Fortinet

Exam Questions NSE7_SDW-7.2

Fortinet NSE 7 - SD-WAN 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.

```
# get router info routing-table all
...
B      10.0.2.0/24 [200/0] via 10.201.1.2 [3] (recursive via VPN0 tunnel 100.64.1.1), 00:00:54
                   [200/0] via 10.202.1.2 [3] (recursive via VPN1 tunnel 100.64.1.9), 00:00:54
                   [200/0] via 10.203.1.1 [3] (recursive via VPN2 tunnel 172.16.1.5), 00:00:54
...
```

The device exchanges routes using IBGP.
Which two statements are correct about the IBGP configuration and routing information on the device? (Choose two.)

A. Each BGP route is three hops away from the destination.
B. ibgp-multipath is disabled.
C. additional-path is enabled.
D. You can run the get router info routing-table database command to display the additional paths.

Answer: CD

NEW QUESTION 2
Refer to the exhibits.

Exhibit A

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 port1), alive, selected
    2: Seq_num(2 port2), alive, selected
  Internet Service(3): GoToMeeting(4294836966,0,0,0 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0 41468) Salesforce(4294837976,0,0,0 16920)
  Src address(1):
      10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2), alive, selected
  Internet Service(2): Facebook(4294836806,0,0,0 15832) Twitter(4294838278,0,0,0 16001)
  Src address(1):
      10.0.1.0-10.0.1.255

branch1_fgt # diagnose sys sdwan internet-service-app-ctrl-list

Facebook(15832 4294836806): 157.240.229.35 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.205.106.86 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.212.249.144 6 443 Tue Mar  8 12:24:39 2022
Salesforce(16920 4294837976): 23.212.249.11 6 443 Tue Mar  8 12:24:04 2022

branch1_fgt # get router info routing-table all
...
S*     0.0.0.0/0 [1/0] via 192.2.0.2, port1
                 [1/0] via 192.2.0.10, port2
...
```

Exhibit B

An administrator is testing application steering in SD-WAN. Before generating test traffic, the administrator collected the information shown in exhibit A.
After generating GoToMeeting test traffic, the administrator examined the respective traffic log on FortiAnalyzer, which is shown in exhibit B. The administrator noticed that the traffic matched the implicit SD-WAN rule, but they expected the traffic to match rule ID 1.
Which two reasons explain why the traffic matched the implicit SD-WAN rule? (Choose two.)

A. FortiGate did not refresh the routing information on the session after the application was detected.
B. Port1 and port2 do not have a valid route to the destination.
C. Full SSL inspection is not enabled on the matching firewall policy.
D. The session 3-tuple did not match any of the existing entries in the ISDB application cache.

Answer: BC

Explanation:
Study guide 7.2 Page 191

NEW QUESTION 3
Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(packet-
loss), link-cost-threshold(0), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0_0), alive, packet loss: 2.000%, selected
    2: Seq_num(4 T_MPLS_0), alive, packet loss: 4.000%, selected
    3: Seq_num(5 T_INET_1_0), alive, packet loss: 12.000%, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255

branch1_fgt (3) # show
config service
    edit 3
        set name "Corp"
        set mode priority
        set dst "Corp-net"
        set src "LAN-net"
        set health-check "VPN_PING"
        set link-cost-factor packet-loss
        set link-cost-threshold 0
        set priority-members 5 3 4
    next
end
```

The exhibit shows the SD-WAN rule status and configuration.
Based on the exhibit, which change in the measured packet loss will make T_INET_1_0 the new preferred member?

A. When all three members have the same packet loss.
B. When T_INET_0_0 has 4% packet loss.
C. When T_INET_0_0 has 12% packet loss.
D. When T_INET_1_0 has 4% packet loss.

Answer: D

NEW QUESTION 4
Exhibit.

```
# diagnose sys sdwan health-check status

Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(22.129), jitter(0.201), mos(4.393),
bandwidth-up(10235), bandwidth-dw(10235), bandwidth-bi(20470) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(7.000%) latency(42.394), jitter(0.912), mos(4.378),
bandwidth-up(10236), bandwidth-dw(10237), bandwidth-bi(20473) sla_map=0x0
Health Check(VPN_PING):
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(131.336), jitter(0.199), mos(4.330),
bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x2
Seq(4 T_INET_1): state(alive), packet-loss(11.000%) latency(1.465), jitter(0.226), mos(4.398),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x1
Seq(3 T_INET_0): state(alive), packet-loss(0.000%) latency(1.440), jitter(0.245), mos(4.403),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
```

The exhibit shows the output of the command diagnose sys sdwan health-check status
collected on a FortiGate device. Which two statements are correct about the health check status on this FortiGate device? (Choose two.)

A. The health-check VPN_PING orders the members according to the lowest jitter.
B. The interface T_INET_1 missed one SLA target.
C. There is no SLA criteria configured for the health-check Level3_DNS.
D. The interface T_INET_0 missed three SLA targets.

Answer: AC

Explanation:
 According to the FortiGate / FortiOS 6.4.2 Administration Guide, the health check status command displays the status of the health check probes for each SD-WAN member interface. The output includes the following information:
? state: the current state of the interface, either alive or dead
? packet-loss: the percentage of packets lost during the health check
? latency: the average round-trip time in milliseconds
? jitter: the variation in latency
? mos: the mean opinion score, a measure of voice quality
? bandwidth: the available bandwidth in kilobits per second for each direction (up, down, bi)
? sla map: a bitmap that indicates which SLA criteria are met or failed Based on the exhibit, the following statements are correct:
? The health-check VPN_PING orders the members according to the lowest jitter. This means that the interface with the lowest jitter value is listed first, followed by the next lowest, and so on1. In the exhibit, the order is T_MPLS, T_INET_1, and T_INET_0.
? There is no SLA criteria configured for the health-check Level3_DNS. This means that the health check does not use any SLA parameters to determine the state of the interface2. In the exhibit, the sla map value is 0x0 for both port1 and port2, indicating that no SLA criteria are applied.

NEW QUESTION 5
Refer to the exhibit.

```
session info: proto=6 proto_state=11 duration=242 expire=3349 timeout=3600
flags=00000000 socktype=0 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 dirty may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=3421/20/1 reply=3777/17/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=0.0.0.0/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:34676->128.66.0.1:22(192.2.0.1:34676)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.1:34676(10.0.1.101:34676)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:34676(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 pol_uuid_idx=14721 auth_info=0 chk_client_info=0 vd=0
serial=000032d9 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=2
rpdb_link_id=ff000002 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x001008
```

Which statement explains the output shown in the exhibit?

A. FortiGate performed standard FIB routing on the session.
B. FortiGate will not re-evaluate the session following a firewall policy change.
C. FortiGate used 192.2.0.1 as the gateway for the original direction of the traffic.
D. FortiGate must re-evaluate the session due to routing change.

Answer: D

Explanation:
The snat-route-change option is enabled by default. This option enables FortiGate to re- evaluate the routing table and select a new egress interface if the next hop IP address changes. This option only applies to sessions in the dirty state. Sessions in the log state are not affected by routing changes.

NEW QUESTION 6
Refer to the exhibits.
Exhibit A

Network Properties	
Service	Critical-DIA
Identity	
Device ID	FGVM01TM22000077
Device Name	branch1_fgt
Type	
Sub Type	sdwan
Type	event
Alerts	
Level	notice
General	
Log Description	SDWAN status
Log ID	0113022923
Message	Service prioritized by performance metric will be redirected in sequence order.
Sequence Number	2,1
Virtual Domain	root
Others	
Date/Time	23:57:29
Destination End User ID	3
Destination Endpoint ID	3
Device Time	2022-03-04 14:57:27
Event Time	1646434647595788893
Event Type	Service
Metric	latency
Service ID	1
Time Stamp	2022-03-04 23:57:29
Time Zone	-0800
UEBA Endpoint ID	3
UEBA User ID	3
logver	700030237

Exhibit B

```
branch1_fgt # diagnose sys sdwan member
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0

config service
    edit 1
        set name "Critical-DIA"
        set mode priority
        set src "LAN-net"
        set internet-service enable
        set internet-service-app-ctrl 16354 41468 16920
        set health-check "Level3_DNS"
        set priority-members 1 2
    next
end
```

Exhibit A shows an SD-WAN event log and exhibit B shows the member status and the SD-WAN rule configuration.
Based on the exhibits, which two statements are correct? (Choose two.)

A. FortiGate updated the outgoing interface list on the rule so it prefers port2.
B. Port2 has the highest member priority.
C. Port2 has a lower latency than port1.
D. SD-WAN rule ID 1 is set to lowest cost (SLA) mode.

Answer: AC

NEW QUESTION 7
Refer to the exhibit.

```
config system sdwan
    set status enable
    set load-balance source-dest-ip-based
    config zone
        edit "virtual-wan-link"
        next
        edit "SASE"
        next
        edit "underlay"
        next
    end
    config members
        edit 1
            set interface "port1"
            set zone "underlay"
            set gateway 192.2.0.2
        next
        edit 2
            set interface "port2"
            set zone "underlay"
            set gateway 192.2.0.10
        next
    end
...
end
```

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD- WAN rules?

A. All traffic from a source IP to a destination IP is sent to the same interface.
B. All traffic from a source IP is sent to the same interface.
C. All traffic from a source IP is sent to the most used interface.
D. All traffic from a source IP to a destination IP is sent to the least used interface.

Answer: A

Explanation:
 Study Guide 7.2, page 176.

NEW QUESTION 8
What are two benefits of using forward error correction (FEC) in IPsec VPNs? (Choose two.)

A. FEC supports hardware offloading.
B. FEC improves reliability of noisy links.
C. FEC transmits parity packets that can be used to reconstruct packet loss.
D. FEC can leverage multiple IPsec tunnels for parity packets transmission.

Answer: BC

NEW QUESTION 9
Refer to the Exhibits:

Exhibit A **Exhibit B**

Link Status

Check interval	500	ms
Failures before inactive ⓘ	3	
Restore link after ⓘ	2	check(s)

Actions when Inactive

Update static route ⓘ 🟢

Exhibit A   Exhibit B

```
NGFW-1 # diagnose sys sdwan health-check
Health Check (Ping):
Seq (1 port1): state (alive), packet-loss (0.000%) latency
(6.196), jitter (0.079) sla_map=0x0
Seq (2 port2): state (dead), packet-loss (6.000%) sla_map=0x0
```

Exhibit A, which shows the SD-WAN performance SLA and exhibit B shows the health of the participating SD-WAN members.
Based on the exhibits, which statement is correct?

A. The dead member interface stays unavailable until an administrator manually brings the interface back.
B. Port2 needs to wait 500 milliseconds to change the status from alive to dead.
C. Static routes using port2 are active in the routing table.
D. FortiGate has not received three consecutive requests from the SLA server configured for port2.

Answer: C

NEW QUESTION 10
Which best describes the SD-WAN traffic shaping mode that bases itself on a percentage of available bandwidth?

A. Interface-based shaping mode
B. Reverse-policy shaping mode
C. Shared-policy shaping mode
D. Per-IP shaping mode

Answer: A

Explanation:
Interface-based shaping goes further, enabling traffic controls based on percentage of the interface bandwidth.

NEW QUESTION 10
Which diagnostic command can you use to show the member utilization statistics measured by performance SLAs for the last 10 minutes?

A. diagnose sys sdwan sla-log
B. diagnose ays sdwan health-check
C. diagnose sys sdwan intf-sla-log
D. diagnose sys sdwan log

Answer: A

NEW QUESTION 11
Refer to the exhibit.

```
config system settings
    set firewall-session-dirty check-new
end
```

Based on the exhibit, which two actions does FortiGate perform on sessions after a firewall policy change? (Choose two.)

A. FortiGate flushes all sessions.
B. FortiGate terminates the old sessions.
C. FortiGate does not change existing sessions.
D. FortiGate evaluates new sessions.

Answer: CD

Explanation:
FortiGate not to flag existing impacted session as dirty by setting firewall-session-dirty to check new. The results is that FortiGate evaluates only new session against the new firewall policy.

NEW QUESTION 15
Refer to the exhibit.

```
config firewall policy
    edit 1
        set anti-replay disable
    next
end
```

In a dual-hub hub-and-spoke SD-WAN deployment, which is a benefit of disabling the anti- replay setting on the hubs?

A. It instructs the hub to disable the reordering of TCP packets on behalf of the receiver, to improve performance.
B. It instructs the hub to disable TCP sequence number check, which is required for TCP sessions originated from spokes to fail over back and forth between the hubs.
C. It instructs the hub to not check the ESP sequence numbers on IPsec traffic, to improve performance.
D. It instructs the hub to skip content inspection on TCP traffic, to improve performance.

Answer: B

NEW QUESTION 18
Exhibit A –

Exhibit B –

Exhibit A shows the system interface with the static routes and exhibit B shows the firewall policies on the managed FortiGate.
Based on the FortiGate configuration shown in the exhibits, what issue might you encounter when creating an SD-WAN zone for port1 and port2?

A. port1 is assigned a manual IP address.
B. port1 is referenced in a firewall policy.
C. port2 is referenced in a static route.
D. port1 and port2 are not administratively down.

Answer: B

NEW QUESTION 19
Which two statements about SLA targets and SD-WAN rules are true? (Choose two.)

A. SD-WAN rules use SLA targets to check if the preferred members meet the SLA requirements
B. Member metrics are measured only if an SLA target is configured
C. When configuring an SD-WAN rule you can select multiple SLA targets of the same performance SLA
D. SLA targets are used only by SD-WAN rules that are configured with Lowest Cost (SLA) or Maximize Bandwidth (SLA) as strategy

Answer: AD

NEW QUESTION 21
Which statement about using BGP for ADVPN is true?

A. You must use BGP to route traffic for both overlay and underlay links.
B. You must configure AS path prepending.
C. You must configure BGP communities.
D. IBGP is preferred over EBGP, because IBGP preserves next hop information.

Answer: D

Explanation:
 ADVPN is a technology that allows dynamic creation of IPsec tunnels between branch sites without requiring pre-configured policies or keys. BGP is a routing protocol that can be used to exchange routes between ADVPN peers. IBGP is a type of BGP that runs between routers in the same autonomous system (AS), while EBGP is a type of BGP that runs between routers in different ASes. IBGP is preferred over EBGP for ADVPN, because IBGP preserves the next hop information of the routes, which is needed to establish the IPsec tunnels. EBGP changes the next hop information to the EBGP peer address, which may not be reachable by the ADVPN peers. Therefore, using IBGP for ADVPN avoids the need to configure additional static routes or redistribute routes between BGP and another routing protocol. References = ADVPN with BGP as the routing protocol, ADVPN, SD-WAN self-healing with BGP, Technical Tip: ADVPN with BGP as the routing protocol
The statement that IBGP is preferred over EBGP for ADVPN because IBGP preserves next hop information (D) is true. In a typical ADVPN deployment, it's beneficial to maintain next hop information across the network to ensure proper routing and optimal path selection. References: This understanding comes from my knowledge of Fortinet's SD-WAN and ADVPN configurations, where BGP's behavior in terms of next hop preservation is a key consideration.

NEW QUESTION 22
Which two tasks are part of using central VPN management? (Choose two.)

A. You can configure full mesh, star, and dial-up VPN topologies.
B. You must enable VPN zones for SD-WAN deployments.
C. FortiManager installs VPN settings on both managed and external gateways.
D. You configure VPN communities to define common IPsec settings shared by all VPN gateways.

Answer: AD

NEW QUESTION 26
Which SD-WAN setting enables FortiGate to delay the recovery of ADVPN shortcuts?

A. hold-down-time
B. link-down-failover
C. auto-discovery-shortcuts
D. idle-timeout

Answer: A

NEW QUESTION 29
Refer to the exhibit.

```
config system virtual-wan-link
    set status enable
    set load-balance-mode source-ip-based
    config members
        edit 1
                    set interface "port1"
                    set gateway 100.64.1.254
                    set source 100.64.1.1
                    set cost 15

        next
        edit 2

                    set interface "port2"
                    set gateway 100.64.2.254
                    set priority 10

        next
    end
end
```

Based on the output shown in the exhibit, which two criteria on the SD-WAN member configuration can be used to select an outgoing interface in an SD-WAN rule? (Choose two.)

A. Set priority 10.
B. Set cost 15.
C. Set load-balance-mode source-ip-ip-based.
D. Set source 100.64.1.1.

Answer: AB

NEW QUESTION 30
Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

A. Encapsulating Security Payload (ESP)
B. Secure Shell (SSH)
C. Internet Key Exchange (IKE)
D. Security Association (SA)

Answer: AC

NEW QUESTION 31
In a hub-and-spoke topology, what are two advantages of enabling ADVPN on the IPsec overlays? (Choose two.)

A. It provides the benefits of a full-mesh topology in a hub-and-spoke network.
B. It provides direct connectivity between spokes by creating shortcuts.
C. It enables spokes to bypass the hub during shortcut negotiation.
D. It enables spokes to establish shortcuts to third-party gateways.

Answer: AB

NEW QUESTION 35
Which two statements are correct when traffic matches the implicit SD-WAN rule? (Choose two.)

A. The sdwan_service_id flag in the session information is 0.
B. All SD-WAN rules have the default setting enabled.
C. Traffic does not match any of the entries in the policy route table.
D. Traffic is load balanced using the algorithm set for the v4-ecmp-mode setting.

Answer: AC

Explanation:
sdwan_service_id is 0 = match SD-WAN implicit rule, study guide 7.0 page 120, 7.2 page 149 SD-WAN rules internally are interpreted as a Policy route, so when the traffic doesn't match with any policy route, it will be flowing by implict policy.

NEW QUESTION 36
Refer to the exhibit.

```
id=20085 trace_id=847 func=print_pkt_detail line=5428 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:33920->74.125.195.93:443) from port3. flag [.], seq
2018554516, ack 4141536963, win 2238"
id=20085 trace_id=847 func=resolve_ip_tuple_fast line=5508 msg="Find an existing
session, id-000008c1, original direction"
id=20085 trace_id=847 func=shaper_handler line=821 msg="exceeded shaper limit, drop"
```

Which conclusion about the packet debug flow output is correct?

A. The original traffic exceeded the maximum packets per second of the outgoing interface, and the packet was dropped.
B. The reply traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.
C. The original traffic exceeded the maximum bandwidth of the outgoing interface, and the packet was dropped.
D. The original traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.

Answer: D

NEW QUESTION 38
In the default SD-WAN minimum configuration, which two statements are correct when traffic matches the default implicit SD-WAN rule? (Choose two)

A. Traffic has matched none of the FortiGate policy routes.
B. Matched traffic failed RPF and was caught by the rule.
C. The FIB lookup resolved interface was the SD-WAN interface.
D. An absolute SD-WAN rule was defined and matched traffic.

Answer: AC

NEW QUESTION 41
Refer to the exhibit.

```
config system sdwan
    set fail-detect enable
    set fail-alert-interfaces "port5"
    config health-check
        edit "Level3_DNS"
            set update-cascade-interface enable
            set members 1 2
        next
        edit "HQ"
            set update-cascade-interface enable
            set members 3
        next
    end
end
```

Based on the exhibit, which action does FortiGate take?

A. FortiGate bounces port5 after it detects all SD-WAN members as dead.
B. FortiGate fails over to the secondary device after it detects all SD-WAN members as dead.
C. FortiGate brings up port5 after it detects all SD-WAN members as alive.
D. FortiGate brings down port5 after it detects all SD-WAN members as dead.

Answer: A

NEW QUESTION 45
Refer to the exhibits. Exhibit A -

Edit Performance SLA

Name	Level3_DNS
IP Version	**IPv4** IPv6
Probe Mode	**Active** Passive Prefer Passive
Protocol	**Ping** TCP ECHO UDP ECHO HTTP TWA
Server	4.2.2.1
	4.2.2.2
Participants	All SD-WAN Members **Specify**
	🔍
	port1
	📶 port2
	2 Entries
Enable Probe Packets	🔵
SLA Targets ℹ️	
	+ Add Target

Link Status

Interval	500 ⌄	Milliseconds
Failure Before Inactive	3 ⌄	(max 3600)
Restore Link After	2 ⌄	(max 3600)

Action When Inactive

Update Static Route	🔵
Cascade Interfaces	🔵

Exhibit B -

```
branch1_fgt # diagnose sys sdwan member | grep port
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0

branch1_fgt # get router info routing-table all | grep port
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1
                  [1/0] via 192.2.0.10, port2
S       8.8.8.8/32 [10/0] via 192.2.0.11, port2
C       10.0.1.0/24 is directly connected, port5
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10

branch1_fgt # diagnose sys sdwan health-check status Level3_DNS
Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(1.919), jitter(0.137), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(1.509), jitter(0.101), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
```

Exhibit A shows the SD-WAN performance SLA and exhibit B shows the SD-WAN member status, the routing table, and the performance SLA status.
If port2 is detected dead by FortiGate, what is the expected behavior?

A. Port2 becomes alive after three successful probes are detected.
B. FortiGate removes all static routes for port2.
C. The administrator manually restores the static routes for port2, if port2 becomes alive.
D. Host 8.8.8.8 is reachable through port1 and port2.

Answer: B

Explanation:
 This is due to Update static route is enable which removes the static route entry referencing the interface if the interface is dead

NEW QUESTION 49
Refer to the exhibit.

```
config router bgp
    set as 65000
    set router-id 10.1.0.1
    set ibgp-multipath enable
    set additional-path enable
    set additional-path-select 3
    config neighbor-group
        edit "Branches_INET_0"
            set interface "T_INET_0_0"
            set remote-as 65000
            set update-source "T_INET_0_0"
        next
        edit "Branches_INET_1"
            set interface "T_INET_1_0"
            set remote-as 65000
            set update-source "T_INET_1_0"
        next
        edit "Branches_MPLS"
            set interface "T_MPLS_0"
            set remote-as 65000
            set update-source "T_MPLS_0"
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.201.1.0 255.255.255.0
            set neighbor-group "Branches_INET_0"
        next
        edit 2
            set prefix 10.202.1.0 255.255.255.0
            set neighbor-group "Branches_INET_1"
        next
        edit 3
            set prefix 10.203.1.0 255.255.255.0
            set neighbor-group "Branches_MPLS"
        next
    end
...
end
```

The exhibit shows the BGP configuration on the hub in a hub-and-spoke topology. The administrator wants BGP to advertise prefixes from spokes to other spokes over the IPsec overlays, including additional paths. However, when looking at the spoke routing table, the administrator does not see the prefixes from other spokes and the additional paths.

Based on the exhibit, which three settings must the administrator configure inside each BGP neighbor group so spokes can learn other spokes prefixes and their additional paths? (Choose three.)

A. Set additional-path to send
B. Enable route-reflector-client
C. Set advertisement-interval to the number of additional paths to advertise
D. Set adv-additional-path to the number of additional paths to advertise
E. Enable soft-reconfiguration

Answer: ABD

NEW QUESTION 53
The administrator uses the FortiManager SD-WAN overlay template to prepare an SD- WAN deployment. With information provided through the SD-WAN overlay template wizard, FortiManager creates templates ready to install on spoke and hub devices.
Select three templates created by the SD-WAN overlay template for a spoke device. (Choose three.)

A. System template
B. BGP template
C. IPsec tunnel template
D. CLI template
E. Overlay template

Answer: ACE

Explanation:
In a FortiManager SD-WAN overlay template configuration for a spoke device, the system template (A) is created to provide basic device settings. The IPsec tunnel template (C) is generated to establish secure tunnels between the spoke and the hub devices. Lastly, the overlay template (E) is configured to specify the overlay network settings, which often include the SD-WAN rules and performance SLAs.

NEW QUESTION 55

Exhibit A shows the firewall policy and exhibit B shows the traffic shaping policy.

Exhibit A	Exhibit B

Edit Policy

Name ⓘ	Internet Access
Incoming interface	▦ port3 ▼
Outgoing interface	◉ virtual-wan link ▼
Source	▣ all ✕ +
Destination	▣ all ✕ +
Schedule	▱ always ▼
Service	▣ ALL ✕ +
Action	✓ ACCEPT ⊘ DENY
Inspection Mode	Flow-based Proxy-based

Firewall / Network Options

NAT	⬤
IP Pool Configuration	Use Outgoing Interface Address Use Dynamic
Preserve Source Port	◯
Protocol Options	PROT default ▼

Exhibit A	Exhibit B

Edit Traffic Shaping Policy

Name	inbound_outbound_shaper
Status	ⓘ Enabled ❗ Disabled
Comments	Write a comment... 0/255

If Traffic Matches:

Source	▣ all ✕ +
Destination	▣ all ✕ +
Schedule	◯
Service	▣ ALL ✕ +
Application ⓘ	+
URL Category	Streaming Media and Download ✕ +

Then:

Action	Apply Shaper Assign Shaping Class ID
Outgoing interface	◉ virtual-wan link ✕ +
Shared shaper	⬤ guarantee-10mbps ▼

The traffic shaping policy is being applied to all outbound traffic; however, inbound traffic is not being evaluated by the shaping policy.
Based on the exhibits, what configuration change must be made in which policy so that traffic shaping can be applied to inbound traffic?

A. Create a new firewall policy, and the select the SD-WAN zone as Incoming Interface.
B. In the traffic shaping policy, select Assign Shaping Class ID as Action.
C. In the firewall policy, select Proxy-based as Inspection Mode.

D. In the traffic shaping policy, enable Reverse shaper, and then select the traffic shaper to use.

Answer: D

NEW QUESTION 58
Which type statements about the SD-WAN members are true? (Choose two.)

A. You can manually define the SD-WAN members sequence number.
B. Interfaces of type virtual wire pair can be used as SD-WAN members.
C. Interfaces of type VLAN can be used as SD-WAN members.
D. An SD-WAN member can belong to two or more SD-WAN zones.

Answer: AC

Explanation:
 SD-WAN members can be manually ordered by changing their sequence number (A), which allows administrators to prioritize the interfaces according to the routing requirements. Also, VLAN interfaces can be used as SD-WAN members (C), providing flexibility in network design and the use of existing VLAN infrastructure within the SD-WAN setup.

NEW QUESTION 62
What are two benefits of choosing packet duplication over FEC for data loss correction on noisy links? (Choose two.)

A. Packet duplication can leverage multiple IPsec overlays for sending additional data.
B. Packet duplication does not require a route to the destination.
C. Packet duplication supports hardware offloading.
D. Packet duplication uses smaller parity packets which results in less bandwidth consumption.

Answer: AC

NEW QUESTION 63
Refer to the exhibit.

```
# diagnose firewall shaper per-ip-shaper list
name FTP_5M
maximum-bandwidth 625 KB/sec
maximum-concurrent-session 5
tos ff/ff
packets dropped 65
bytes dropped 81040
        addr=10.1.0.1 status: bps=0 ses=1
        addr=10.1.0.100 status: bps=0 ses=1
        addr=10.1.10.1 status: bps=1656 ses=3
```

Which are two expected behaviors of the traffic that matches the traffic shaper? (Choose two.)

A. The number of simultaneous connections among all source IP addresses cannot exceed five connections.
B. The traffic shaper limits the combined bandwidth of all connections to a maximum of 5 MB/sec.
C. The number of simultaneous connections allowed for each source IP address cannot exceed five connections.
D. The traffic shaper limits the bandwidth of each source IP address to a maximum of 625 KB/sec.

Answer: CD

NEW QUESTION 64
Which two statements reflect the benefits of implementing the ADVPN solution to replace conventional VPN topologies? (Choose two.)

A. It creates redundant tunnels between hub-and-spokes, in case failure takes place on the primary links.
B. It dynamically assigns cost and weight between the hub and the spokes, based on the physical distance.
C. It ensures that spoke-to-spoke traffic no longer needs to flow through the tunnels through the hub.
D. It provides direct connectivity between all sites by creating on-demand tunnels betweenspokes.

Answer: CD

NEW QUESTION 65
......

Relate Links

100% Pass Your NSE7_SDW-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/NSE7_SDW-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/