



Vendor: Fortinet

Exam Code: NSE7_ZTA-7.2

Exam Name: Fortinet NSE 7 - Zero Trust Access 7.2

Version: DEMO

QUESTION 1

What are two functions of NGFW in a ZTA deployment? (Choose two.)

- A. Acts as segmentation gateway
- B. Endpoint vulnerability management
- C. Device discovery and profiling
- D. Packet Inspection

Answer: AC

Explanation:

NGFW stands for Next-Generation Firewall, which is a network security device that provides advanced features beyond the traditional firewall, such as application awareness, identity awareness, threat prevention, and integration with other security tools. ZTA stands for Zero Trust Architecture, which is a security model that requires strict verification of the identity and context of every request before granting access to network resources. ZTA assumes that no device or user can be trusted by default, even if they are connected to a corporate network or have been previously verified.

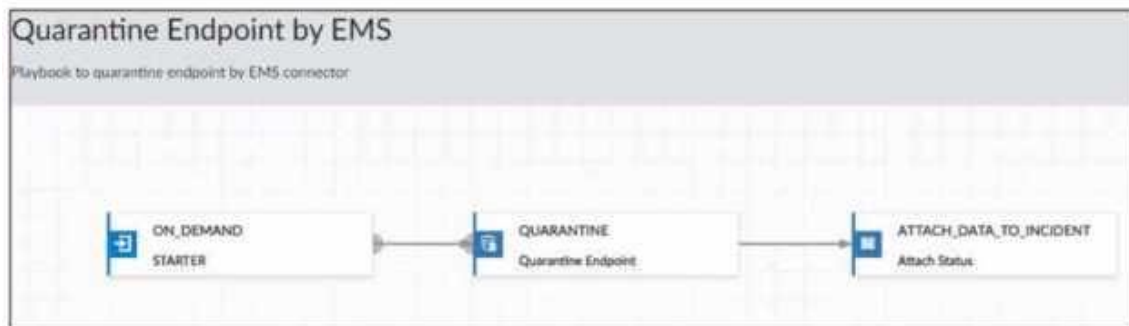
In a ZTA deployment, NGFW can perform two functions:

Acts as segmentation gateway: NGFW can act as a segmentation gateway, which is a device that separates different segments of the network based on security policies and rules. Segmentation can help isolate and protect sensitive data and applications from unauthorized or malicious access, as well as reduce the attack surface and contain the impact of a breach. NGFW can enforce granular segmentation policies based on the identity and context of the devices and users, as well as the applications and services they are accessing. NGFW can also integrate with other segmentation tools, such as software-defined networking (SDN) and microsegmentation, to provide a consistent and dynamic segmentation across the network.

Device discovery and profiling: NGFW can also perform device discovery and profiling, which are processes that identify and classify the devices that are connected to the network, as well as their attributes and behaviors. Device discovery and profiling can help NGFW to apply the appropriate security policies and rules based on the device type, role, location, health, and activity. Device discovery and profiling can also help NGFW to detect and respond to anomalous or malicious devices that may pose a threat to the network.

QUESTION 2

Exhibit.



Which statement is true about the FortiAnalyzer playbook configuration shown in the exhibit?

- A. The playbook is run on a configured schedule
- B. The playbook is run when an incident is created that matches the filters.
- C. The playbook is run when an event is created that matches the filters

D. The playbook is manually started by an administrator

Answer: D

Explanation:

The FortiAnalyzer playbook configuration shown in the exhibit indicates that:

D. The playbook is manually started by an administrator: The "ON DEMAND" trigger in the playbook suggests that it is initiated manually, as opposed to being automated or scheduled. This typically means that an administrator decides when to run the playbook based on specific needs or incidents.

QUESTION 3

What are the three core principles of ZTA? (Choose three.)

- A. Verity
- B. Be compliant
- C. Certify
- D. Minimal access
- E. Assume breach

Answer: ADE

Explanation:

Zero Trust Architecture (ZTA) is a security model that follows the philosophy of "never trust, always verify" and does not assume any implicit trust for any entity within or outside the network perimeter. ZTA is based on a set of core principles that guide its implementation and operation. According to the NIST SP 800-207, the three core principles of ZTA are:

A) Verify and authenticate. This principle emphasizes the importance of strong identification and authentication for all types of principals, including users, devices, and machines. ZTA requires continuous verification of identities and authentication status throughout a session, ideally on each request. It does not rely solely on traditional network location or controls. This includes implementing modern strong multi-factor authentication (MFA) and evaluating additional environmental and contextual signals during authentication processes.

D) Least privilege access. This principle involves granting principals the minimum level of access required to perform their tasks. By adopting the principle of least privilege access, organizations can enforce granular access controls, so that principals have access only to the resources necessary to fulfill their roles and responsibilities. This includes implementing just-in-time access provisioning, role-based access controls (RBAC), and regular access reviews to minimize the surface area and the risk of unauthorized access.

E) Assume breach. This principle assumes that the network is always compromised and that attackers can exploit any vulnerability or weakness. Therefore, ZTA adopts a proactive and defensive posture that aims to prevent, detect, and respond to threats in real-time. This includes implementing micro-segmentation, end-to-end encryption, and continuous monitoring and analytics to restrict unnecessary pathways, protect sensitive data, and identify anomalies and potential security events.

QUESTION 4

An administrator wants to prevent direct host-to-host communication at layer 2 and use only FortiGate to inspect all the VLAN traffic. What three things must the administrator configure on FortiGate to allow traffic between the hosts? (Choose three.)

- A. Configure proxy ARP to allow traffic
- B. Block intra-VLAN traffic in the VLAN interface settings
- C. Add the VLAN interface to a software switch

- D. Configure static routes to allow subnets
- E. Configure a firewall policy to allow the desired traffic between hosts

Answer: BDE

Explanation:

To prevent direct host-to-host communication at layer 2 and use only FortiGate to inspect all the VLAN traffic, an administrator must configure:

B) Block intra-VLAN traffic in the VLAN interface settings: This setting prevents direct communication between hosts within the same VLAN, forcing traffic to be routed through FortiGate for inspection.

D) Configure static routes to allow subnets: By setting up static routes, the administrator ensures that traffic between different subnets is correctly routed through the FortiGate for inspection and policy enforcement.

E) Configure a firewall policy to allow the desired traffic between hosts: Firewall policies on the FortiGate will dictate what traffic is permitted between hosts, ensuring that only authorized traffic is allowed.

The other options are not typically required for this setup:

A) Configure proxy ARP to allow traffic: Proxy ARP is not necessary for this scenario as it involves answering ARP requests on behalf of another host, which is not relevant to blocking intra-VLAN traffic.

C) Add the VLAN interface to a software switch: This would create a switch-like environment on the FortiGate, which is counterproductive to the goal of preventing direct host-to-host communication at layer 2.

QUESTION 5

Which statement is true about FortiClient EMS in a ZTNA deployment?

- A. Uses endpoint information to grant or deny access to the network
- B. Provides network and user identity authentication services
- C. Generates and installs client certificates on managed endpoints
- D. Acts as ZTNA access proxy for managed endpoints

Answer: A

Explanation:

In a ZTNA (Zero Trust Network Access) deployment, FortiClient EMS:

A) Uses endpoint information to grant or deny access to the network: FortiClient EMS plays a critical role in ZTNA by using information about the endpoint, such as its security posture and compliance status, to determine whether to grant or deny network access.

The other options do not accurately represent the role of FortiClient EMS in ZTNA:


B) Provides network and user identity authentication services: While it contributes to the overall ZTNA strategy, FortiClient EMS itself does not directly provide authentication services.

C) Generates and installs client certificates on managed endpoints: Certificate management is typically handled by other components in the ZTNA framework.

D) Acts as ZTNA access proxy for managed endpoints: FortiClient EMS does not function as an access proxy; its role is more aligned with endpoint management and policy enforcement.

QUESTION 6

Exhibit.

Status	Host Name ↕	Host Role ↕	Operating System ↕
w ⁺ 	hr	Corporate	Windows Server 2019 ...

Which two statements are true about the hr endpoint? (Choose two.)

- A. The endpoint application inventory could not be retrieved
- B. The endpoint is marked as a rogue device
- C. The endpoint has failed the compliance scan
- D. The endpoint will be moved to the remediation VLAN

Answer: BC

Explanation:

Based on the exhibit, the true statements about the hr endpoint are:

B) The endpoint is marked as a rogue device: The "w" symbol typically indicates a warning or an at-risk status, which can be associated with an endpoint being marked as rogue due to failing to meet the security compliance requirements or other reasons.

C) The endpoint has failed the compliance scan: The "w" symbol can also signify that the endpoint has failed a compliance scan, which is a common reason for an endpoint to be marked as at risk.

QUESTION 7

With the increase in IoT devices, which two challenges do enterprises face? (Choose two.)

- A. Bandwidth consumption due to added overhead of IoT
- B. Maintaining a high performance network
- C. Unpatched vulnerabilities in IoT devices
- D. Achieving full network visibility

Answer: CD

Explanation:

With the increase in IoT devices, enterprises face many challenges in securing and managing their network and data. Two of the most significant challenges are:

Unpatched vulnerabilities in IoT devices (Option C): IoT devices are often vulnerable to cyber attacks due to their increased exposure to the internet and their limited computing resources. Some of the security challenges in IoT include weak password protection, lack of regular patches and updates, insecure interfaces, insufficient data protection, and poor IoT device management. Unpatched vulnerabilities in IoT devices can allow hackers to exploit them and compromise the network or data. For example, the Mirai malware infected IoT devices by using default credentials and created a massive botnet that launched DDoS attacks on internet services.

Achieving full network visibility (Option D): IoT devices can generate a large amount of data that needs to be collected, processed, and analyzed. However, many enterprises lack the tools and capabilities to monitor and manage the IoT devices and data effectively. This can result in poor performance, inefficiency, and security risks. Achieving full network visibility means having a clear and comprehensive view of all the IoT devices, their status, their connectivity, their data flow, and their potential threats. This can help enterprises optimize their network performance, ensure data quality and integrity, and detect and prevent any anomalies or attacks.

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>



10% Discount Coupon Code: ASTR14