



Vendor: Fortinet

Exam Code: FCSS_EFW_AD-7.6

Exam Name: FCSS - Enterprise Firewall 7.6 Administrator

Version: DEMO

QUESTION 1

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

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.

QUESTION 2

Why does the ISDB block layers 3 and 4 of the OSI model when applying content filtering? (Choose two.)

- A. FortiGate has a predefined list of all IPs and ports for specific applications downloaded from FortiGuard.
- B. The ISDB blocks the IP addresses and ports of an application predefined by FortiGuard.
- C. The ISDB works in proxy mode, allowing the analysis of packets in layers 3 and 4 of the OSI model.
- D. The ISDB limits access by URL and domain.

Answer: AB

Explanation:

The Internet Service Database (ISDB) in FortiGate is used to enforce content filtering at Layer 3 (Network Layer) and Layer 4 (Transport Layer) of the OSI model by identifying applications based on their predefined IP addresses and ports.

FortiGate has a predefined list of all IPs and ports for specific applications downloaded from FortiGuard:

FortiGate retrieves and updates a predefined list of IPs and ports for different internet services from FortiGuard.

This allows FortiGate to block specific services at Layer 3 and Layer 4 without requiring deep packet inspection.

The ISDB blocks the IP addresses and ports of an application predefined by FortiGuard: ISDB works by matching traffic to known IP addresses and ports of categorized services. When an application or service is blocked, FortiGate prevents communication by denying traffic based on its destination IP and port number.

QUESTION 3

A user reports that their computer was infected with malware after accessing a secured HTTPS website. However, when the administrator checks the FortiGate logs, they do not see that the website was detected as insecure despite having an SSL certificate and correct profiles applied on the policy.

How can an administrator ensure that FortiGate can analyze encrypted HTTPS traffic on a website?

- A. The administrator must enable reputable websites to allow only SSL/TLS websites rated by FortiGuard web filter.
- B. The administrator must enable URL extraction from SNI on the SSL certificate inspection to ensure the TLS three-way handshake is correctly analyzed by FortiGate.
- C. The administrator must enable DNS over TLS to protect against fake Server Name Indication (SNI) that cannot be analyzed in common DNS requests on HTTPS websites.
- D. The administrator must enable full SSL inspection in the SSL/SSH Inspection Profile to decrypt packets and ensure they are analyzed as expected.

Answer: D

Explanation:

FortiGate, like other security appliances, cannot analyze encrypted HTTPS traffic unless it decrypts it first. If only certificate inspection is enabled, FortiGate can see the certificate details (such as the domain and issuer) but cannot inspect the actual web content.

To fully analyze the traffic and detect potential malware threats:

Full SSL inspection (Deep Packet Inspection) must be enabled in the SSL/SSH Inspection Profile. This allows FortiGate to decrypt the HTTPS traffic, inspect the content, and then re-encrypt it before forwarding it to the user.

Without full SSL inspection, threats embedded in encrypted traffic may go undetected.

QUESTION 4

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

Answer: ABE

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.

QUESTION 5

An administrator is checking an enterprise network and sees a suspicious packet with the MAC address e0:23:ff:fc:00:86.

What two conclusions can the administrator draw? (Choose two.)

- A. The suspicious packet is related to a cluster that has VDOMs enabled.
- B. The network includes FortiGate devices configured with the FGSP protocol.
- C. The suspicious packet is related to a cluster with a group-id value lower than 255.
- D. The suspicious packet corresponds to port 7 on a FortiGate device.

Answer: AC

Explanation:

The MAC address e0:23:ff:fc:00:86 follows the format used in FortiGate High Availability (HA) clusters. When FortiGate devices are in an HA configuration, they use virtual MAC addresses for failover and redundancy purposes.

The suspicious packet is related to a cluster that has VDOMs enabled:

FortiGate devices with Virtual Domains (VDOMs) enabled use specific MAC address ranges to differentiate HA-related traffic. This MAC address is likely part of that mechanism.

The suspicious packet is related to a cluster with a group-id value lower than 255:

FortiGate HA clusters assign virtual MAC addresses based on the group ID. The last octet (00:86) corresponds to a group ID that is below 255, confirming this option.

QUESTION 6

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

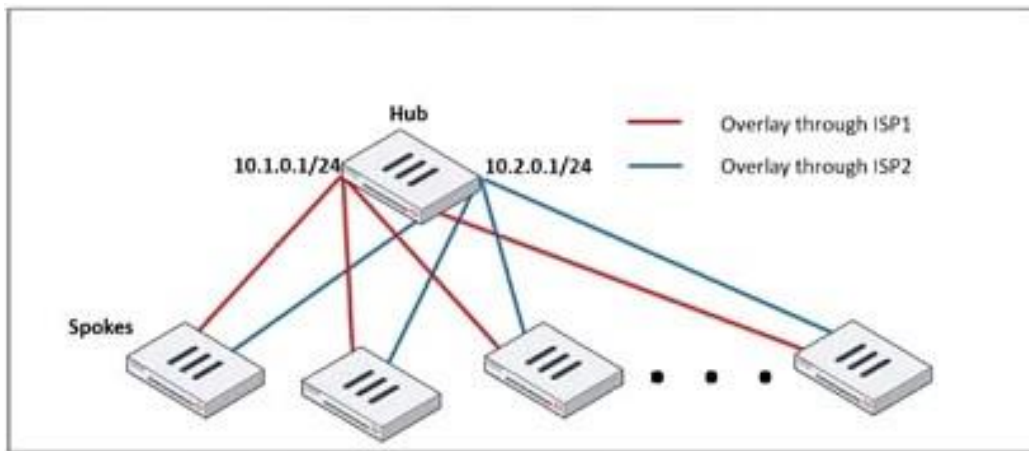
Explanation:

When FortiGate is operating in proxy mode with full SSL inspection enabled, it inspects encrypted HTTPS traffic by default on port 443. However, some websites may use non-standard HTTPS ports (such as 8443), which FortiGate does not inspect unless explicitly configured.

To ensure that FortiGate inspects HTTPS traffic on port 8443, administrators must manually add port 8443 in the Protocol Port Mapping section of the SSL/SSH Inspection Profile. This allows FortiGate to treat HTTPS traffic on port 8443 the same as traffic on port 443, enabling proper inspection and enforcement of FortiGuard category-based web filtering.

QUESTION 7

Refer to the exhibit, which shows a hub and spokes deployment.



An administrator is deploying several spokes, including the BGP configuration for the spokes to connect to the hub.

Which two commands allow the administrator to minimize the configuration? (Choose two.)

- A. neighbor-group
- B. route-reflector-client
- C. neighbor-range
- D. ibgp-enforce-multihop

Answer: AC

Explanation:

neighbor-group:

This command is used to group multiple BGP neighbors with the same configuration, reducing redundant configuration.

Instead of defining individual BGP settings for each spoke, the administrator can create a neighbor-group and apply the same policies, reducing manual work.

neighbor-range:

This command allows the configuration of a range of neighbor IPs dynamically, reducing the need to manually define each spoke neighbor.

It automatically adds BGP neighbors that match a given prefix, simplifying deployment.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14

