FCSS_EFW_AD-7.6 Real Torrent & Premium FCSS_EFW_AD-7.6 Exam

P.S. Free & New FCSS_EFW_AD-7.6 dumps are available on Google Drive shared by TrainingDump: https://drive.google.com/open?id=1t6Sv9LK6GnK1A3szp9NYFPqxGx2xpOLI

Here in this Desktop practice test software, the FCSS - Enterprise Firewall 7.6 Administrator (FCSS_EFW_AD-7.6) practice questions given are very relevant to the actual Fortinet FCSS_EFW_AD-7.6 exam. It is compatible with Windows computers. TrainingDump provides its valued customers with customizable FCSS - Enterprise Firewall 7.6 Administrator (FCSS_EFW_AD-7.6) practice exam sessions. The Fortinet FCSS_EFW_AD-7.6 practice test software also keeps track of the previous Fortinet FCSS_EFW_AD-7.6 practice exam attempts.

Fortinet FCSS_EFW_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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	• 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 3	• 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 4	• 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.

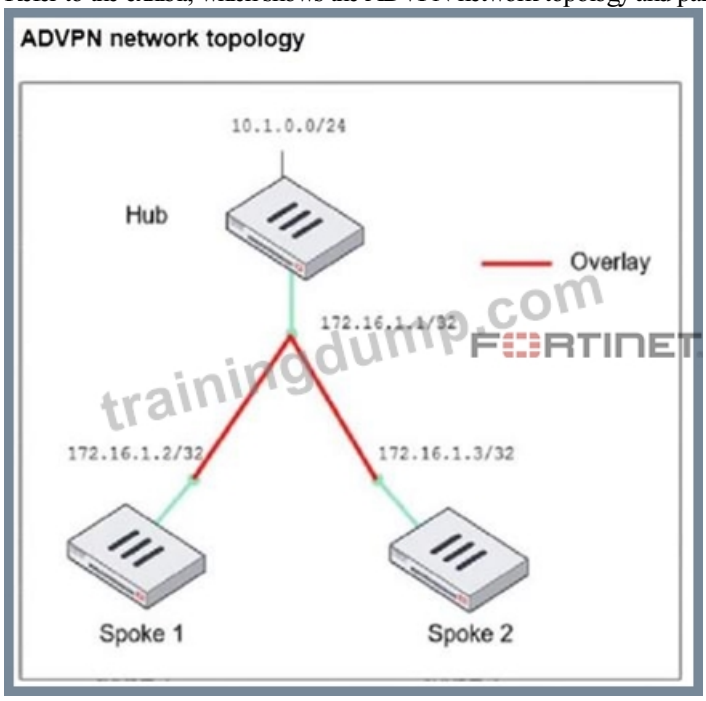
Topic 5	• Security Profiles: This section of the exam measures the skills of a Threat Prevention Specialist and covers the configuration and management of comprehensive security profiling systems. It includes implementing SSL • SSH inspection, combining web filtering and application control mechanisms, integrating intrusion prevention systems, and utilizing the Internet Service Database to create layered security protections for organizational networks.

100% Pass Quiz FCSS_EFW_AD-7.6 - FCSS - Enterprise Firewall 7.6 Administrator Updated Real Torrent

The Certified Production and FCSS_EFW_AD-7.6 certification is a valuable credential earned by individuals to validate their skills and competence to perform certain job tasks. Your FCSS - Enterprise Firewall 7.6 Administrator FCSS_EFW_AD-7.6 Certification is usually displayed as proof that you've been trained, educated, and prepared to meet the specific requirement for your professional role.

Fortinet FCSS - Enterprise Firewall 7.6 Administrator Sample Questions (Q41-Q46):

NEW QUESTION # 41
Refer to the exhibit, which shows the ADVPN network topology and partial BGP configuration.



Partial BGP configuration

```
Hub # config router bgp
set as 65100
set router-id 172.16.1.1
config neighbor-group
    edit "advpn"
    set remote-as 65100
    ...
    end
config neighbor-range
    edit 1
    end
config network
    ..
end
```

Which two parameters must an administrator configure in the config neighbor range for spokes shown in the exhibit? (Choose two.)

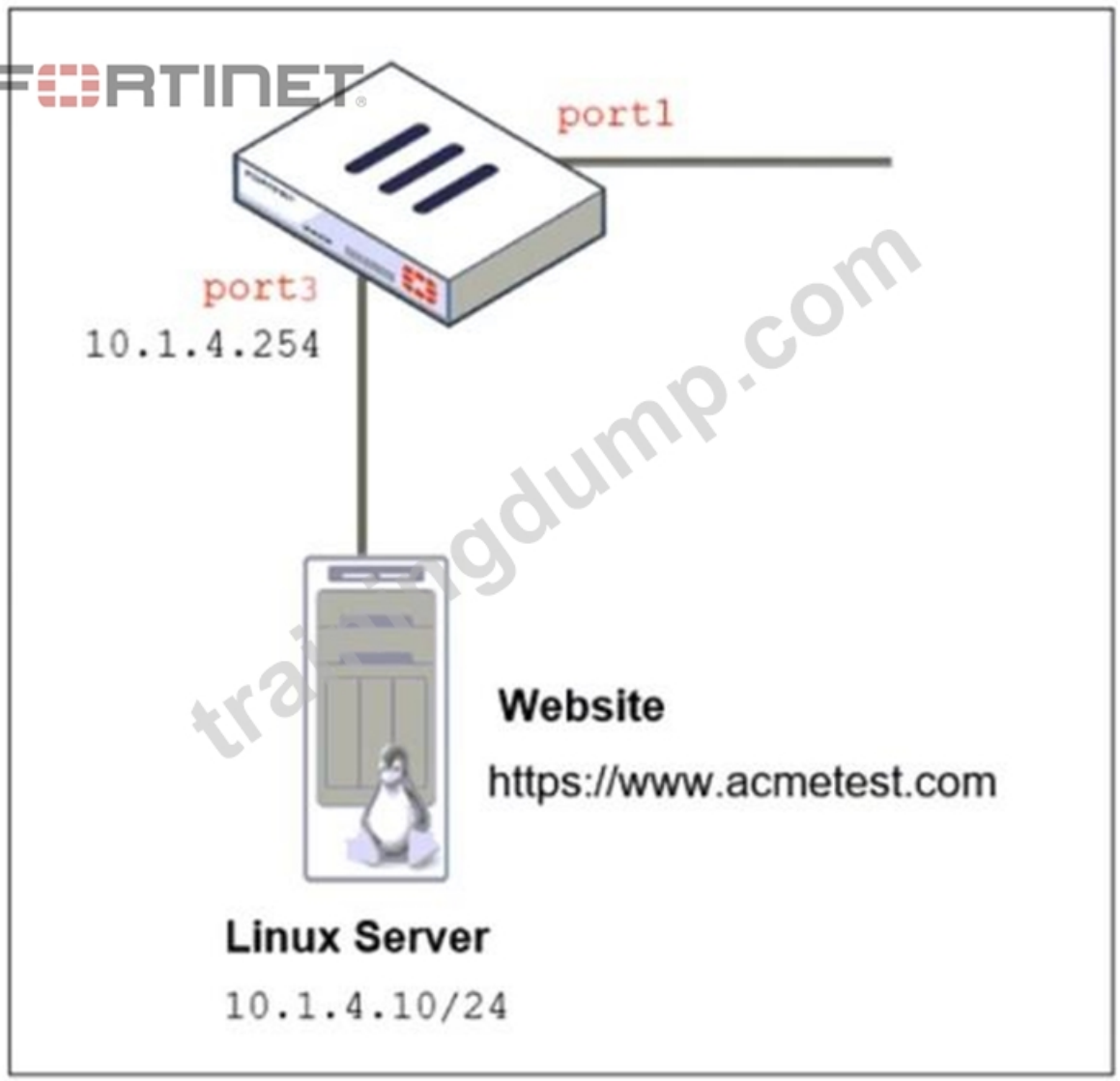
- A. set max-neighbor-num 2
- B. set prefix 172.16.1.0 255.255.255.0
- C. set neighbor-group advpn
- D. set route-reflector-client enable

Answer: B,C

Explanation:
In the given ADVPN (Auto-Discovery VPN) topology, BGP is being used to dynamically establish routes between spokes. The neighbor-range configuration is crucial for simplifying BGP peer setup by automatically assigning neighbors based on their IP range.
set neighbor-group advpn
The neighbor-group parameter is used to apply pre-defined settings (such as AS number) to dynamically discovered BGP neighbors.
The advpn neighbor-group is already defined in the configuration, and assigning it to the neighbor-range ensures consistent BGP settings for all spoke neighbors.
set prefix 172.16.1.0 255.255.255.0
This command allows dynamic BGP peer discovery by defining a range of potential neighbor IPs (172.16.1.1 - 172.16.1.255).
Since each spoke has a unique /32 IP within this subnet, this ensures that any spoke within the 172.16.1.0
/24 range can automatically establish a BGP session with the hub.

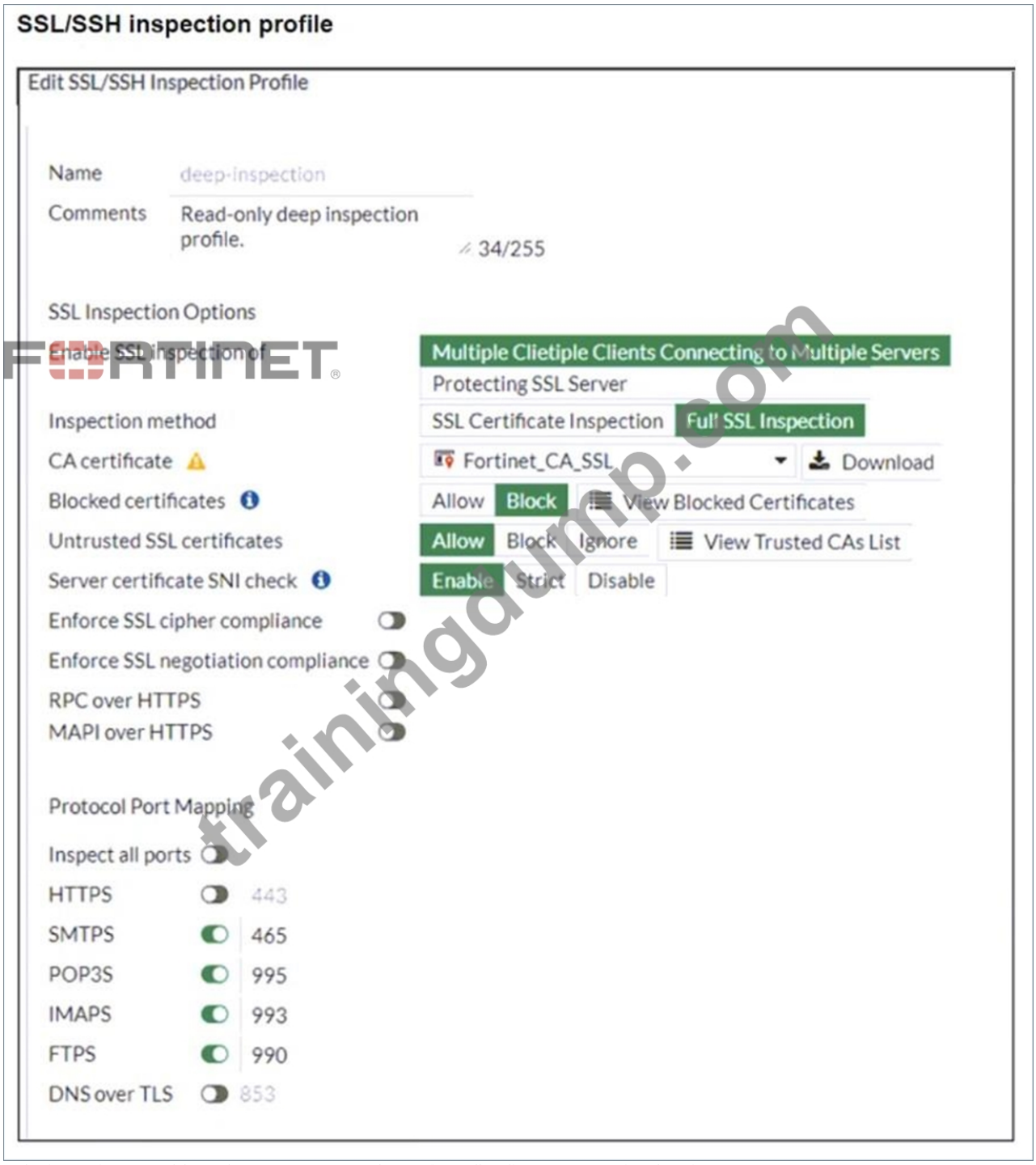
NEW QUESTION # 42
Refer to the exhibits. The exhibits show a network topology, a firewall policy, and an SSL/SSH inspection profile configuration.

Network Topology



Firewall policy on FortiGate

```
DCFW # sh firewall policy 3
config firewall policy
edit 3
set name "To Linux Servers"
set uuid bf77d59e-5513-51ef-147d-e35066c267e9
set srcintf "port1"
set dstintf "port3"
set action accept
set srcaddr "all"
set dstaddr "10.1.4.10"
set schedule "always"
set service "ALL"
set utm-status enable
set inspection-mode proxy
set ssl-ssh-profile "deep-inspection"
set ips-sensor "IPS Monitor"
set logtraffic all
next
end
```



Why is FortiGate unable to detect HTTPS attacks on firewall policy ID 3 targeting the Linux server?

- A. The administrator must set the policy to inspection mode to analyze the HTTPS packets as expected.
- B. The administrator must enable SSL inspection of the SSL server and upload the certificate of the Linux server website to the SSL/SSH inspection profile.
- C. The administrator must enable HTTPS in the protocol port mapping of the deep- inspection SSL/SSH inspection profile.
- D. The administrator must enable cipher suites in the SSL/SSH inspection profile to decrypt the message.

Answer: B

Explanation:
The FortiGate SSL/SSH inspection profile is configured for Full SSL Inspection, which is necessary to analyze encrypted HTTPS traffic. However, the firewall policy is protecting an SSL server (the Linux server hosting the website), and currently, the SSL/SSH profile only applies to client-side SSL inspection.
To detect HTTPS-based attacks targeting the Linux server:
FortiGate must act as an SSL intermediary to inspect encrypted traffic destined for the web server.
The administrator must upload the SSL certificate of the Linux web server to FortiGate so that the server-side SSL inspection can

decrypt incoming HTTPS traffic before analyzing it.

NEW QUESTION # 43
An administrator is setting up an ADVPN configuration and wants to ensure that peer IDs are not exposed during VPN establishment.
Which protocol can the administrator use to enhance security?

- A. Stick with IKEv1 main mode because it offers better performance.
- B. Use IKEv2, which encrypts peer IDs and prevents exposure.
- C. Opt for SSL VPN web mode because it does not use peer IDs at all.
- D. Choose IKEv1 aggressive mode because it simplifies peer identification.

Answer: B

Explanation:
In ADVPN (Auto-Discovery VPN) configurations, security concerns include protecting peer IDs during VPN establishment. Peer IDs are exchanged in the IKE (Internet Key Exchange) negotiation phase, and their exposure could lead to privacy risks or targeted attacks.
IKEv2 encrypts peer IDs, making it more secure compared to IKEv1, where peer IDs can be exposed in plaintext in aggressive mode.
IKEv2 also provides better performance and flexibility while supporting dynamic tunnel establishment in ADVPN.

NEW QUESTION # 44
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. Enable Scan Outgoing Connections to avoid clicking suspicious links or attachments that can deliver botnet malware and create false positives.
- B. Use an IPS profile with action monitor, however, the administrator must be aware that this can compromise network integrity.
- C. 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.
- D. Install missing or expired SSUTLS certificates on the client PC to prevent expected false positives.

Answer: C

Explanation:
False positives in Intrusion Prevention System (IPS) analysis can disrupt legitimate traffic and negatively impact user experience. To reduce false positives while maintaining security, administrators can:
Use IPS profile extensions to fine-tune the settings based on the organization's environment.
Select the correct operating system, protocol, and application types to ensure that IPS signatures match the network's actual traffic patterns, reducing false positives.
Customize signature selection based on the network's specific services, filtering out unnecessary or irrelevant signatures.

NEW QUESTION # 45
A company that acquired multiple branches across different countries needs to install new FortiGate devices on each of those branches. However, the IT staff lacks sufficient knowledge to implement the initial configuration on the FortiGate devices.
Which three approaches can the company take to successfully deploy advanced initial configurations on remote branches? (Choose three.)

- A. Use metadata variables to dynamically assign values according to each FortiGate device.
- B. Apply Jinja in the FortiManager scripts for large-scale and advanced deployments.
- C. Add FortiGate devices on FortiManager as model devices, and use ZTP or LTP to connect to FortiGate devices.
- D. Use the Global ADOM to deploy global object configurations to each FortiGate device.
- E. Use provisioning templates and install configuration settings at the device layer.

Answer: A,C,E

Explanation:
Use metadata variables to dynamically assign values according to each FortiGate device:
Metadata variables in FortiManager allow device-specific configurations to be dynamically assigned without manually configuring each FortiGate. This is especially useful when deploying multiple devices with similar base configurations.
Use provisioning templates and install configuration settings at the device layer:
Provisioning templates in FortiManager provide a structured way to configure FortiGate devices. These templates can define interfaces, policies, and settings, ensuring that each device is correctly configured upon deployment.
Add FortiGate devices on FortiManager as model devices, and use ZTP or LTP to connect to FortiGate devices:
Zero-Touch Provisioning (ZTP) and Local Touch Provisioning (LTP) help automate the deployment of FortiGate devices. By adding devices as model devices in FortiManager, configurations can be pushed automatically when devices connect for the first time, reducing manual effort.

NEW QUESTION # 46
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, study.stcs.edu.np, www.stes.tyc.edu.tw, ummalife.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

2026 Latest TrainingDump FCSS_EFW_AD-7.6 PDF Dumps and FCSS_EFW_AD-7.6 Exam Engine Free Share: https://drive.google.com/open?id=1t6Sv9LK6GnK1A3szp9NYFPqxGx2xpOLI