



## 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

What are two reasons for using FortiManager to organize and manage the network for a group of FortiGate devices? (Choose two.)

- A. It simplifies the deployment and administration of SD-WAN on managed FortiGate devices.
- B. It improves SD-WAN performance on the managed FortiGate devices.
- C. It sends probe signals as health checks to the beacon servers on behalf of FortiGate.
- D. It acts as a policy compliance entity to review all managed FortiGate devices.
- E. It reduces WAN usage on FortiGate devices by acting as a local FortiGuard server.

Answer: AE

### NEW QUESTION 2

Which two statements about the SD-WAN zone configuration are true? (Choose two.)

- A. The service-sla-tie-break setting enables you to configure preferred member selection based on the best route to the destination.
- B. You can delete the default zones.
- C. The default zones are virtual-wan-link and SASE.
- D. An SD-WAN member can belong to two or more zones.

Answer: AC

### NEW QUESTION 3

Which are two benefits of using CLI templates in FortiManager? (Choose two.)

- A. You can reference meta fields.
- B. You can configure interfaces as SD-WAN members without having to remove references first.
- C. You can configure FortiManager to sync local configuration changes made on the managed device, to the CLI template.
- D. You can configure advanced CLI settings.

Answer: AD

### NEW QUESTION 4

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

Destination IP	Service	Application	Security Event List	SD-WAN Rule Name	Destination Interface
23.212.248.205	HTTPS	GoToMeeting	sec:2	Critical-DIA	port2
23.205.106.86	HTTPS	GoToMeeting	sec:2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	sec:2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	sec:2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	sec:2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	sec:2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	sec:2	Critical-DIA	port2
23.205.106.86	HTTPS	GoToMeeting	sec:2	Critical-DIA	port2

Security	APP Count	Level	notice
General	Log ID	0000000013	
	Session ID	769	
	Tran Display	nat	
	Virtual Domain	nat	
Source	Country	Reserved	
	Device ID	FGVM017M42000077	
	Device Name	branch1_fgt	
	IP	10.0.1.101	
	Interface	port3	
	Interface Role	undefined	
	NAT IP	192.2.0.9	
	NAT Port	55042	
	Port	55042	
	Source	10.0.1.101	
	UEBA Endpoint ID	1025	
	UEBA User ID	3	
Destination	Country	United States	
	End User ID	3	
	Endpoint ID	155	
	Host Name	www.gotomeeting.com	
	IP	23.212.248.205	
	Interface	port2	

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 5**

Which two statements are true about using SD-WAN to steer local-out traffic? (Choose two.)

- A. FortiGate does not consider the source address of the packet when matching an SD- WAN rule for local-out traffic.
- B. By default, local-out traffic does not use SD-WAN.
- C. By default, FortiGate does not check if the selected member has a valid route to the destination.
- D. You must configure each local-out feature individually, to use SD-WAN.

**Answer:** BD

**NEW QUESTION 6**

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), health-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 7**

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
origin->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_uid_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
rpdh_link_id=ff000002 rpdh_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.

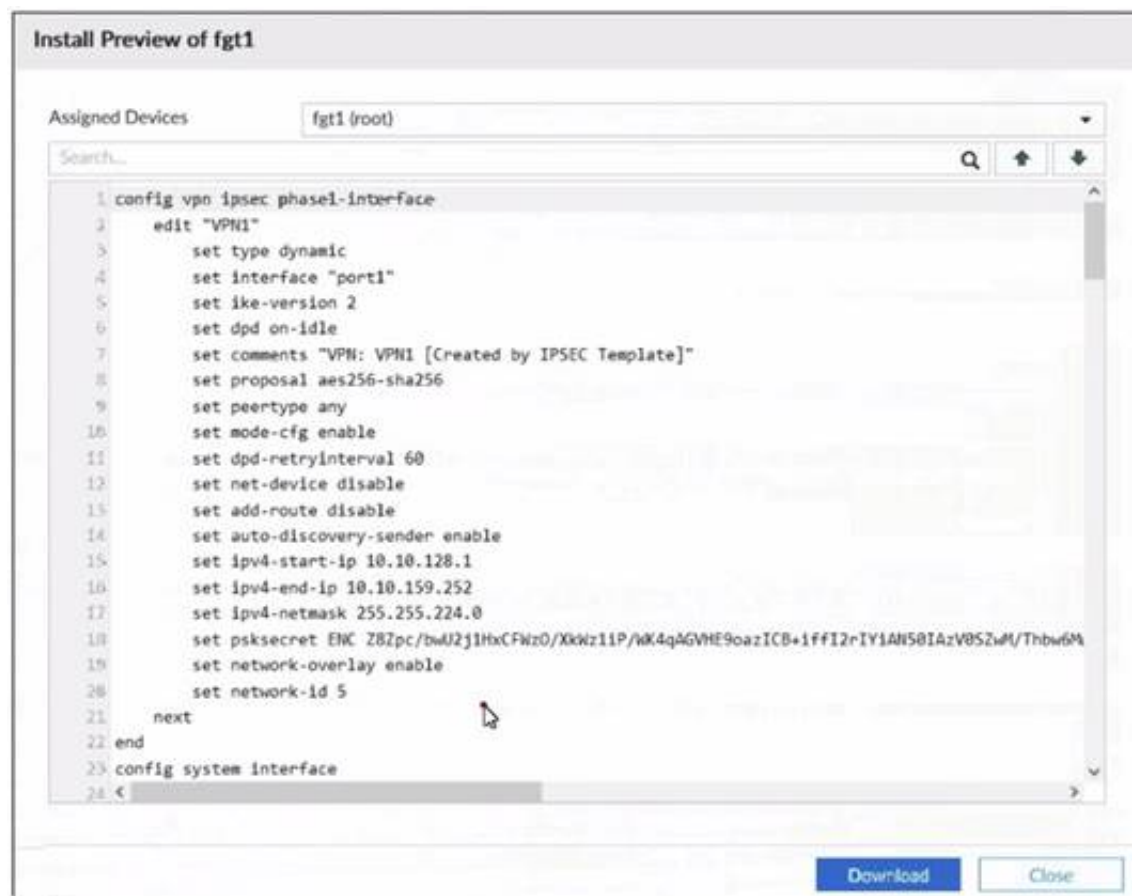
**Answer:** D

**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 8

Refer to the exhibit.



An administrator used the SD-WAN overlay template to prepare an IPsec configuration for a hub-and-spoke SD-WAN topology. The exhibit shows the installation preview for one FortiGate device. In the exhibit, which statement best describes the configuration applied to the FortiGate device?

- A. It is a hub device
- B. It can send ADVPN shortcut offers.
- C. It is a spoke device that establishes dynamic IPsec tunnels to the hu
- D. The subnet range is 10.10.128.0/23.
- E. It is a spoke device that establishes dynamic IPsec tunnels to the hu
- F. It can send ADVPN shortcut requests.
- G. It is a hub device and will automatically discover the spoke devices that are in the SD- WAN topology.

**Answer: C**

### Explanation:

According to the SD-WAN 7.2 Study Guide, the SD-WAN overlay template simplifies the configuration of IPsec tunnels in a hub-and-spoke topology. The template defines the following parameters:

- ? type: dynamic for spokes, static for hubs
  - ? interface: the WAN interface to use for the IPsec tunnel
  - ? network-overlay: enable for spokes, disable for hubs
  - ? network-id: a unique identifier for each spoke
  - ? auto-discovery-sender: enable for hubs, disable for spokes
  - ? auto-discovery-receiver: enable for spokes, disable for hubs
- Based on the exhibit, the FortiGate device has the following configuration:
- ? type: dynamic
  - ? interface: port1
  - ? network-overlay: enable
  - ? network-id: 5
  - ? auto-discovery-sender: disable
  - ? auto-discovery-receiver: enable

Therefore, the FortiGate device is a spoke that establishes dynamic IPsec tunnels to the hub. It also has the network-overlay and auto-discovery-receiver options enabled, which means it can send ADVPN shortcut requests to other spokes when it receives a shortcut offer from the hub

## NEW QUESTION 9

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 10

Refer to the exhibit.



```
config system interface
  edit "port2"
    set vdom "root"
    set ip 192.2.0.9 255.255.255.248
    set allowaccess ping
    set type physical
    set role wan
    set snmp-index 2
    set preserve-session-route enable
  next
end
```

Based on the exhibit, which two actions does FortiGate perform on traffic passing through port2? (Choose two.)

- A. FortiGate does not change the routing information on existing sessions that use a valid gateway, after a route change.
- B. FortiGate performs routing lookups for new sessions only, after a route change.
- C. FortiGate always blocks all traffic, after a route change.
- D. FortiGate flushes all routing information from the session table, after a route change.

**Answer:** AB

#### NEW QUESTION 10

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 14

Which two conclusions for traffic that matches the traffic shaper are true? (Choose two.)

```
# diagnose firewall shaper traffic-shaper list name VoIP_Shaper
name VoIP_Shaper
maximum-bandwidth 6250 KB/sec
guaranteed-bandwidth 2500 KB/sec
current-bandwidth 93 KB/sec
priority 2
overhead 0
tos ff
packets dropped 0
bytes dropped 0
```

- A. The traffic shaper drops packets if the bandwidth is less than 2500 KBps.
- B. The measured bandwidth is less than 100 KBps.
- C. The traffic shaper drops packets if the bandwidth exceeds 6250 KBps.
- D. The traffic shaper limits the bandwidth of each source IP to a maximum of 6250 KBps.

**Answer:** BC

#### NEW QUESTION 18

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 20

Exhibit.

```
7: [...]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.1.9 locip=192.2.0.9
rempo=500 locpo=500 outintf="port2" cookies="773c72b48060051d/529ac435532959b6" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.202.1.1
vpntunnel="T_INET_1" tunnelip=N/A tunnelid=2595348112 tunneltype="ipsec" duration=3581
sentbyte=386431 rcvdbyte=387326 nextstat=600 advpnsc=0

9: [...]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=172.16.0.9 locip=172.16.0.1
rempo=500 locpo=500 outintf="port4" cookies="0624890597f0096d/ed1bd5247375c46f" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="T_MPLS_0"
tunnelip=0.0.0.0 tunnelid=2595348102 tunneltype="ipsec" duration=223 sentbyte=115040
rcvdbyte=345160 nextstat=600 advpnsc=1

9: [...]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.1.1 locip=192.2.0.1
rempo=500 locpo=500 outintf="port1" cookies="747b432459497188/6616a969a6937853" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.201.1.1
vpntunnel="T_INET_0" tunnelip=N/A tunnelid=2595348115 tunneltype="ipsec" duration=3580
sentbyte=388020 rcvdbyte=387994 nextstat=600 advpnsc=0
```

The exhibit shows VPN event logs on FortiGate. In the output shown in the exhibit, which statement is true?

- A. There are no IPsec tunnel statistics log messages for ADVPN cuts.
- B. There is one shortcut tunnel built from master tunnel T\_MPLS\_0.
- C. The VPN tunnel T\_MPLS\_0 is a shortcut tunnel.
- D. The master tunnel T\_INET\_0 cannot accept the ADVPN shortcut.

**Answer: B**

#### Explanation:

VPN event logs record the status of VPN tunnels, such as the establishment, termination, or failure of a tunnel. The output includes the following information:

- ? logid: the log ID number
- ? type: the log type, either traffic or event
- ? subtype: the log subtype, either vpn or ipsec
- ? level: the log level, either error, warning, or notice
- ? vd: the virtual domain name
- ? logdesc: the log description
- ? msg: the log message
- ? action: the log action, such as tunnel-up, tunnel-down, or tunnel-stats
- ? remip: the remote IP address
- ? locip: the local IP address
- ? rempo: the remote port number
- ? locpo: the local port number
- ? outintf: the outgoing interface name
- ? cookies: the IKE SA cookies
- ? user: the user name
- ? group: the user group name
- ? useralt: the alternative user name
- ? xauthuser: the XAuth user name
- ? authgroup: the XAuth user group name
- ? assignip: the assigned IP address
- ? vpntunnel: the VPN tunnel name
- ? tunnelip: the tunnel loopback IP address
- ? tunnelid: the tunnel ID number
- ? tunneltype: the tunnel type, either ipsec or ssl
- ? duration: the tunnel duration in seconds
- ? sentbyte: the number of bytes sent
- ? rcvdbyte: the number of bytes received
- ? nextstat: the next statistics interval in seconds
- ? advpnsc: the ADVPN shortcut flag, either 0 or 1 Based on the exhibit, the following statement is true:

? There is one shortcut tunnel built from master tunnel T\_MPLS\_0. This means that the VPN tunnel T\_MPLS\_0 is a master tunnel that can send ADVPN shortcut offers to other spokes, and the VPN tunnel T\_MPLS\_0\_0 is a shortcut tunnel that is built from the master tunnel T\_MPLS\_01. In the exhibit, the log action for T\_MPLS\_0 is tunnel-up, and the log action for T\_MPLS\_0\_0 is shortcut-up. The advpnsc flag for T\_MPLS\_0 is 0, indicating that it is not a shortcut tunnel, while the advpnsc flag for T\_MPLS\_0\_0 is 1, indicating that it is a shortcut tunnel.

#### NEW QUESTION 22

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 23

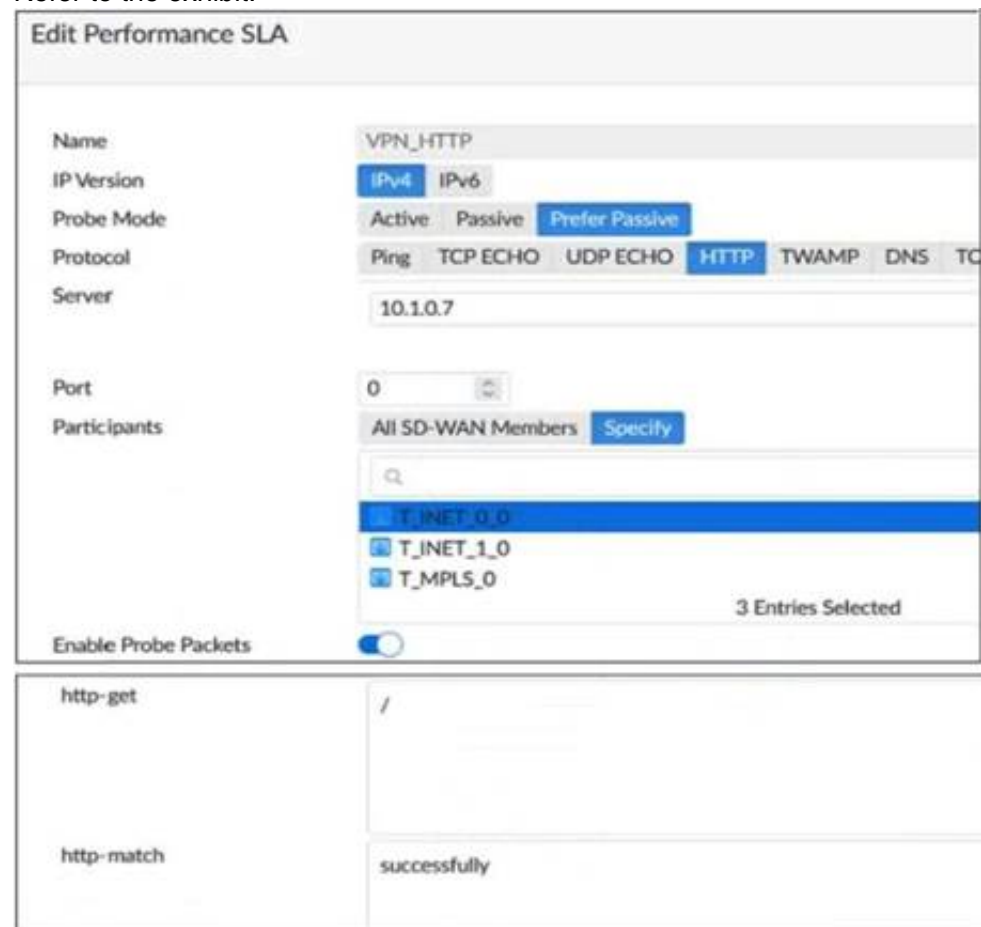
Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

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

**Answer:** AC

#### NEW QUESTION 28

Refer to the exhibit.



Based on the exhibit, which two statements are correct about the health of the selected members? (Choose two.)

- A. After FortiGate switches to active mode, FortiGate never fails back to passive monitoring.
- B. During passive monitoring, FortiGate can't detect dead members.
- C. FortiGate can offload the traffic that is subject to passive monitoring to hardware.
- D. FortiGate passively monitors the member if TCP traffic is passing through the member.

**Answer:** BD

#### NEW QUESTION 32

Which CLI command do you use to perform real-time troubleshooting for ADVPN negotiation?

- A. get router info routing-table all
- B. diagnose debug application ike
- C. diagnose vpn tunnel list
- D. get ipsec tunnel list

**Answer:** B

#### Explanation:

IKE real-time debug - useful when debugging ADVPN shortcut messages and spoke-to-spoke negotiations.

- diagnose debug console timestamp enable
- diagnose vpn ike log filter clear
- diagnose vpn ike log filter mdst-addr4 <ip.of.hub> <ip.of.spoke>
- diagnose debug application ike -1
- diagnose debug enable

#### NEW QUESTION 33

What are two advantages of using an IPsec recommended template to configure an IPsec tunnel in a hub-and-spoke topology? (Choose two.)



- A. VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.
- B. FortiManager automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM.
- C. IPsec recommended template guides the administrator to use Fortinet recommended settings.
- D. IPsec recommended template ensures consistent settings between phase1 and phase2

**Answer:** BC

**Explanation:**

According to the SD-WAN 7.2 Study Guide, IPsec recommended templates are designed to simplify the configuration of IPsec tunnels in a hub-and-spoke topology. They have the following advantages:

? FortiManager automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM. This reduces the manual effort and ensures that all spokes have the same configuration.

? IPsec recommended template guides the administrator to use Fortinet recommended settings, such as encryption algorithms, key lifetimes, and dead peer detection. This ensures optimal performance and security of the IPsec tunnels.

**NEW QUESTION 35**

Exhibit.

```
id=20010 trace_id=1402 func=print_pkt_detail line=5588 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:52490->42.44.50.10:443) from port3. flag [.), seq 1213725680,
ack 1169005655, win 65535"
id=20010 trace_id=1402 func=resolve_ip_tuple_fast line=5669 msg="Find an existing
session, id=00001ca4, original direction"
id=20010 trace_id=1402 func=fw_forward_dirty_handler line=447 msg="Denied by quota
check"
```

Which conclusion about the packet debug flow output is correct?

- A. The total number of daily sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.
- B. The packet size exceeded the outgoing interface MTU.
- C. The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.
- D. The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the firewall policy, and the packet was dropped.

**Answer:** C

**Explanation:**

In a Per-IP shaper configuration, if an IP address exceeds the configured concurrent session limit, the message "Denied by quota check" appears. SD-WAN 7.0 Study Guide page 287

**NEW QUESTION 36**

Which two interfaces are considered overlay links? (Choose two.)

- A. LAG
- B. IPsec
- C. Physical
- D. GRE

**Answer:** BD

**NEW QUESTION 41**

Which are three key routing principles in SD-WAN? (Choose three.)

- A. FortiGate performs route lookups for new sessions only.
- B. Regular policy routes have precedence over SD-WAN rules.
- C. SD-WAN rules have precedence over ISDB routes.
- D. By default, SD-WAN members are skipped if they do not have a valid route to the destination.
- E. By default, SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

**Answer:** BDE

**Explanation:**

Study Guide 7.2, pages 125, 129, 151

**NEW QUESTION 44**

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 45

.....

## Relate Links

**100% Pass Your NSE7\_SDW-7.2 Exam with Examible Prep Materials**

[https://www.exambible.com/NSE7\\_SDW-7.2-exam/](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/>