

New FCSS_EFW_AD-7.6 Test Bootcamp, FCSS_EFW_AD-7.6 Practice Online



2026 Latest Prep4sureExam FCSS_EFW_AD-7.6 PDF Dumps and FCSS_EFW_AD-7.6 Exam Engine Free Share:
https://drive.google.com/open?id=1A00G_ysZk1HVsoLQLf_pxId96XqJUGzd

Fortinet FCSS_EFW_AD-7.6 can ensure your success. So here comes Fortinet, who provides you with the Fortinet FCSS_EFW_AD-7.6 exam dumps to get your dream Fortinet FCSS_EFW_AD-7.6 certification with no hassle. Fortinet FCSS_EFW_AD-7.6 Certification will add up to your excellence in your field and leave no space for any doubts in the mind of the hiring team.

Fortinet FCSS_EFW_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">Central Management: This section of the exam measures the skills of a Security Operations Manager and covers the implementation of centralized management systems for coordinated control and oversight of distributed Fortinet security infrastructures across enterprise environments.
Topic 2	<ul style="list-style-type: none">VPN: This section of the exam measures the skills of a VPN Solutions Engineer and covers the implementation of various virtual private network technologies. It includes configuring IPsec VPN using IKE version 2 protocols and implementing Automatic Discovery VPN solutions to establish on-demand secure tunnels between multiple sites within an enterprise network infrastructure.
Topic 3	<ul style="list-style-type: none">System Configuration: This section of the exam measures the skills of a Network Security Architect and covers the implementation and integration of core Fortinet infrastructure components. It includes deploying the Security Fabric, enabling hardware acceleration, configuring high availability operational modes, and designing enterprise networks utilizing VLANs and VDOM technologies to meet specific organizational requirements.
Topic 4	<ul style="list-style-type: none">Routing: This section of the exam measures the skills of a Network Infrastructure Engineer and covers the implementation of dynamic routing protocols for enterprise network traffic management. It includes configuring both OSPF and BGP routing protocols to ensure efficient and reliable data transmission across complex organizational networks.

Topic 5	<ul style="list-style-type: none"> • Security Profiles: This section of the exam measures the skills of a Threat Prevention Specialist and covers the configuration and management of comprehensive security profiling systems. It includes implementing SSL • SSH inspection, combining web filtering and application control mechanisms, integrating intrusion prevention systems, and utilizing the Internet Service Database to create layered security protections for organizational networks.
---------	--

>> New FCSS_EFW_AD-7.6 Test Bootcamp <<

Fortinet FCSS_EFW_AD-7.6 Practice Online - FCSS_EFW_AD-7.6 Test Torrent

In this version, you don't need an active internet connection to use the FCSS_EFW_AD-7.6 practice test software. This software mimics the style of real test so that users find out pattern of the real test and kill the exam anxiety. Prep4sureExam offline practice exam is customizable and users can change questions and duration of FCSS - Enterprise Firewall 7.6 Administrator (FCSS_EFW_AD-7.6) mock tests. All the given practice questions in the desktop software are identical to the FCSS - Enterprise Firewall 7.6 Administrator (FCSS_EFW_AD-7.6) actual test.

Fortinet FCSS - Enterprise Firewall 7.6 Administrator Sample Questions (Q49-Q54):

NEW QUESTION # 49

What is the initial step performed by FortiGate when handling the first packets of a session?

- A. Installation of the session key in the network processor (NP)
- B. **Security inspections such as ACL, HPE, and IP integrity header checking**
- C. Data encryption and decryption
- D. Offloading the packets directly to the content processor (CP)

Answer: B

Explanation:

When FortiGate processes the first packets of a session, it follows a sequence of steps to determine how the traffic should be handled before establishing a session. The initial step involves:

Access Control List (ACL) checks: Determines if the traffic should be allowed or blocked based on predefined security rules.

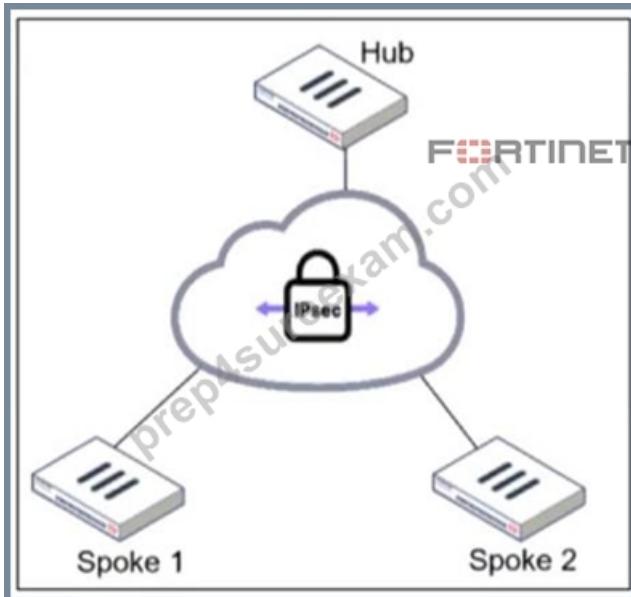
Hardware Packet Engine (HPE) inspections: Ensures that packet headers are valid and comply with protocol standards.

IP Integrity Header Checking: Verifies if the IP headers are intact and not malformed or spoofed.

Once these security inspections are completed and the session is validated, FortiGate then installs the session in hardware (if offloading is enabled) or processes it in software.

NEW QUESTION # 50

Refer to the exhibit.



An administrator is deploying a hub and spokes network and using OSPF as dynamic protocol. Which configuration is mandatory for neighbor adjacency?

- A. Set virtual-link enable in the hub interface
- B. Set bfd enable in the router configuration
- C. Set network-type point-to-multipoint in the hub interface
- D. Set rfc1583-compatible enable in the router configuration

Answer: C

Explanation:

In a hub-and-spoke topology using OSPF over IPsec VPNs, the point-to-multipoint network type is necessary to establish neighbor adjacencies between the hub and spokes. This network type ensures that OSPF operates correctly without requiring a designated router (DR) and allows dynamic routing updates across the IPsec tunnels.

NEW QUESTION # 51

Refer to the exhibit.

Routing table on FortiGate_A

```
FortiGate_A # 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 [10/0] via 10.1.0.254, port1, [1/0]
C  10.1.0.0/24 is directly connected, port1
C  10.1.4.0/24 is directly connected, port3
B  100.64.1.0/24 [200/0] via 10.1.0.254 (recursive is directly connected, port1), 00:39:45, [1/0]
B  172.16.1.252/30 [200/0] via 10.1.0.1 (recursive is directly connected, port1), 00:42:48, [1/0]
C  172.16.100.0/24 is directly connected, port8
```

Routing table on FortiGate_B

```
FortiGate_B # 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 [10/0] via 10.1.0.254, port1, [1/0]
S  4.2.2.2/32 [10/0] via 10.1.5.254, port4, [1/0]
C  10.1.0.0/24 is directly connected, port1
B  10.1.4.0/24 [200/0] via 10.1.0.100 (recursive is directly connected, port1), 00:41:02, [1/0]
C  10.1.5.0/24 is directly connected, port4
B  100.64.1.0/24 [200/0] via 10.1.0.254 (recursive is directly connected, port1), 00:38:14, [1/0]
C  172.16.1.248/30 is directly connected, C0
C  172.16.1.252/30 is directly connected, A0
C  172.16.100.0/24 is directly connected, port8
```



The routing tables of FortiGate_A and FortiGate_B are shown. FortiGate_A and FortiGate_B are in the same autonomous system. The administrator wants to dynamically add only route 172.16.1.248/30 on FortiGate_A. What must the administrator configure?

- A. Enable Redistribute Connected in the BGP section on FortiGate_B.
- B. The prefix 172.16.1.248/30 in the BGP Networks section on FortiGate_B
- C. A BGP route map out for 172.16.1.248/30 on FortiGate_B**
- D. A BGP route map in for 172.16.1.248/30 on FortiGate_A

Answer: C

Explanation:

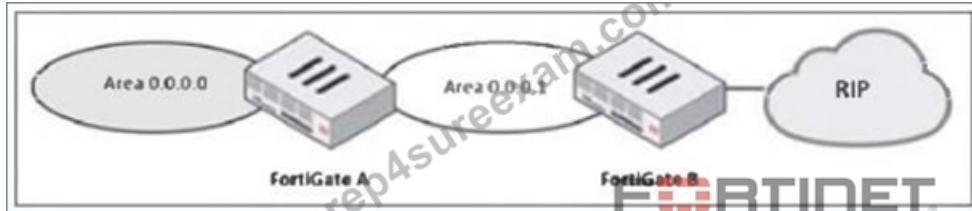
FortiGate_A and FortiGate_B are in the same autonomous system (AS), and FortiGate_A does not currently have route 172.16.1.248/30 in its routing table. However, FortiGate_B has this route as a connected route.

To dynamically advertise only 172.16.1.248/30 from FortiGate_B to FortiGate_A, the administrator must configure a BGP route map out on FortiGate_B that specifically permits only this prefix.

A BGP route map out on FortiGate_B controls which routes FortiGate_B advertises to FortiGate_A. If no filtering is applied, FortiGate_B might advertise all BGP-learned and connected routes, which is not what the administrator wants. The route map should include a prefix-list that explicitly allows only 172.16.1.248/30 and denies everything else.

NEW QUESTION # 52

Refer to the exhibit, which shows a partial enterprise network.



An administrator would like the area 0.0.0.0 to detect the external network.

What must the administrator configure?

- A. Set the area 0.0.0.1 type to stub on FortiGate A and B.
- B. **Enable RIP redistribution on FortiGate B.**
- C. Configure a distribute-route-map-in on FortiGate B.
- D. Configure a virtual link between FortiGate A and B.

Answer: B

Explanation:

The diagram shows a multi-area OSPF network where:

FortiGate A is in OSPF Area 0 (Backbone area).

FortiGate B is in OSPF Area 0.0.0.1 and is connected to an RIP network.

To ensure that OSPF Area 0 (0.0.0.0) learns routes from the external RIP network, FortiGate B must redistribute RIP routes into OSPF.

Steps to achieve this:

1. Enable route redistribution on FortiGate B to inject RIP-learned routes into OSPF.
2. This allows OSPF Area 0.0.0.1 to forward RIP routes to OSPF Area 0 (0.0.0.0), making the external network visible.

NEW QUESTION # 53

Refer to the exhibit, which shows the packet capture output of a three-way handshake between FortiGate and FortiManager Cloud.

Packet capture output of three-way handshake between a FortiGate and a FortiManager Cloud

```

> Frame 35: 1034 bytes on wire (8272 bits), 1034 bytes captured (8272 bits) on interface -, id 0
> Ethernet II, Src: 50:e5:d5: (50:e5:d5:), Dst: Fortinet_ (e0:23:ff: )
> Internet Protocol Version 4, Src: 192.168.2.60, Dst: 154.52.4.164
> Transmission Control Protocol, Src Port: 16304, Dst Port: 541, Seq: 1, Ack: 1, Len: 980
  ▾ Transport Layer Security
    ▾ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 975
    ▾ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 971
    > Version: TLS 1.2 (0x0303)
      Random: a14f6c4b8f9313bf
      Session ID Length: 32
      Session ID: a0de426e96e83a5
      Cipher Suites Length: 34
      > Cipher Suites (17 suites)
      Compression Methods Length: 1
      > Compression Methods (1 method)
      Extensions Length: 864
    ▾ Extension: server_name (len=45) name=9398.support.fortinet-ca2.fortinet.com
      Type: server_name (0)
      Length: 45
    ▾ Server Name Indication extension
      Server Name list length: 43
      Server Name Type: host_name (0)
      Server Name length: 40
      Server Name: 9398.support.fortinet-ca2.fortinet.com
    > Extension: ec_point_formats (len=4)
    > Extension: supported_groups (len=22)
    > Extension: session_ticket (len=0)
    > Extension: encrypt_then_mac (len=0)
    > Extension: extended_master_secret (len=0)
    > Extension: signature_algorithms (len=48)
    > Extension: supported_versions (len=9) TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0
    > Extension: psk_key_exchange_modes (len=2)
  
```

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

- A. The wildcard for the domain *.fortinet-ca2.support.fortinet.com must be supported by FortiManager Cloud.
- B. FortiGate will receive a certificate that supports multiple domains because FortiManager operates in a cloud computing environment.
- C. FortiGate is connecting to the same IP server and will receive an independent certificate for its connection between FortiGate and FortiManager Cloud.
- D. If the TLS handshake contains 17 cipher suites it means the TLS version must be 1.0 on this three-way handshake.

Answer: A

Explanation:

The packet capture output displays a TLS Client Hello message from FortiGate to FortiManager Cloud. This message contains Server Name Indication (SNI), which is used to indicate the domain name that FortiGate is trying to connect to.

FortiGate will receive a certificate that supports multiple domains because FortiManager operates in a cloud computing environment.

FortiManager Cloud hosts multiple customers and domains under a shared infrastructure.

The TLS handshake includes SNI (Server Name Indication), which allows FortiManager Cloud to serve multiple certificates based on the requested domain.

This means FortiGate will likely receive a multi-domain or wildcard certificate that can be used for multiple customers under FortiManager Cloud.

The wildcard for the domain .fortinet-ca2.support.fortinet.com must be supported by FortiManager Cloud.

The SNI extension contains the domain 9398.support.fortinet-ca2.fortinet.com

FortiManager Cloud must support wildcard certificates such as *.fortinet-ca2.support.fortinet.com to securely manage multiple subdomains and customers.

This ensures that FortiGate can validate the server certificate without any TLS errors.

NEW QUESTION # 54

.....

Our product boosts varied functions to be convenient for you to master the FCSS_EFW_AD-7.6 training materials and get a good preparation for the exam and they include the self-learning, the self-assessment, stimulating the exam and the timing function. We provide 24-hours online on FCSS_EFW_AD-7.6 Guide prep customer service and the long-distance professional personnel assistance to for the client. If clients have any problems about our FCSS_EFW_AD-7.6 study materials they can contact our

customer service anytime.

FCSS_EFW_AD-7.6 Practice Online: https://www.prep4sureexam.com/FCSS_EFW_AD-7.6-dumps-torrent.html

DOWNLOAD the newest Prep4sureExam FCSS_EFW_AD-7.6 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1A00G_ysZk1HVs0LQLf_pxId96XqJUGzd