signature to be valid and savable on a FortiGate device, it must include certain mandatory fields. Severity is used to specify the level of threat that the signature represents, and attack_id is a unique identifier for the signature. Without these, the signature would not be complete and could not be correctly utilized by the FortiGate's Intrusion Prevention System (IPS).

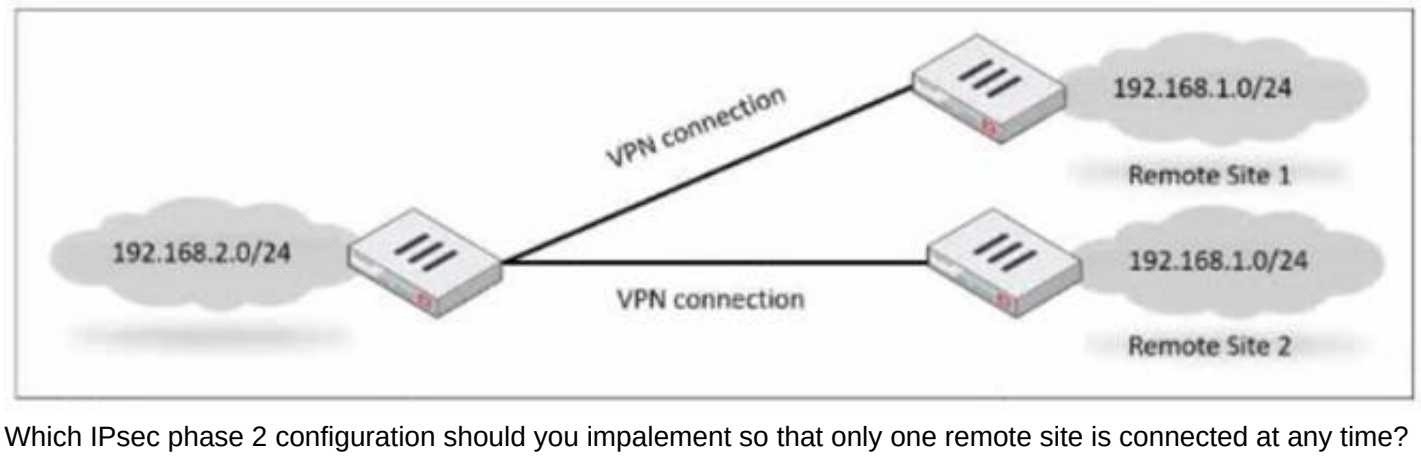
NEW QUESTION 4
Which two statements about the neighbor-group command are true? (Choose two.)

A. You can configure it on the GUI.
B. It applies common settings in an OSPF area.
C. It is combined with the neighbor-range parameter.
D. You can apply it in Internal BGP (IBGP) and External BGP (EBGP).

Answer: BD

Explanation:
The neighbor-group command in FortiOS allows for the application of common settings to a group of neighbors in OSPF, and can also be used to simplify configuration by applyingcommon settings to both IBGP and EBGP neighbors. This grouping functionality is a part of the FortiOS CLI and is documented in the Fortinet CLI reference.

NEW QUESTION 5
Refer to the exhibit, which shows a network diagram.



Which IPsec phase 2 configuration should you impalement so that only one remote site is connected at any time?

A. Set route-overlap to allow.
B. Set single-source to enable
C. Set route-overlap to either use—new or use-old
D. Set net-device to enable

Answer: C

Explanation:
To ensure that only one remote site is connected at any given time in an
IPsec VPN scenario, you should useroute-overlapwith the option to either use-new or use- old. This setting dictates which routes are preferred and how overlaps in routes are handled, allowing for one connection to take precedence over the other (C).
References:
? FortiOS Handbook - IPsec VPN

NEW QUESTION 6
Refer to the exhibit, which contains information about an IPsec VPN tunnel.

```
FortiGate # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=tunnel_0 ver=2 serial=1 100.64.3.1:0->100.64.1.1:0 tun_id=100.64.1.1 tun_id6=::100.64.1.1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_s

proxyid_num=1 child_num=0 refcnt=3 ilast=42949917 olast=42949917 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=off on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=tunnel_0_0 proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=30202 type=00 soft=0 mtu=1280 expire=1454/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=192 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=1768/1800
  dec: spi=877d6590 esp=aes key=16 be308ec1fb05464205764424bc40a76d
       ah=sha256 key=32 cc8894be3390983521a48b2e7a5c998e6b28a10a3ddd8e7bc7ecbe672dfe7cc5
  enc: spi=63d0f38a esp=aes key=16 d8d3343af2fed4ddd958a022cd656b06
       ah=sha256 key=32 264402ba8ad04a7e97732b52ec27c92ff86e0a97bb33e22887677336f1670c7d
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=100.64.1.1 npu_lgwy=100.64.3.1 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

What two conclusions can you draw from the command output? (Choose two.)

A. Dead peer detection is set to enable.
B. The IKE version is 2.
C. Both IPsec SAs are loaded on the kernel.
D. Forward error correction in phase 2 is set to enable.

Answer: BC

Explanation:
From the command output shown in the exhibit:
* B. The IKE version is 2: This can be deduced from the presence of 'ver=2' in the output, which indicates that IKEv2 is being used.
* C. Both IPsec SAs are loaded on the kernel: This is indicated by the line 'npu flags=0x0/0', suggesting that no offload to NPU is occurring, and hence, both Security Associations are
loaded onto the kernel for processing.
Fortinet documentation specifies that the version of IKE (Internet Key Exchange) used and the loading of IPsec Security Associations can be verified through the diagnostic commands related to VPN tunnels.

NEW QUESTION 7
You want to block access to the website ww.eicar.org using a custom IPS signature. Which custom IPS signature should you configure?
A)

```
F-SBID( --name "eicar"; --protocol udp; --flow from_server; --pattern "eicar"; --context host;)
```

B)

```
F-SBID( --name "detect_eicar"; --protocol udp; --service ssl; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)
```

C)

```
F-SBID( --name "detect_eicar"; --protocol tcp; --service dns; --flow from_server; --pattern "eicar"; --no_case;)
```

D)

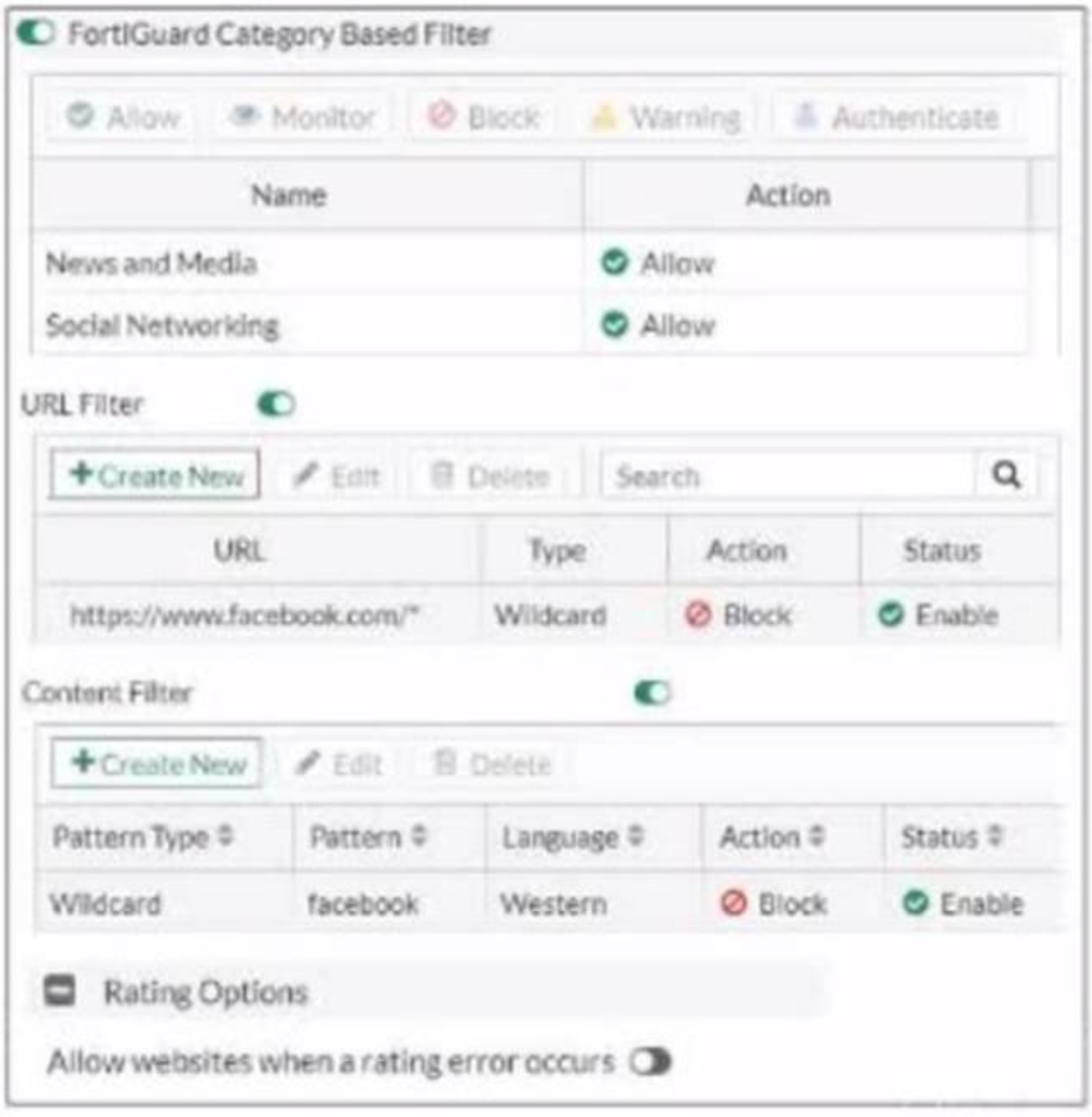
```
F-SBID( --name "eicar"; --protocol tcp; --service HTTP; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

Explanation:
Option D is the correct answer because it specifically blocks access to the website “www.eicar.org” using TCP protocol and HTTP service, which are commonly used for web browsing. The other options either use the wrong protocol (UDP), the wrong service (DNS or SSL), or the wrong pattern (“eicar” instead of “www.eicar.org”). References := Configuring custom signatures | FortiGate / FortiOS 7.4.0 - Fortinet Document Library, section “Signature to block access to example.com”.

NEW QUESTION 8
Exhibit.



Refer to the exhibit, which shows a partial web filter profile conjuration
What can you cone udo from this configuration about access towww.facebook, com, which is categorized as Social Networking?

A. The access is blocked based on the Content Filter configuration
B. The access is allowed based on the FortiGuard Category Based Filter configuration
C. The access is blocked based on the URL Filter configuration
D. The access is hocked if the local or the public FortiGuard server does not reply

Answer: C

Explanation:
The access to www.facebook.com is blocked based on the URL Filter configuration. In the exhibit, it shows that the URL “www.facebook.com” is specifically set to “Block” under the URL Filter section1. References := Fortigate: How to configure Web Filter function on Fortigate, Web filter | FortiGate / FortiOS 7.0.2 | Fortinet Document Library, FortiGate HTTPS web URL filtering … - Fortinet … - Fortinet Community

NEW QUESTION 9
Which two statements about the BFD parameter in BGP are true? (Choose two.)

A. It allows failure detection in less than one second.
B. The two routers must be connected to the same subnet.
C. It is supported for neighbors over multiple hops.
D. It detects only two-way failures.

Answer: AC

Explanation:
Bidirectional Forwarding Detection (BFD) is a rapid protocol for detecting failures in the forwarding path between two adjacent routers, including interfaces, data links, and forwarding planes. BFD is designed to detect forwarding path failures in a very short amount of time, often less than one second, which is significantly faster than traditional failure detection mechanisms like hold-down timers in routing protocols.
Fortinet supports BFD for BGP, and it can be used over multiple hops, which allows the detection of failures even if the BGP peers are not directly connected. This functionality enhances the ability to maintain stable BGP sessions over a wider network topology and is documented in Fortinet's guides.

NEW QUESTION 10
Exhibit.

```
# get router info bgp neighbors
VRF 0 neighbor table:
BGP neighbor is 10.2.0.254, remote AS 65100, local AS 65200, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Not directly connected EBGP
  Last read 00:04:40, hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 180, keepalive interval is 60 seconds
  Received 5 messages, 0 notifications, 0 in queue
  Sent 4 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  NLRI treated as withdraw: 0
  Minimum time between advertisement runs is 30 seconds…
```

Refer to the exhibit, which provides information on BGP neighbors. Which can you conclude from this command output?

A. The router are in the number to match the remote peer.
B. You must change the AS number to match the remote peer.
C. BGP is attempting to establish a TCP connection with the BGP peer.
D. The bfd configuration to set to enable.

Answer: C

Explanation:
The BGP state is “Idle”, indicating that BGP is attempting to establish a TCP connection with the peer. This is the first state in the BGP finite state machine, and it means that no TCP connection has been established yet. If the TCP connection fails, the BGP state will reset to either active or idle, depending on the configuration. References: You can find more information about BGP states and troubleshooting in the following Fortinet Enterprise Firewall 7.2 documents:
? Troubleshooting BGP
? How BGP works

NEW QUESTION 10
Which ADVPN configuration must be configured using a script on fortiManager, when using VPN Manager to manage fortiGate VPN tunnels?

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

Answer: A

Explanation:
To enable AD-VPN, you need to edit an SD-WAN overlay template and enable the Auto-Discovery VPN toggle. This will automatically add the required settings to the IPsec template and the BGP template. You cannot enable AD-VPN directly in the IPsec phase 1 settings using VPN Manager. References := ADVPN | FortiManager 7.2.0 - Fortinet Documentation

NEW QUESTION 15
Which two statements about IKE vision 2 are true? (Choose two.)

A. Phase 1 includes main mode
B. It supports the extensible authentication protocol (EAP)
C. It supports the XAuth protocol.
D. It exchanges a minimum of four messages to establish a secure tunnel

Answer: BD

Explanation:
IKE version 2 supports the extensible authentication protocol (EAP), which allows for more flexible and secure authentication methods1. IKE version 2 also exchanges a minimum of four messages toestablish a secure tunnel, which is more efficient than IKE version 12. References: = IKE settings | FortiClient 7.2.2 - Fortinet
Documentation, Technical Tip: How to configure IKE version 1 or 2 … - Fortinet Community

NEW QUESTION 19
Refer to the exhibit, which shows the output of a BGP summary.

```
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 two conclusions can you draw from this BGP summary? (Choose two.)

A. External BGP (EBGP) exchanges routing information.
B. The BGP session with peer 10. 127. 0. 75 is established.
C. The router 100. 64. 3. 1 has the parameter bfd set to enable.

D. The neighbors displayed are linked to a local router with the neighbor-range set to a value of 4.

Answer: AB

Explanation:
The output of the BGP (Border Gateway Protocol) summary shows details about the BGP neighbors of a router, their Autonomous System (AS) numbers, the state of the BGP session, and other metrics like messages received and sent.
From the BGP summary provided:
* A.External BGP (EBGP) exchanges routing information.This conclusion can be inferred because the AS numbers for the neighbors are different from the local AS number (65117), which suggests that these are external connections.
* B.The BGP session with peer 10.127.0.75 is established.This is indicated by the state/prefix received column showing a numeric value (1), which typically means that the session is established and a number of prefixes has been received.
* C.The router 100.64.3.1 has the parameter bfd set to enable.This cannot be concluded directly from the summary without additional context or commands specifically showing
BFD (Bidirectional Forwarding Detection) configuration.
* D.The neighbors displayed are linked to a local router with the neighbor-range set to a value of 4.The neighbor-range concept does not apply here; the value 4 in the 'V' column stands for the BGP version number, which is typically 4.

NEW QUESTION 22
Which two statements about ADVPN are true? (Choose two.)

A. You must disable add-route in the hub.
B. AllFortiGate devices must be in the same autonomous system (AS).
C. The hub adds routes based on IKE negotiations.
D. You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0.

Answer: CD

Explanation:
C. The hub adds routes based on IKE negotiations: This is part of the ADVPN functionality where the hub learns about the networks behind the spokes and can add routes dynamically based on the IKE negotiations with the spokes.
* D. You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0: This wildcard
setting in the phase 2 selectors allows any-to-any tunnel establishment, which is necessary for the dynamic creation of spoke-to-spoke tunnels.
These configurations are outlined in Fortinet's documentation for setting up ADVPN, where the hub's role in route control and the use of wildcard selectors for phase 2 are emphasized to enable dynamic tunneling betwen spokes.

NEW QUESTION 24
Which statement about network processor (NP) offloading is true?

A. For TCP traffic FortiGate CPU offloads the first packets of SYN/ACK and ACK of the three-way handshake to NP
B. The NP provides IPS signature matching
C. You can disable the NP for each firewall policy using the command np-acceleration st to loose.
D. The NP checks the session key or IPSec SA

Answer: B

Explanation:
Network processors (NPs) are specialized hardware within FortiGate devices that accelerate certain security functions. One of the primary functions of NPs is to provide IPS signature matching (B), allowing for high-speed inspection of traffic against a database of known threat signatures.

NEW QUESTION 26
Exhibit.

```
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
```

Refer to exhibit, which shows a central management configuration
Which server will FortiGate choose for web filler rating requests if 10.0.1.240 is experiencing an outage?

A. Public FortiGuard servers
B. 10.0.1.242
C. 10.0.1.244
D. 10.0.1.243

Answer: C

Explanation:
In the event of an outage at 10.0.1.240, the FortiGate will choose the next server in the sequence for web filter rating requests, which is 10.0.1.244 according to the configuration shown in the exhibit. This is because the server list is ordered by priority, and the server with the lowest priority number is chosen first. If that server is unavailable, the next server with the next lowest priority number is chosen, and so on. The public FortiGuard servers are only used if the include-default-servers option is enabled and all the custom servers are unavailable. References := Fortinet Enterprise Firewall Study Guide for FortiOS 7.2, page 132.

NEW QUESTION 29
Refer to the exhibit, which contains a partial BGP combination.

```
config router bgp
    set as 65200
    set router-id 172.16.1.254
    config neighbor
        edit 100.64.1.254
            set remote-as 65100
        next
    end
end
```

You want to configure a loopback as the OGP source.
Which two parameters must you set in the BGP configuration? (Choose two)

A. ebgp-enforce-multihop
B. recursive-next-hop
C. ibgp-enfoce-multihop
D. update-source

Answer: AD

Explanation:
To configure a loopback as the BGP source, you need to set the “ebgp- enforce-multihop” and “update-source” parameters in the BGP configuration. The “ebgp-

enforce-multihop" allows EBGP connections to neighbor routers that are not directly connected, while "update-source" specifies the IP address that should be used for the BGP
session1. References := BGP on loopback, Loopback interface, Technical Tip: Configuring EBGP Multihop Load-Balancing, Technical Tip: BGP routes are not installed in routing
table with loopback as update source

NEW QUESTION 34
Refer to the exhibit, which shows a routing table.

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.1.0.254	port1	10	Static
10.1.0.0/24	0.0.0.0	port1	0	Connected
10.1.4.0/24	10.1.0.100	port1	110	OSPF
10.1.10.0/24	0.0.0.0	port2	0	Connected
172.16.100.0/24	0.0.0.0	port3	0	Connected

What two options can you configure in OSPF to block the advertisement of the 10.1.10.0 prefix? (Choose two.)

A. Remove the 16.1.10.C prefix from the OSPF network
B. Configure a distribute-list-out
C. Configure a route-map out
D. Disable Redistribute Connected

Answer: BC

Explanation:
To block the advertisement of the 10.1.10.0 prefix in OSPF, you can configure a distribute-list-out or a route-map out. A distribute-list-out is used to filter outgoing routing updates from being advertised to OSPF neighbors1. A route-map out can also be used for filtering and is applied to outbound routing updates2. References := Technical Tip: Inbound route filtering in OSPF usi … - Fortinet Community, OSPF | FortiGate / FortiOS 7.2.2 - Fortinet Documentation

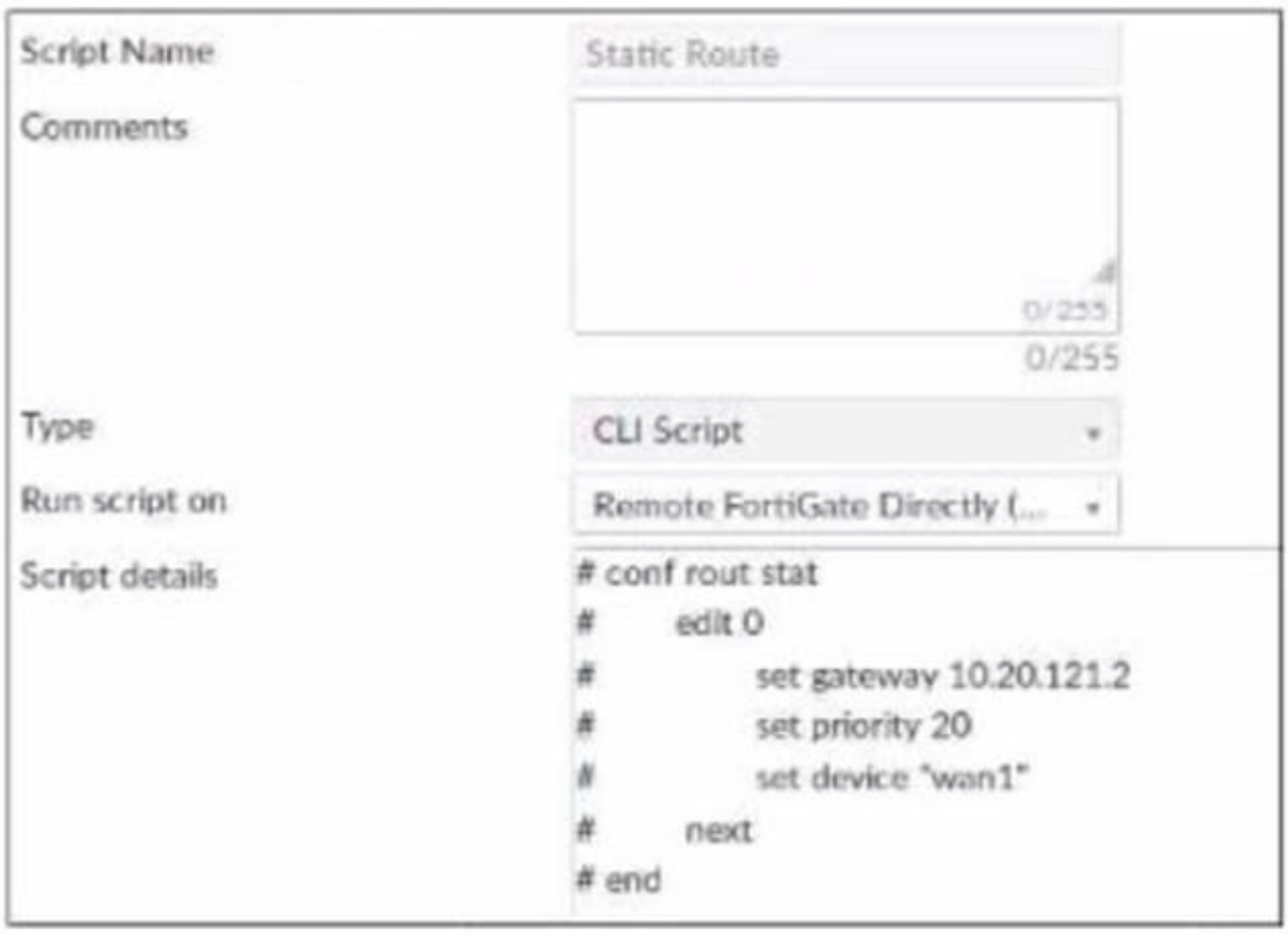
NEW QUESTION 38
Which, three conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

A. OSPF interface network types match
B. OSPF router IDs are unique
C. OSPF interface priority settings are unique
D. OSPF link costs match
E. Authentication settings match

Answer: ABE

Explanation:
? Option A is correct because the OSPF interface network types determine how the routers form adjacencies and exchange LSAs on a network segment. The network types must match for the routers to become neighbors1.
? Option B is correct because the OSPF router IDs are used to identify each router in the OSPF domain and to establish adjacencies. The router IDs must be unique for the routers to become neighbors2.
? Option E is correct because the authentication settings control how the routers authenticate each other before exchanging OSPF packets. The authentication settings must match for the routers to become neighbors3.
? Option C is incorrect because the OSPF interface priority settings are used to elect
the designated router (DR) and the backup designated router (BDR) on a broadcast or non-broadcast multi-access network. The priority settings do not have to be unique for the routers to become neighbors, but they affect the DR/BDR election process4.
? Option D is incorrect because the OSPF link costs are used to calculate the
shortest path to a destination network based on the bandwidth of the links. The link costs do not have to match for the routers to become neighbors, but they affect the routing decisions5. References: =
? 1: OSPF network types
? 2: OSPF router ID
? 3: OSPF authentication
? 4: OSPF interface priority
? 5: OSPF link cost

NEW QUESTION 43
Exhibit.



Refer to the exhibit, which contains a CLI script configuration on fortiManager. An administrator configured the CLI script on FortiManager rut the script tailed to apply any changes to the managed
device after being executed.
What are two reasons why the script did not make any changes to the managed device? (Choose two)

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

Answer: AB

Explanation:
The commands that start with the # sign did not run because they are treated as comments in the CLI script. Incomplete commands can cause CLI scripts to fail because they are not recognized by the FortiGate device. The other options are incorrect because static routes can be added using CLI or GUI, and CLI scripts do not need to start with #!. References := Configuring custom scripts | FortiManager 7.2.0 - Fortinet Documentation, section “CLI script syntax”.

NEW QUESTION 44
Refer to the exhibit, which contains a partial OSPF configuration.

```
config router ospf
    set router-id 0.0.0.3
    set restart-mode graceful-restart
    set restart-period 30
    set restart-on-topology-change enable
    ...
end
```

What can you conclude from this output?

A. Neighbors maintain communication with the restarting router.
B. The router sends grace LSAs before it restarts.
C. FortiGate restarts if the topology changes.
D. The restarting router sends gratuitous ARP for 30 seconds.

Answer: B

Explanation:
From the partial OSPF (Open Shortest Path First) configuration output:
* B. The router sends grace LSAs before it restarts: This is implied by the command 'set restart-mode graceful-restart'. When OSPF is configured with graceful restart, the router sends grace LSAs (Link State Advertisements) to inform its neighbors that it is restarting, allowing for a seamless transition without recalculating routes.
Fortinet documentation on OSPF configuration clearly states that enabling graceful restart mode allows the router to maintain its adjacencies and routes during a brief restart period.

NEW QUESTION 49

You want to improve reliability over a lossy IPSec tunnel.
Which combination of IPSec phase 1 parameters should you configure?

A. fec-ingress and fec-egress
B. Odpd and dpd-retryinterval
C. fragmentation and fragmentation-mtu
D. keepalive and keylive

Answer: C

Explanation:
For improving reliability over a lossy IPSec tunnel, the fragmentation and fragmentation-mtu parameters should be configured. In scenarios where there might be issues with packet size or an unreliable network, setting the IPsec phase 1 to allow for fragmentation will enable large packets to be broken down, preventing them from being dropped due to size or poor network quality. The fragmentation-mtu specifies the size of the fragments. This is aligned with Fortinet's recommendations for handling IPsec VPN over networks with potential packet loss or size limitations.

NEW QUESTION 52
Exhibit.

```
# diagnose webfilter fortiguard cache dump

Saving to file [/tmp/urlCache.txt]
Cache Contents:
---------------
Cache Mode:    TTL
Cache DB Ver: 23.6106

Domain   |IP        DB Ver    T URL
34000000|34000000 23.6106   P Bhttp://training.fortinet.com/
25000000|25000000 23.6106   E Bhttps://twitter.com/…

# get webfilter categories
…
g07 General Interest - Business:
     31 Finance and Banking
     …
     51 Government and Legal Organizations
     52 Information Technology
```

Refer to the exhibit, which shows the output from the webfilter fortiguard cache dump and webfilter categories commands.
Using the output, how can an administrator determine the category of the training.fortinet.comam website?

A. The administrator must convert the first three digits of the IP hex value to binary
B. The administrator can look up the hex value of 34 in the second command output.
C. The administrator must add both the Pima in and Iphex values of 34 to get the category number
D. The administrator must convert the first two digits of the Domain hex value to a decimal value

Answer: B

Explanation:
? Option B is correct because the administrator can determine the category of the training.fortinet.com website by looking up the hex value of 34 in the second command output. This is because the first command output shows that the domain and the IP of the website are both in category (Hex) 34, which corresponds to Information Technology in the second command output1.
? Option A is incorrect because the administrator does not need to convert the first three digits of the IP hex value to binary. The IP hex value is already in the same format as the category hex value, so the administrator can simply compare them without any conversion2.
? Option C is incorrect because the administrator does not need to add both the
Pima in and Iphex values of 34 to get the category number. The Pima in and Iphex values are not related to the category number, but to the cache TTL and the database version respectively3.
? Option D is incorrect because the administrator does not need to convert the first
two digits of the Domain hex value to a decimal value. The Domain hex value is already in the same format as the category hex value, so the administrator can simply compare them without any conversion2. References: =
? 1: Technical Tip: Verify the webfilter cache content4
? 2: Hexadecimal to Decimal Converter5
? 3: FortiGate - Fortinet Community6
? : Web filter | FortiGate / FortiOS 7.2.0 - Fortinet Documentation7

NEW QUESTION 56
.....

Relate Links

100% Pass Your NSE7_EFW-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/NSE7_EFW-7.2-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/