

# Fortinet

## Exam Questions FCSS\_EFW\_AD-7.6

FCSS - Enterprise Firewall 7.6 Administrator



**NEW QUESTION 1**

A company's users on an IPsec VPN between FortiGate A and B have experienced intermittent issues since implementing VXLAN. The administrator suspects that packets exceeding the 1500-byte default MTU are causing the problems.

In which situation would adjusting the interface's maximum MTU value help resolve issues caused by protocols that add extra headers to IP packets?

- A. Adjust the MTU on interfaces only if FortiGate has the FortiGuard enterprise bundle, which allows MTU modification.
- B. Adjust the MTU on interfaces in all FortiGate devices that support the latest family of Fortinet SPUs: NP7, CP9 and SP5.
- C. Adjust the MTU on interfaces in controlled environments where all devices along the path allow MTU interface changes.
- D. Adjust the MTU on interfaces only in wired connections like PPPoE, optic fiber, and ethernet cable.

**Answer: C**

**NEW QUESTION 2**

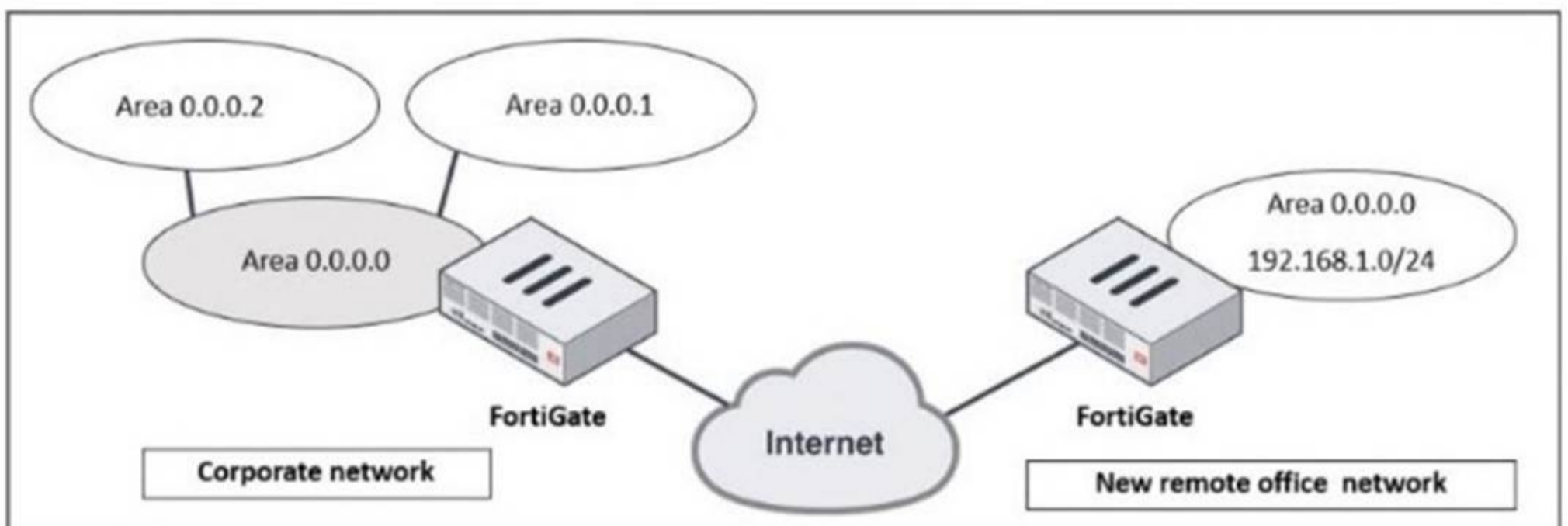
The IT department discovered during the last network migration that all zero phase selectors in phase 2 IPsec configurations impacted network operations. What are two valid approaches to prevent this during future migrations? (Choose two.)

- A. Use routing protocols to specify allowed subnets over the tunnel.
- B. Configure an IPsec-aggregate to create redundancy between each firewall peer.
- C. Clearly indicate to the VPN which segments will be encrypted in the phase two selectors.
- D. Configure an IP address on the IPsec interface of each firewall to establish unique peer connections and avoid impacting network operations.

**Answer: AC**

**NEW QUESTION 3**

Refer to the exhibit, which shows a corporate network and a new remote office network.



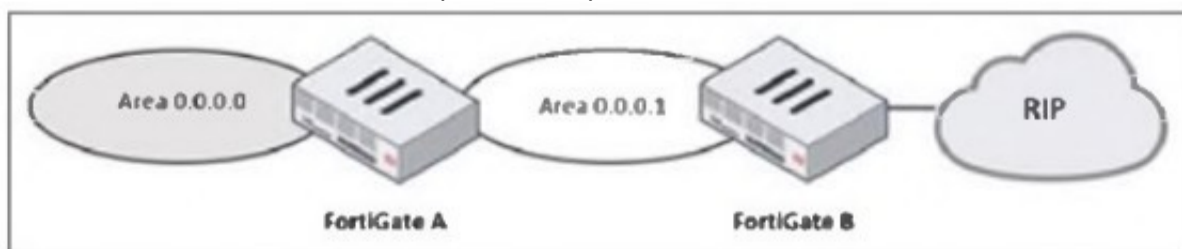
An administrator must integrate the new remote office network with the corporate enterprise network. What must the administrator do to allow routing between the two networks?

- A. The administrator must implement BGP to inject the new remote office network into the corporate FortiGate device
- B. The administrator must configure a static route to the subnet 192.168.1.0/24 on the corporate FortiGate device.
- C. The administrator must configure virtual links on both FortiGate devices.
- D. The administrator must implement OSPF over IPsec on both FortiGate devices.

**Answer: D**

**NEW QUESTION 4**

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

**Answer: A**

**NEW QUESTION 5**

An administrator needs to install an IPS profile without triggering false positives that can impact applications and cause problems with the user's normal traffic flow. Which action can the administrator take to prevent false positives on IPS analysis?

- A. Use the IPS profile extension to select an operating system, protocol, and application for all the network internal services and users to prevent false positives.
- B. Enable Scan Outgoing Connections to avoid clicking suspicious links or attachments that can deliver botnet malware and create false positives.
- C. Use an IPS profile with action monitor, however, the administrator must be aware that this can compromise network integrity.
- D. Install missing or expired SSUTLS certificates on the client PC to prevent expected false positives.

**Answer:** A

#### **NEW QUESTION 6**

An administrator wants to scale the IBGP sessions and optimize the routing table in an IBGP network. Which parameter should the administrator configure?

- A. network-import-check
- B. ibgp-enforce-multihop
- C. neighbor-group
- D. route-reflector-client

**Answer:** D

#### **NEW QUESTION 7**

A company's guest internet policy, operating in proxy mode, blocks access to Artificial Intelligence Technology sites using FortiGuard. However, a guest user accessed a page in this category using port 8443.

Which configuration changes are required for FortiGate to analyze HTTPS traffic on nonstandard ports like 8443 when full SSL inspection is active in the guest policy?

- A. Add a URL wildcard domain to the website CA certificate and use it in the SSL/SSH Inspection Profile.
- B. In the Protocol Port Mapping section of the SSL/SSH Inspection Profile, enter 443, 8443 to analyze both standard (443) and non-standard (8443) HTTPS ports.
- C. To analyze nonstandard ports in web filter profiles, use TLSv1.3 in the SSL/SSH Inspection Profile.
- D. Administrators can block traffic on nonstandard ports by enabling the SNI check in the SSL/SSH Inspection Profile.

**Answer:** B

#### **NEW QUESTION 8**

A FortiGate device with UTM profiles is reaching the resource limits, and the administrator expects the traffic in the enterprise network to increase. The administrator has received an additional FortiGate of the same model.

Which two protocols should the administrator use to integrate the additional FortiGate device into this enterprise network? (Choose two.)

- A. FGSP with external load balancers
- B. FGCP in active-active mode and with switches
- C. FGCP in active-passive mode and with VDOM disabled
- D. VRRP with switches

**Answer:** AB

#### **NEW QUESTION 9**

Refer to the exhibit, which contains a partial VPN configuration.

```

config vpn ipsec phase1-interface
edit tunnel
set type dynamic
set interface "port1"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256 aes256-sha256
set dpd on-idle
set add-route enable
set psksecret fortinet
next
end

```

What can you conclude from this VPN IPsec phase 1 configuration?

- A. This configuration is the best for networks with regular traffic intervals, providing a balance between connectivity assurance and resource utilization.
- B. Peer IDs are unencrypted and exposed, creating a security risk.
- C. FortiGate will not add a route to its routing or forwarding information base when the dynamic tunnel is negotiated.
- D. A separate interface is created for each dial-up tunnel, which can be slower and more resource intensive, especially in large networks.

Answer: A

**NEW QUESTION 10**

What action can be taken on a FortiGate to block traffic using IPS protocol decoders, focusing on network transmission patterns and application signatures?

- A. Use the DNS filter to block application signatures and protocol decoders.
- B. Use application control to limit non-URL-based software handling.
- C. Enable application detection-based SD-WAN rules.
- D. Configure a web filter profile in flow mode.

Answer: B

**NEW QUESTION 10**

Refer to the exhibit, which shows a command output.

```

FortiGate_B # get system session list | grep icmp

FortiGate_B #

```

FortiGate\_A and FortiGate\_B are members of an FGSP cluster in an enterprise network. While testing the cluster using the ping command, the administrator monitors packet loss and found that the session output on FortiGate\_B is as shown in the exhibit. What could be the cause of this output on FortiGate\_B?

- A. The session synchronization is encrypted.
- B. session-pickup-connectionless is set to disable on FortiGate\_B.
- C. FortiGate\_B is configured in passive mode.
- D. FortiGate\_A and FortiGate\_B have the same standalone-group-id value.

Answer: B

**NEW QUESTION 13**

An administrator must minimize CPU and RAM use on a FortiGate firewall while also enabling essential security features, such as web filtering and application control for HTTPS traffic.

Which SSL inspection setting helps reduce system load while also enabling security features, such as web filtering and application control for encrypted HTTPS traffic?

- A. Use full SSL inspection to thoroughly inspect encrypted payloads.
- B. Disable SSL inspection entirely to conserve resources.
- C. Configure SSL inspection to handle HTTPS traffic efficiently.
- D. Enable SSL certificate inspection mode to perform basic checks without decrypting traffic.

**Answer: D**

**NEW QUESTION 14**

Refer to the exhibit, which shows a physical topology and a traffic log.



The administrator is checking on FortiAnalyzer traffic from the device with IP address 10.1.10.1, located behind the FortiGate ISFW device. The firewall policy in on the ISFW device does not have UTM enabled and the administrator is surprised to see a log with the action Malware, as shown in the exhibit.

What are the two reasons FortiAnalyzer would display this log? (Choose two.)

- A. Security rating is enabled in ISFW.
- B. ISFW is in a Security Fabric environment.
- C. ISFW is not connected to FortiAnalyzer and must go through NGFW-1.
- D. The firewall policy in NGFW-1 has UTM enabled.

**Answer: BD**

**NEW QUESTION 19**

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

Answer: D

**NEW QUESTION 23**

.....

## **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

### **FCSS\_EFW\_AD-7.6 Practice Exam Features:**

- \* FCSS\_EFW\_AD-7.6 Questions and Answers Updated Frequently
- \* FCSS\_EFW\_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff
- \* FCSS\_EFW\_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* FCSS\_EFW\_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The FCSS\\_EFW\\_AD-7.6 Practice Test Here](#)**