

Fortinet

Exam Questions NSE7_SDW-7.2

Fortinet NSE 7 - SD-WAN 7.2



NEW QUESTION 1

Which two statements describe how IPsec phase 1 main mode is different from aggressive mode when performing IKE negotiation? (Choose two)

- A. A peer ID is included in the first packet from the initiator, along with suggested security policies.
- B. XAuth is enabled as an additional level of authentication, which requires a username and password.
- C. A total of six packets are exchanged between an initiator and a responder instead of three packets.
- D. The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

Answer: BC

NEW QUESTION 2

What does enabling the exchange-interface-ip setting enable FortiGate devices to exchange?

- A. The gateway address of their IPsec interfaces
- B. The tunnel ID of their IPsec interfaces
- C. The IP address of their IPsec interfaces
- D. The name of their IPsec interfaces

Answer: C

NEW QUESTION 3

Refer to the exhibits.

Exhibit A

```
branch1_fgt # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Service disabled caused by no destination.
Members(2):
  1: Seq_num(4 T_INET_1_0), alive, selected
  2: Seq_num(5 T_MPLS_0), alive, selected
Src address(1):
  10.0.1.0-10.0.1.255

branch1_fgt # get router info bgp community 65000:10
VRF 0 BGP table version is 3, local router ID is 10.0.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight RouteTag Path
*>i10.1.0.0/24      10.202.1.254       0      100    0         1 i <-/1>
* i                 10.203.1.254       0      100    0         1 i <-/->

Total number of prefixes 1
```

Exhibit B

```
branch1_igt (1) # show
config service
  edit 1
    set name "Corp"
    set route-tag 10
    set src "LAN-net"
    set priority-zone "overlay"
  next
end

config router bgp
...
  config neighbor
    edit "10.202.1.254"
      set soft-reconfiguration enable
      set interface "T_INET_1_0"
      set remote-as 65000
      set route-map-in "dcl-lan-rm"
      set update-source "T_INET_1_0"
    next
    edit "10.203.1.254"
      set soft-reconfiguration enable
      set interface "T_MPLS_0"
      set remote-as 65000
      set route-map-in "dcl-lan-rm"
      set update-source "T_MPLS_0"
    next
  end
...
  config router route-map
    edit "dcl-lan-rm"
      config rule
        edit 1
          set match-community "dcl-lan-cl"
          set set-route-tag 1
        next
      end
    next
  end
end
```

Exhibit A shows the SD-WAN rule status and the learned BGP routes with community 65000:10. Exhibit B shows the SD-WAN rule configuration, the BGP neighbor configuration, and the route map configuration. The administrator wants to steer corporate traffic using routes tags in the SD-WAN rule ID 1. However, the administrator observes that the corporate traffic does not match the SD-WAN rule ID 1. Based on the exhibits, which configuration change is required to fix issue?

- A. In the dcl-lab-rm route map configuration, set set-route-tag to 10.
- B. In SD-WAN rule ID 1, change the destination to use ISDB entries.
- C. In the BGP neighbor configuration, apply the route map dcl-lab-rm in the outbound direction.
- D. In the dcl-lab-rm route map configuration, unset match-community.

Answer: C

NEW QUESTION 4

Which three matching traffic criteria are available in SD-WAN rules? (Choose three.)

- A. Type of physical link connection
- B. Internet service database (ISDB) address object
- C. Source and destination IP address
- D. URL categories
- E. Application signatures

Answer: BCE

NEW QUESTION 5

Which two settings can you configure to speed up routing convergence in BGP? (Choose two.)

- A. update-source
- B. set-route-tag
- C. holdtime-timer
- D. link-down-failover

Answer: CD

NEW QUESTION 6

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 7

Which two performance SLA protocols enable you to verify that the server response contains a specific value? (Choose two.)

- A. http
- B. icmp
- C. twamp
- D. dns

Answer: AD

Explanation:

Performance SLA (Service Level Agreement) protocols are used in SD-WAN to monitor the quality and performance of various network services. The two protocols that specifically allow for verifying a specific value in the server response are:

? HTTP (Hypertext Transfer Protocol): HTTP is the foundation of data communication on the World Wide Web. It allows for fetching resources, such as HTML documents. You can configure an HTTP performance SLA to send specific requests (e.g., GET or POST) and then check if the response body contains a particular string or value. This is useful for validating web server functionality and content delivery.

? DNS (Domain Name System): DNS is responsible for translating domain names into IP addresses. A DNS performance SLA can be set up to query a specific domain and verify that the returned IP address or other DNS record values match what is expected. This helps ensure proper name resolution and accessibility of resources.

NEW QUESTION 8

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

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

Answer: BD

NEW QUESTION 9

Which diagnostic command can you use to show the configured SD-WAN zones and their assigned members?

- A. diagnose sys sdwan zone
- B. diagnose sys sdwan service
- C. diagnose sys sdwan member
- D. diagnose sys sdwan interface

Answer: C

NEW QUESTION 10

What are two common use cases for remote internet access (RIA)? (Choose two.)

- A. Provide direct internet access on spokes
- B. Provide internet access through the hub
- C. Centralize security inspection on the hub
- D. Provide thorough inspection on spokes

Answer: BC

Explanation:

* B. Provide internet access through the hub: This involves routing branch or remote office internet traffic through a central hub, ensuring consistent security policies and possibly better management of network resources.

* C. Centralize security inspection on the hub: With this approach, all internet-bound traffic from various spokes is inspected at the hub, leveraging centralized security mechanisms for thorough inspection and policy enforcement.

NEW QUESTION 10

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
remport=500 locport=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 rcvbyte=387326 nextstat=600 advpns=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
remport=500 locport=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
rcvbyte=345160 nextstat=600 advpns=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
remport=500 locport=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 rcvbyte=387994 nextstat=600 advpns=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
- ? remport: the remote port number
- ? locport: 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
- ? rcvbyte: the number of bytes received
- ? nextstat: the next statistics interval in seconds
- ? advpns: 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 advpns flag for T_MPLS_0 is 0, indicating that it is not a shortcut tunnel, while the advpns flag for T_MPLS_0_0 is 1, indicating that it is a shortcut tunnel.

NEW QUESTION 11

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

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

Answer: AB

Explanation:

The use of an IPsec recommended template offers the advantage of ensuring consistent settings between phase1 and phase2 (A), which is essential for the stability and security of the IPsec tunnel. Additionally, it guides the administrator to use Fortinet's recommended settings (B), which are designed to optimize performance and security based on Fortinet's best practices. References: The benefits of using IPsec recommended templates are outlined in Fortinet's SD-WAN documentation, which emphasizes the importance of consistency and adherence to recommended configurations.

NEW QUESTION 14

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 implicit policy.

NEW QUESTION 19

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 20

Refer to the exhibit.

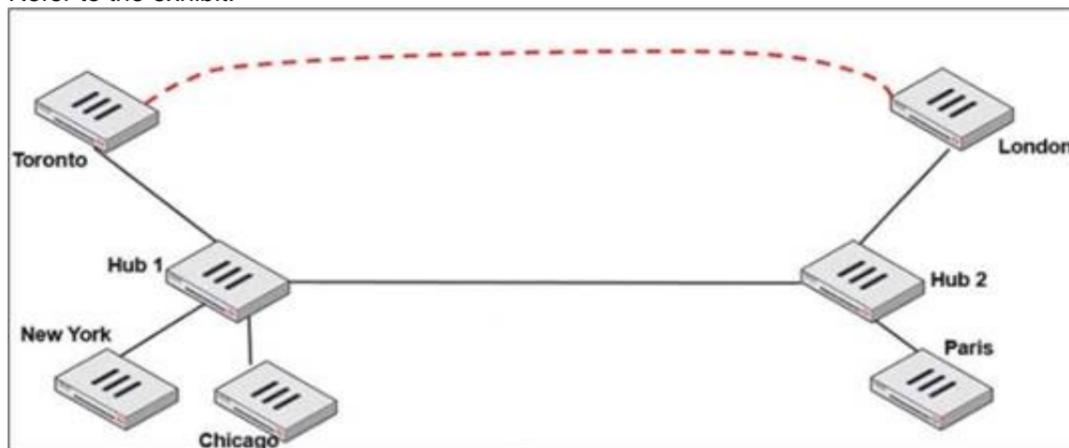
Which two SD-WAN template member settings support the use of FortiManager meta fields? (Choose two.)

- A. Cost
- B. Interface member
- C. Priority
- D. Gateway IP

Answer: BD

NEW QUESTION 21

Refer to the exhibit.



Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2. Which two configuration settings are required for Toronto and London spokes to establish an ADVPN shortcut? (Choose two.)

- A. On the hubs, auto-discovery-sender must be enabled on the IPsec VPNs to spokes.
- B. On the spokes, auto-discovery-receiver must be enabled on the IPsec VPN to the hub.
- C. auto-discovery-forwarder must be enabled on all IPsec VPNs.
- D. On the hubs, net-device must be enabled on all IPsec VPNs.

Answer: AB

NEW QUESTION 26

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 28

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 33

Refer to the exhibit.

```
ike 0:T_INET_0 0:214: received informational request
ike 0:T_INET_0 0:214: processing notify type SHORTCUT_QUERY
ike 0:T_INET_0 0: recv shortcut-query 9065761962601467474
07409008f7fbd17e/0000000000000000 192.2.0.1 10.0.1.101->10.0.2.101 psk 64 ppk 0 ttl 32
nat 0 ver 2 mode 0
ike 0:T_INET_0: iif 20 10.0.1.101->10.0.2.101 route lookup oif 20 T_INET_0 gw
10.201.1.1
ike 0:T_INET_0 1: forward shortcut-query 9065761962601467474
07409008f7fbd17e/0000000000000000 192.2.0.1 10.0.1.101->10.0.2.101 psk 64 ppk 0 ttl 31
ver 2 mode 0, ext-mapping 192.2.0.1:500
```

Which statement about the role of the ADVPN device in handling traffic is true?

- A. This is a spoke that has received a query from a remote hub and has forwarded the response to its hub.
- B. Two hubs, 10.0.1.101 and 10.0.2.101, are receiving and forwarding queries between each other.
- C. This is a hub that has received a query from a spoke and has forwarded it to another spoke.
- D. Two spokes, 192.2.0.1 and 10.0.2.101, forward their queries to their hubs.

Answer: C

NEW QUESTION 34

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 37

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE7_SDW-7.2 Practice Exam Features:

- * NSE7_SDW-7.2 Questions and Answers Updated Frequently
- * NSE7_SDW-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_SDW-7.2 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * NSE7_SDW-7.2 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_SDW-7.2 Practice Test Here](#)