Prepare Smart for Success Free Fortinet NSE7_FSN_AR-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 7 - Secure Networking 7.6 Architect exam PDF questions now. Get authentic NSE7_FSN_AR-7.6 dumps packed with verified answers and secure your certification success with PrepBolt NSE7_FSN_AR-7.6 exam pdf questions and answers.

Thank you for Downloading NSE7_FSN_AR-7.6 exam PDF Demo

https://prepbolt.com/NSE7_FSN_AR-7.6.html

Question 1

Question Type: MultipleChoice

You want to harden the SSL/SSH inspection profile for access to HTTPS web servers.

Which two configuration changes allow you to remove vulnerabilities? (Choose two answers.)

Options:

A- Set unsupported-ssl-version to block.
B- Set Server certificate SNI check to Enable.
C- Set Untrusted SSL certificates to Ignore.
D- Set min-allowed-ssl-version to ssl-3.0.

Answer:

A, B

Explanation:

Setting unsupported-ssl-version to block prevents HTTPS connections from continuing when the negotiated SSL/TLS version falls below the version permitted by the inspection profile. The Enterprise Firewall 7.6 Administrator Study Guide demonstrates this hardening control together with an appropriate minimum version and explains that it can block obsolete TLS versions while accepting newer, secure versions. Therefore, option A is correct.

Enabling Server certificate SNI check protects against hostname inconsistencies between the client-supplied SNI and the server certificate. The FortiOS guide explains that, when enabled, FortiGate uses the certificate's CN when the SNI hostname does not match any CN or SAN entry. This reduces the risk of SNI-based filtering evasion or domain-fronting behavior, making option B correct.

Setting untrusted certificates to Ignore weakens security. FortiGate proceeds with the SSL session regardless of whether the server certificate is trusted. Option C is therefore incorrect.

SSL 3.0 is obsolete and vulnerable, including exposure to POODLE-style attacks. Setting it as the minimum permitted version does not constitute secure hardening. A hardened profile should normally require TLS 1.2 or later, so option D is incorrect.

Question 2

Question Type: MultipleChoice

You use the FortiManager SD-WAN overlay orchestrator to prepare an SD-WAN deployment. Using information provided through the SD-WAN overlay template wizard, FortiManager creates templates that are ready to install on the spoke and hub devices.

Which three templates are created by the SD-WAN overlay orchestrator for a spoke device? (Choose three answers.)

Options:

A- Rules template
B- CLI template
C- IPsec tunnel template
D- BGP template
E- Static route template

Answer:

B, C, D

Explanation:

The SD-WAN 7.6 Enterprise Administrator Study Guide states: ''For branches and hubs, it creates BGP, IPsec, and CLI templates to accommodate all required configuration changes.''

Accordingly, the overlay orchestrator generates the following templates for each spoke:

The IPsec tunnel template configures the spoke as an IPsec dial-up client and applies the tunnel parameters appropriate to the selected topology, authentication method, routing design, and ADVPN settings.

The BGP template configures the spoke's BGP routing, including the autonomous system, neighbor relationships, and either BGP-per-overlay or BGP-on-loopback behavior selected in the wizard.

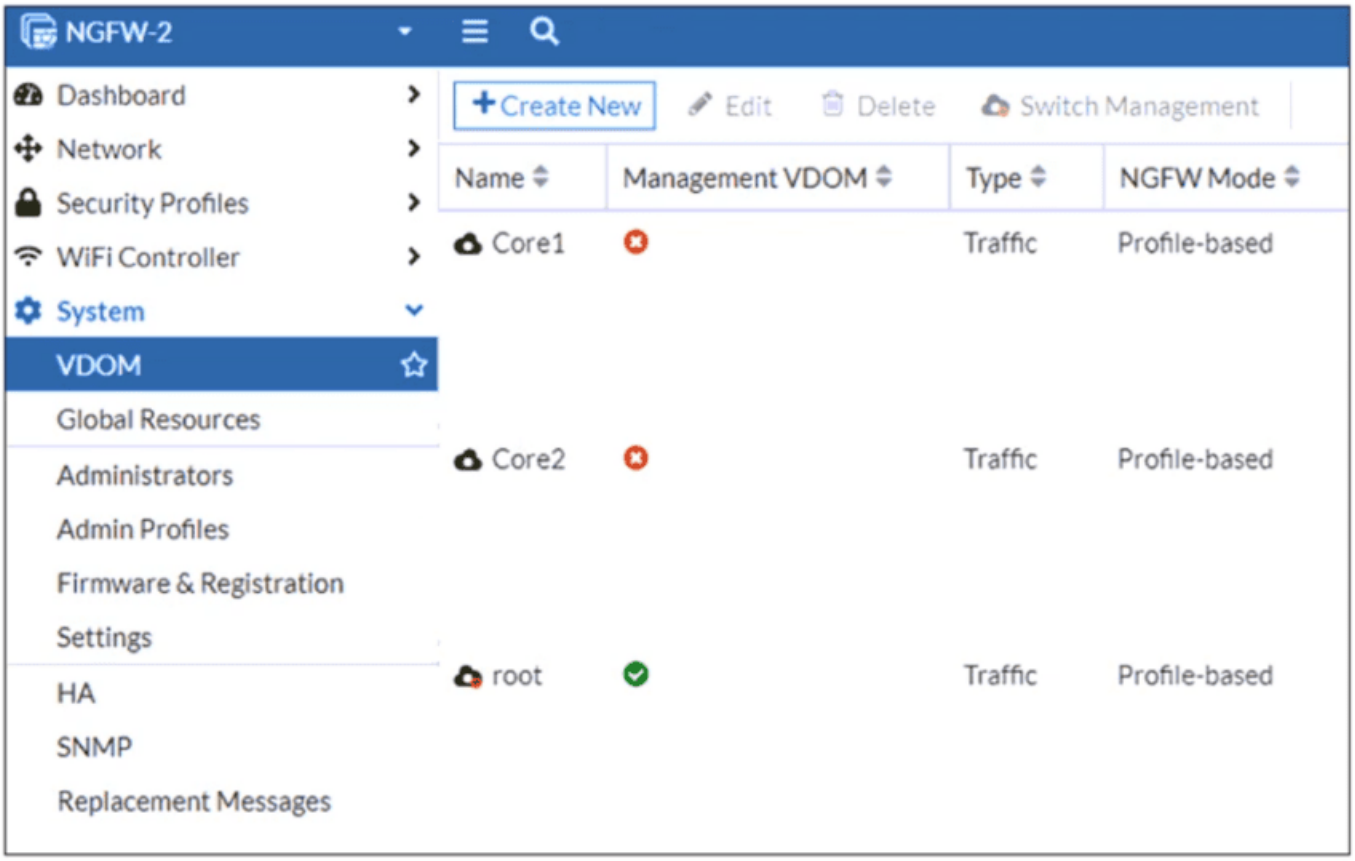
The CLI template supplies additional configuration that cannot be represented entirely by the dedicated IPsec and BGP templates.

The guide separately explains that, for branch devices, FortiManager adds the required members and zones to the defined SD-WAN template. It does not generate a separate rules template for the spoke. Static routes are also not delivered through a dedicated static-route template; routing for the overlay is configured using the generated BGP template. Therefore, options A and E are incorrect.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



The VDOM configuration on a FortiGate device is shown. You discover that web filtering stopped working in Core1 and Core2 after a maintenance window.

What are two reasons why web filtering stopped working? (Choose two answers.)

Options:

A- The root VDOM does not have access to FortiManager in a closed network.
B- The root VDOM does not have access to any valid public Fortinet Distribution Network (FDN) server.
C- The Core1 and Core2 VDOMs must also be enabled as management VDOMs to receive FortiGuard updates.
D- The root VDOM does not use a VDOM link to connect with the Core1 and Core2 VDOMs.

Answer:

A, B

Explanation:

The exhibit identifies the root VDOM as the management VDOM, indicated by the green check mark. The Enterprise Firewall 7.6 Administrator Study Guide explains that the management VDOM handles FortiGuard database downloads, license validation, and FortiGuard rating connectivity on behalf of the entire FortiGate system. It states that FortiGuard updates obtained through the management VDOM ''will affect all VDOMs.''

Consequently, the root VDOM must reach either a public Fortinet Distribution Network server or a FortiManager configured as a FortiGuard Distribution Server in an isolated environment. The guide specifically identifies connectivity to ''a FortiManager serving as a FortiGuard Distribution Server (FDS) in a closed network'' as the alternative to public FortiGuard access. Loss of both paths prevents Core1 and Core2 from using current FortiGuard web-filtering information. Therefore, options A and B are correct.

Core1 and Core2 do not need to become management VDOMs; FortiGate uses one designated management VDOM for these system-level services. A VDOM link is used to route user traffic between VDOMs and is not required for distributing FortiGuard services, eliminating option D.

Question 4

Question Type: MultipleChoice

You configure the overlay tunnels for an SD-WAN hub-and-spoke topology defined with IPsec tunnels, BGP on loopback, and dynamic BGP.

Which two are recommended IPsec settings for this topology? (Choose two answers.)

Options:

A- On the hub, set the tunnel type to static.
B- On the hub, set the parameter mode-cfg to enable.
C- On the spoke, set the parameter net-device to enable.
D- On the spoke, configure the parameter localid.

Answer:

C, D

Explanation:

The SD-WAN 7.6 Enterprise Administrator Study Guide identifies the recommended BGP-on-loopback IPsec settings. For branches, it specifies:

''Static tunnel type (remote end IP address is known).''

''net-device enable.''

Enabling net-device on the spoke creates a kernel interface for the tunnel. This assists with tunnel monitoring and management and is required to support ADVPN shortcut tunnels. Dynamic BGP establishes on-demand BGP peerings between spokes after an ADVPN shortcut is created; therefore, the spoke must support those dynamic shortcut interfaces. This makes option C correct.

The spoke should also configure localid. The FortiOS 7.6 Administrator Study Guide explains: ''Local ID: if the peer accepts a specific peer ID, type that same peer ID in this field.'' The local ID supplies the spoke's IKE identity to the dial-up hub, allowing the hub to identify and authenticate the connecting spoke correctly. Therefore, option D is correct.

Option A reverses the recommended roles. The hub must use a dynamic tunnel type because it operates as the dial-up server and does not require every spoke's changing public gateway address in advance.

Option B is also incorrect. The guide states: ''There is no need to configure any tunnel IP address, so the IKE Mode Config is not used.'' BGP on loopback uses the loopback address and exchange-interface-ip instead of IKE mode configuration.

Question 5

Question Type: MultipleChoice

Refer to the exhibits.

FortiGate Diagnose Output

```
branch1_fgt # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority), link-cost-factor
(latency), link-cost-threshold(10), health-check(Corp_HC)
  Members(2):
    1: Seq_num(2 port2 underlay), alive, latency: 0.971, selected
    2: Seq_num(1 port1 underlay), alive, latency: 1.170, selected
  Application Control(3): Salesforce(16920,0) Microsoft.Portal(41469,0) Microsoft.Outlook(15816,0)

  Src address(1):
        10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x24200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla hash-mode=round-robin)
  Members(2):
    1: Seq_num(3 port7 SiteA), alive, sla(0x1), gid(2), num of pass(1), selected
    2: Seq_num(4 port8 SiteA), alive, sla(0x1), gid(2), num of pass(1), selected
  Src address(1):
        10.0.1.0-10.0.1.255
  Dst address(1):
        128.66.0.0-128.66.255.255
```

FortiGate Routing Table

```
branch1_fgt # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 192.2.0.2, port1, [1/0]
                  [5/0] via 192.2.0.10, port2, [1/0]
C       10.0.1.0/24 is directly connected, port7
                    is directly connected, port8
C       10.0.2.0/24 is directly connected, port5
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4, [1/0]
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
```

How does FortiGate handle traffic with the source IP address 10.0.1.125 and the destination IP address 128.66.0.125?

Options:

A- FortiGate routes the traffic flow according to the forwarding information base (FIB).
B- FortiGate steers the traffic flow through port7.
C- FortiGate load balances the traffic flow through port7 and port8.
D- FortiGate drops the traffic flow.

Answer:

A

Explanation:

The traffic matches service 2's address criteria: 10.0.1.125 belongs to the configured source range 10.0.1.0--10.0.1.255, and 128.66.0.125 belongs to the destination range 128.66.0.0--128.66.255.255. Service 2 lists port7 and port8 as selected SLA members and uses round-robin load balancing.

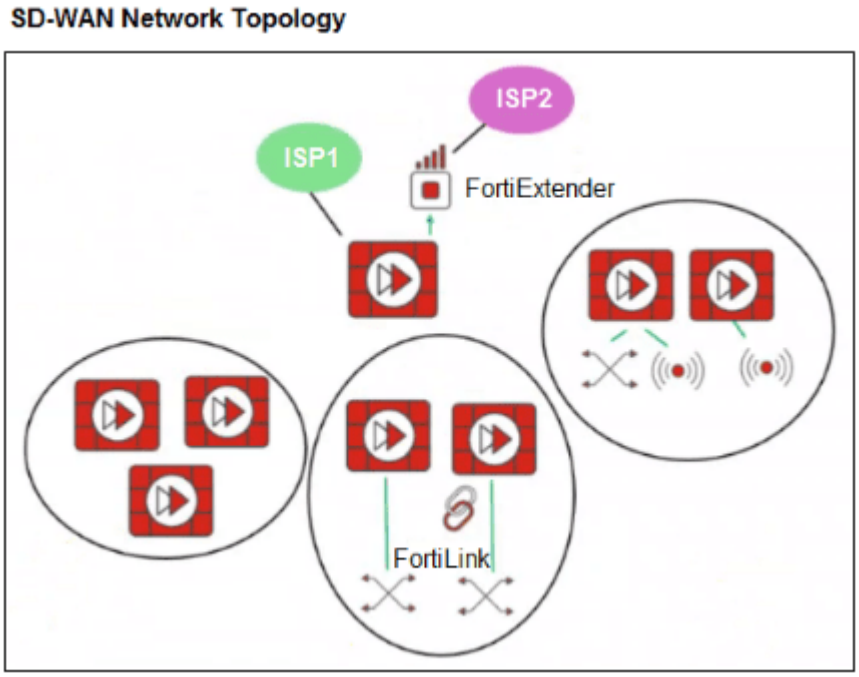
However, the SD-WAN guide states: ''SD-WAN requires a valid route in the forwarding information base (FIB) so the member can be used to steer traffic.'' The routing table contains routes through port7 and port8 only for 10.0.1.0/24. It contains no route to 128.66.0.125 through either member.

The only route covering the destination is the default route, which has equal-cost paths through port1 and port2. Consequently, port7 and port8 cannot be used for this flow despite being SLA-selected. FortiGate skips the unusable explicit SD-WAN rule and processes the traffic through the implicit rule using standard FIB routing. Therefore, option A is correct. Options B and C incorrectly assume that selected overrides route availability, while option D is incorrect because valid default routes exist.

Question 6

Question Type: MultipleChoice

Refer to the exhibit.



You want to configure SD-WAN on a network, as shown in the exhibit. The network contains many FortiGate devices. Some are used as next-generation firewalls (NGFWs), and some are deployed with extensions such as FortiSwitch, FortiAP, or FortiExtender.

Which factor should you consider when planning the deployment? (Choose one answer.)

Options:

A- You can build an SD-WAN topology that includes all devices. The hubs must be devices without extensions.
B- You should exclude FortiGate devices with FortiLink connections from the SD-WAN topology.
C- You should build multiple SD-WAN topologies. Each topology should contain only one type of extension.
D- You can build an SD-WAN topology that includes all devices. The hubs can be FortiGate devices with FortiExtender.

Answer:

D

Explanation:

The SD-WAN 7.6 Enterprise Administrator Study Guide states: ''An SD-branch is a site with an SD-WAN spoke FortiGate device and one or multiple extensions.'' It explains that FortiSwitch and FortiAP provide wired and wireless LAN connectivity through FortiLink, while FortiExtender supplements WAN connectivity by providing 4G/5G transport.

The guide further explains that the management plane sees extension-device ports as logical interfaces belonging to the controlling FortiGate. Therefore, FortiSwitch, FortiAP, and FortiExtender do not become independent SD-WAN topology nodes and do not require separate topologies. FortiGate devices with FortiLink connections also do not need to be excluded.

FortiExtender is specifically designed as a natural SD-WAN extension that introduces cellular connectivity as another WAN transport. Consequently, a FortiGate using FortiExtender can function as a hub, provided it satisfies the required capacity, routing, and IPsec design requirements. There is no rule requiring hubs to be extension-free. Therefore, option D correctly describes the unified topology shown in the exhibit.

Thank You for trying NSE7_FSN_AR-7.6 PDF Demo

To try our NSE7_FSN_AR-7.6 practice exam software visit link below

https://prepbolt.com/NSE7_FSN_AR-7.6.html

Start Your NSE7_FSN_AR-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE7_FSN_AR-7.6 preparation with actual exam questions.