ITCertTest

ITCERTTEST
IT Exam study guide / simulations

http://www.itcerttest.com

IT exam study guide / simulations

Exam : **FCSS_EFW_AD-7.6**

Title : FCSS - Enterprise Firewall 7.6 Administrator

Vendor : Fortinet

Version : DEMO

NO.1 Refer to the exhibit, which contains the partial output of an OSPF command.
An administrator is checking the OSPF status of a FortiGate device and receives the output shown in the exhibit.
Which statement on this FortiGate device is correct?
A. The FortiGate device can inject external routing information.
B. The FortiGate device is in the area 0.0.0.5.
C. The FortiGate device does not support OSPF ECMP.
D. The FortiGate device is a backup designated router.
Answer: A
Explanation:
From the OSPF status output, the key information is:
" This router is an ASBR " # This means the FortiGate is acting as an Autonomous System Boundary Router (ASBR).
An ASBR is responsible for injecting external routing information into OSPF from another routing protocol (such as BGP, static routes, or connected networks).

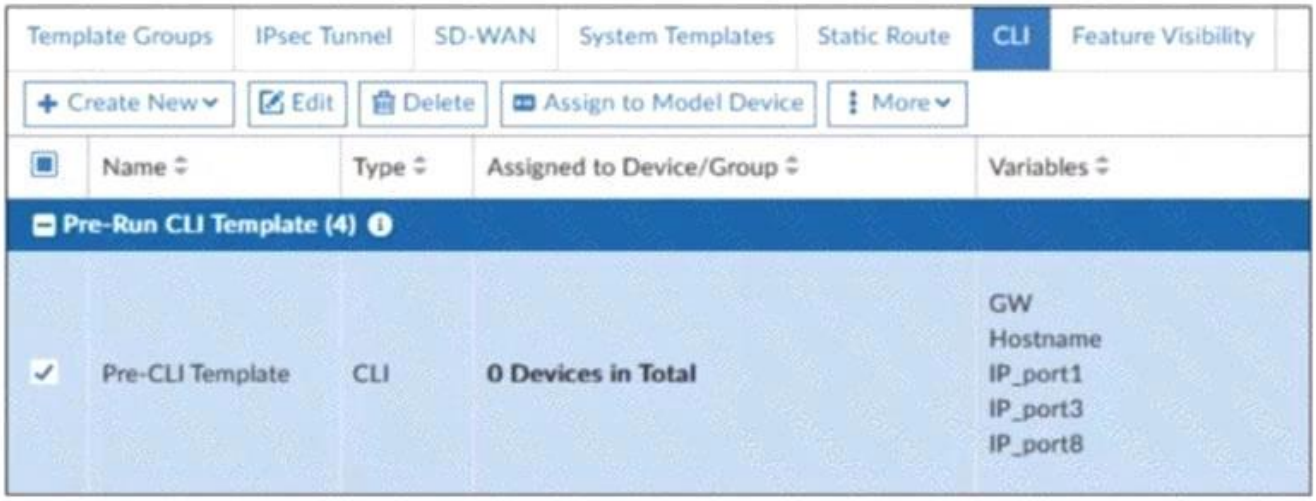
NO.2 Refer to the exhibit.
The routing tables of FortiGate_A and FortiGate_B are shown. FortiGate_A and FortiGate_B are in the same autonomous system.
The administrator wants to dynamically add only route 172.16.1.248/30 on FortiGate_A.
What must the administrator configure?
A. A BGP route map in for 172.16.1.248/30 on FortiGate_A
B. Enable Redistribute Connected in the BGP section on FortiGate_
C. The prefix 172.16.1.248/30 in the BGP Networks section on FortiGate_B
D. A BGP route map out for 172.16.1.248/30 on FortiGate_B
Answer: D

NO.3 What can be inferred from the OSPF status output shown?
A. Is ASBR
B. Is BDR
C. Supports ECMP
D. Is in area 0.0.0.5
Answer: A
Explanation:
Comprehensive and Detailed Explanation From Exact Extract documents and Knowledge:
In an OSPF status output (typically retrieved via get router info ospf status), the unit identifies its role within the OSPF autonomous system. If the output indicates that the device is an ASBR (Autonomous System Boundary Router) , it means the FortiGate is redistributing routes from another protocol (like BGP, RIP, or static routes) into OSPF. The status will explicitly state " This router is an ASBR " if redistribution is active.
This role is critical for providing connectivity between OSPF and external networks.

NO.4 You must configure a loopback as a BGP source to connect to the ISP.
Which two commands must you use to establish the connection? (Choose two.)

A. ebgp-enforce-multihop
B. update-source
C. ibgp-enforce-multihop
D. recursive-next-hop
Answer: A B
Explanation:
When configuring a BGP peering session with an external neighbor (eBGP), such as an ISP, using a loopback interface as the source, two specific configuration requirements must be met in FortiOS:
* update-source (B): By default, BGP uses the IP address of the physical egress interface to initiate the TCP connection to a neighbor. If you want the BGP session to be sourced from a loopback interface (which is a common practice for stability, as loopbacks do not go down unless the entire router fails), you must explicitly define this using the set update-source < interface > command under the neighbor configuration.
* ebgp-enforce-multihop (A): Standard eBGP sessions have a default Time-to-Live (TTL) of 1, meaning the peer is expected to be directly connected. When peering using loopback addresses, the loopback interface is logically one hop away from the physical link. Therefore, the connection will fail unless you increase the TTL. The set ebgp-enforce-multihop < hop-count > command allows the BGP session to be established even if the peer is not on a directly connected subnet or if loopbacks are used.
In the provided exhibit (image_bd178a.jpg), the CLI shows the neighbor configuration. To successfully peer with the ISP (10.200.3.1) using a local loopback, the administrator would need to add:
* set update-source " loopback0 "
* set ebgp-enforce-multihop 2 (or a higher value)

NO.5 Refer to the exhibit.
A pre-run CLI template that is used in zero-touch provisioning (ZTP) and low-touch provisioning (LTP) with FortiManager is shown.



The template is not assigned even though the configuration has already been installed on FortiGate.
What is true about this scenario?
A. The administrator did not assign the template correctly when adding the model device because pre-CLI templates remain permanently assigned to the firewall
B. Pre-run CLI templates are automatically unassigned after their initial installation
C. Pre-run CLI templates for ZTP and LTP must be unassigned manually after the first installation to avoid conflicting error objects when importing a policy package

D. The administrator must use post-run CLI templates that are designed for ZTP and LTP

Answer: B

Explanation:

In FortiManager, pre-run CLI templates are used in Zero-Touch Provisioning (ZTP) and Low-Touch Provisioning (LTP) to configure a FortiGate device before it is fully managed by FortiManager. These templates apply configurations when a device is initially provisioned. Once the pre-run CLI template is executed, FortiManager automatically unassigns it from the device because it is not meant to persist like other policy configurations. This prevents conflicts and ensures that the FortiGate configuration is not repeatedly applied after the initial setup.

NO.6 Which action should you take after applying a block-all IPS profile that caused applications to stop working?

A. Disable IPS

B. Use monitor mode

C. Enable flow mode

D. Remove server targets

Answer: B

Explanation:

In high-security environments, applying a restrictive IPS profile can sometimes lead to false positives , where legitimate application traffic is incorrectly identified as a threat and blocked. The standard troubleshooting procedure is to change the signature action to monitor mode .

Monitor mode allows the traffic to pass through while still generating logs in FortiAnalyzer or the FortiGate dashboard. By reviewing these logs, an administrator can identify the exact signature ID causing the issue and subsequently create an IPS sensor override or exception for that specific traffic, ensuring the application works while maintaining security for other threats.

NO.7 How can FortiGate_B advertise only 172.16.1.248/30 using BGP?

A. Redistribute connected

B. Route map out

C. Prefix list in

D. Network

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract documents and Knowledge:

In BGP (Border Gateway Protocol), there are two primary ways to inject routes into the BGP table: using the network command or through redistribution. The network command is the standard and most precise method for advertising a specific prefix that already exists in the local routing table.

In the lab environment, " Link C " is identified as the subnet 172.16.1.248/30 , which is directly connected to the FortiGate. By using the Network command (e.g., set network 172.16.1.248 255.255.255.252), the administrator ensures that only this specific prefix is advertised to BGP neighbors. In contrast, " Redistribute connected " (Option A) would advertise every directly connected network on the device, which would require an additional " Route map out " (Option B) to filter, making the " Network " command the most direct and correct configuration for the requirement.

NO.8 How do you resolve object conflicts when importing a policy package?

A. Rename

B. FortiManager accept

C. Non-default

D. Retrieve config

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract documents and Knowledge:

When importing a policy package from a FortiGate into a FortiManager ADOM, the Import Wizard compares the objects on the FortiGate with the objects already existing in the FortiManager ADOM database. If an object (e.g., an Address Object) has the same name but different values, a conflict occurs.

* To resolve this, the administrator must choose which version to keep. Choosing FortiManager accept (or " Use FortiManager value ") resolves the conflict by keeping the existing object in the FortiManager database and applying its settings to the imported policy. This maintains global consistency across the ADOM.

NO.9 What does the command set forward-domain < domain_ID > in a transparent VDOM interface do?

A. It configures the interface to prioritize traffic based on the domain ID, enhancing quality of service for specified VLANs.

B. It isolates traffic within a specific VLAN by assigning a broadcast domain to an interface based on the VLAN ID.

C. It restricts the interface to managing traffic only from the specified VLAN, effectively segregating network traffic.

D. It assigns a unique domain ID to the interface, allowing it to operate across multiple VLANs within the same VDOM.

Answer: B

Explanation:

In a transparent mode Virtual Domain (VDOM) configuration, FortiGate operates as a Layer 2 bridge rather than performing Layer 3 routing. The set forward-domain < domain_ID > command is used to control how traffic is forwarded between interfaces within the same transparent VDOM.

A forward-domain acts as a broadcast domain, meaning only interfaces with the same forward-domain ID can exchange traffic. This setting is commonly used to separate different VLANs or network segments within the transparent VDOM while still allowing FortiGate to apply security policies.

NO.10 Which three approaches can successfully deploy advanced initial configurations?

A. Metadata variables

B. Model device ZTP/LTP

C. Jinja scripting

D. Global ADOM

Answer: A B C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract documents and Knowledge:
To deploy advanced initial configurations, FortiManager utilizes several specialized tools:
* Model device ZTP/LTP: FortiManager uses model devices to support Zero-Touch Provisioning (ZTP) and Low-Touch Provisioning (LTP). This allows configurations to be prepared on FortiManager and automatically pushed to a real device once it connects.
* Metadata variables: These are used within CLI templates and provisioning templates to provide dynamic, per-device configuration values (like specific IP addresses or unique identifiers).
* Jinja scripting: Both CLI and pre-run CLI templates support Jinja scripting, which provides a powerful way to use logic (if/then, loops) and variables to generate complex, dynamic configurations tailored to each device.

NO.11 Refer to the exhibit, which shows the packet capture output of a three-way handshake between FortiGate and FortiManager Cloud.
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: A D

NO.12 What is the effect of configuring tcp-mss-sender and tcp-mss-receiver?
A. Fragment only
B. Header change
C. Largest payload
D. Allow/Deny
Answer: C