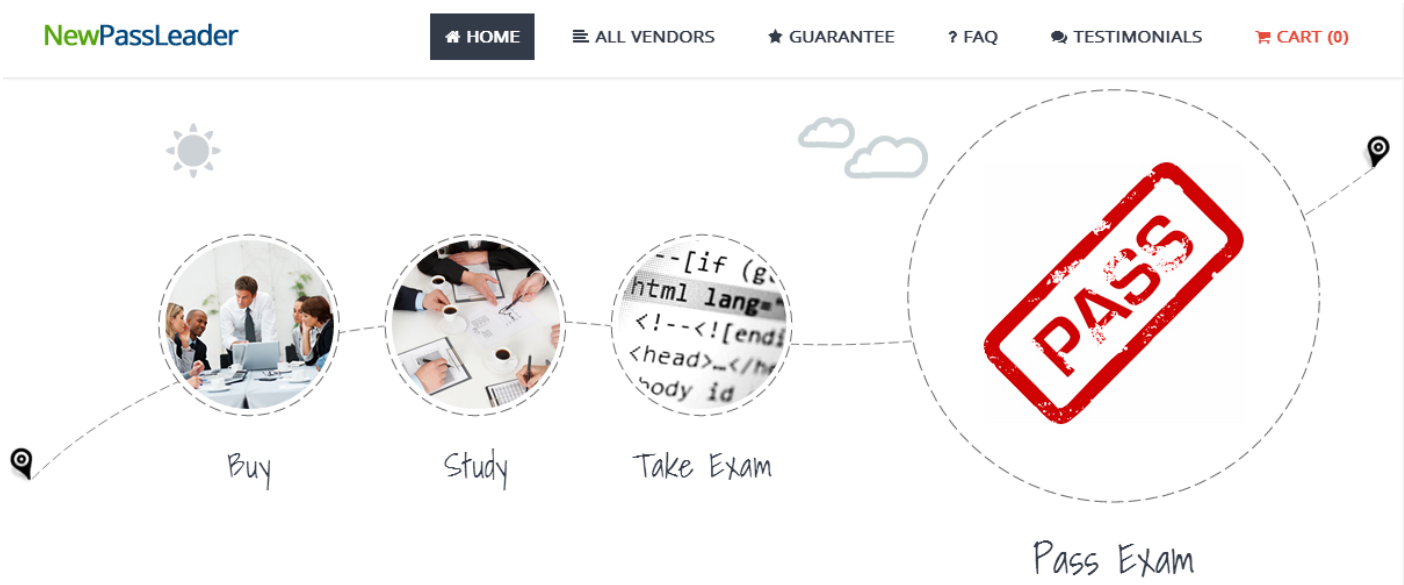
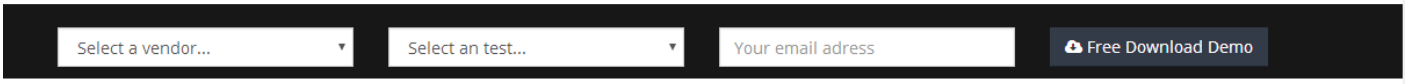
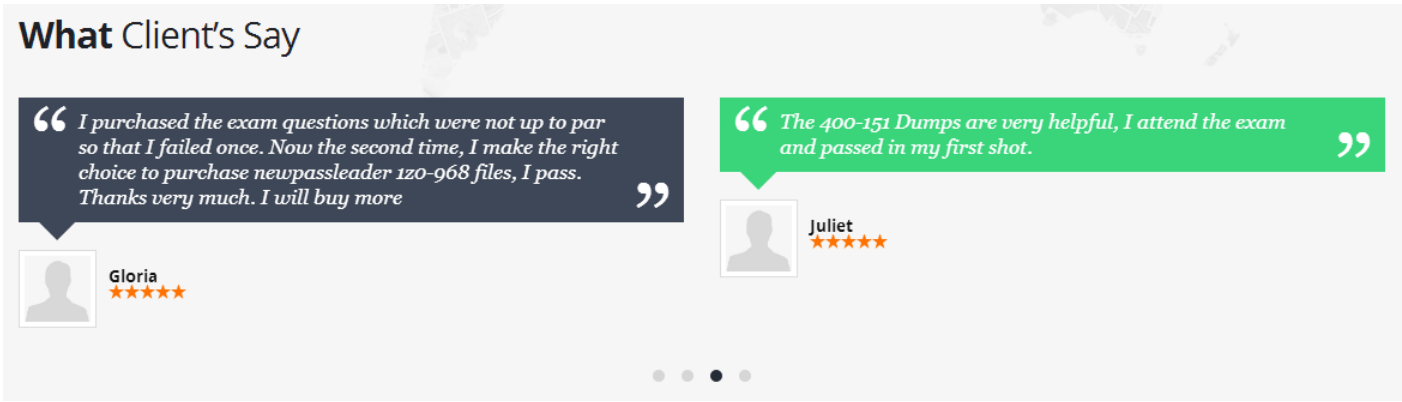
NewPassleader





Try **PDF Demo** before you buy

Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.
PDF format: Easy to read and print learning materials, our products are available in PDF file format.
Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.



http://www.newpassleader.com/

Attentive Service Exam Torrent and Valid Dumps - NewPassLeader

Exam : **NSE7_OTS-7.2**

Title : Fortinet NSE 7 - OT Security 7.2

Vendor : Fortinet

Version : DEMO

NO.1 An OT customer is using multiple FortiGate devices in their network to implement two-factor authentication with hardware FortiTokens. A supervisor is carrying multiple FortiTokens to be used when logging in to a critical server behind different FortiGate devices.
As an OT network architect, which approach must you take in order to assign one token per user and still use two-factor authentication on multiple FortiGate devices?

A. Implement a FortiManager and manage all FortiGate devices in the OT network to share the FortiTokens database.

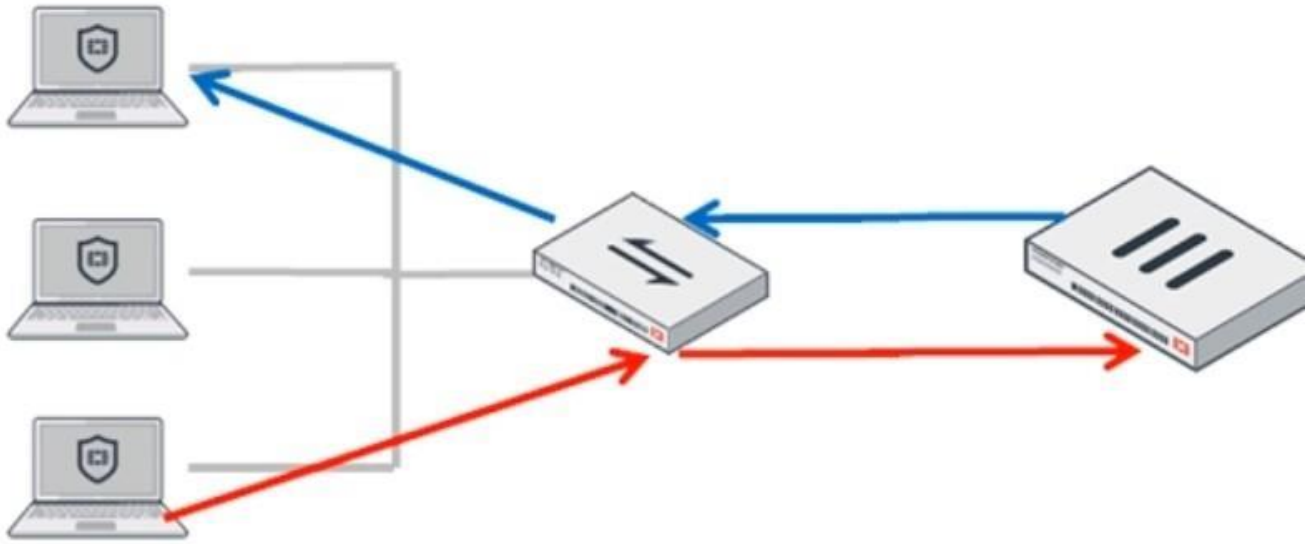
B. Implement FortiAuthenticator with FortiTokens provisioned for each user, and configure FortiAuthenticator as remote authentication server on all FortiGate devices in the OT network.

C. Provision the Edge-FortiGate device with all the FortiTokens and configure it as a remote authentication server on other FortiGate devices.

D. Configure FSSO-based two-factor authentication.

Answer: B

NO.2 Refer to the exhibit. In order for a FortiGate device to act as router on a stick, what configuration must an OT network architect implement on FortiGate to achieve inter-VLAN routing?



A. Set a unique forward domain on each interface on the network.

B. Set FortiGate to operate in transparent mode.

C. Set a software switch on FortiGate to handle inter-VLAN traffic.

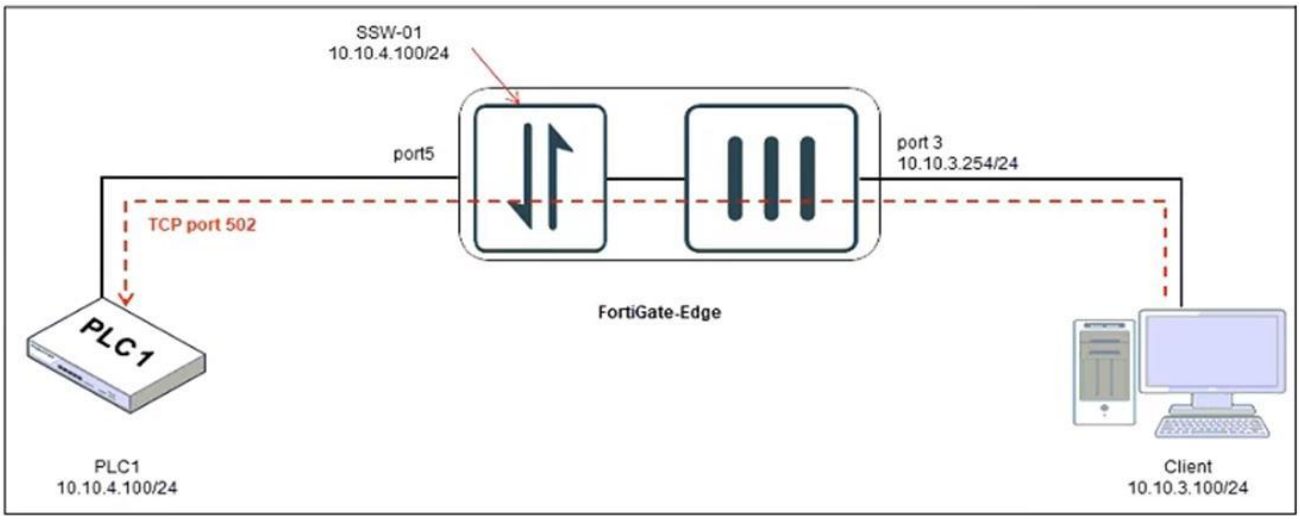
D. Set a FortiGate interface with the switch to operate as an 802.1 q trunk.

Answer: D

Explanation:
The router on a stick configuration requires a single physical interface on the FortiGate to carry traffic for multiple VLANs using 802.1q VLAN tagging.
The FortiGate interface connected to the switch must be configured as a trunk port to handle tagged VLAN traffic.
Sub-interfaces on the FortiGate are then created for each VLAN to route traffic between VLANs.
This setup enables efficient inter-VLAN routing over a single physical link, as shown in the diagram where traffic from multiple VLANs converges on a switch and is carried over a trunk port.

NO.3 Refer to the exhibit. An operational technology (OT) architect has implemented Modbus TCP with a simulation Conpot server to identify and control Modbus traffic in their OT network. The FortiGate-Edge device is configured with a software switch interface, SSW-01.
Based on the topology shown in the exhibit, which two statements must be true for the simulation of traffic between client and server to be successful? (Choose two.)

Topology



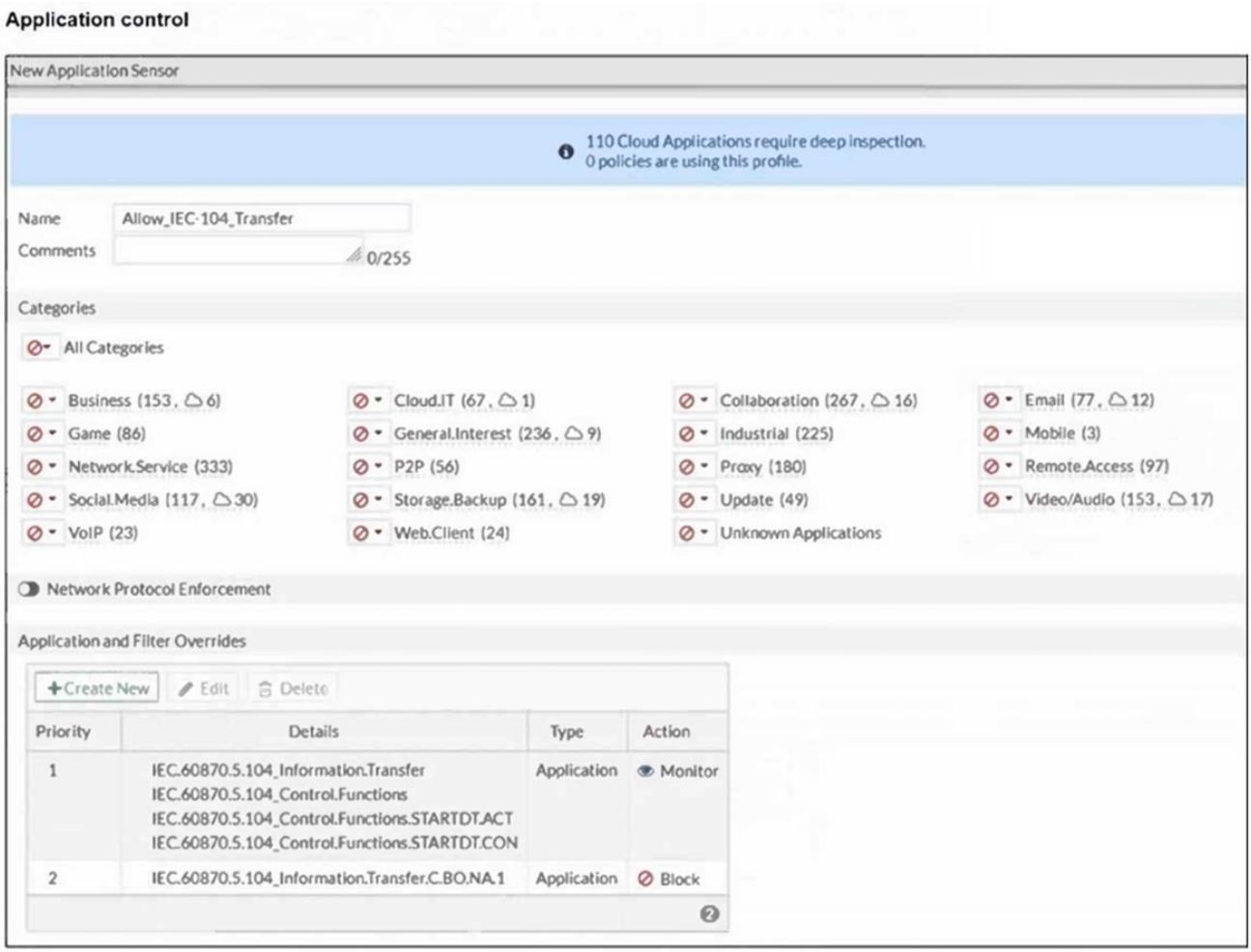
A. An IP address must be assigned to port5
B. In the FortiGate firewall policy, NAT must be enabled from port3 to SSW-01
C. The FortiGate device must be in offline intrusion detection system (IDS) mode
D. The FortiGate-Edge device must be in network address translation (NAT) operation mode
Answer: BD
Explanation:
In the FortiGate firewall policy, NAT must be enabled from port3 to SSW-01: To ensure successful communication between the client and the Conpot server through FortiGate, Network Address Translation (NAT) must be configured in the firewall policy. This allows the client to access the server via the FortiGate interface by properly routing the traffic.
The FortiGate-Edge device must be in network address translation (NAT) operation mode:
FortiGate in NAT operation mode ensures that traffic between different subnets (e.g., client and server) is routed correctly, enabling communication and simulation in the given topology.

NO.4 Which three Fortinet products can you use for device identification in an OT industrial control system (ICS)? (Choose three.)
A. FortiSIEM
B. FortiManager
C. FortiAnalyzer
D. FortiGate
E. FortiNAC
Answer: ADE
Explanation:
FortiNAC continuously collects identity records, profiles, and classifies devices in OT networks using a variety of methods including active and passive scanning.

FortiGate contributes by providing session and flow data that helps in device identification and classification.
FortiSIEM aggregates security and operational data from various sources including FortiGate and FortiNAC to provide comprehensive visibility and identification.

NO.5 What are two critical tasks the OT network auditors must perform during OT network risk assessment and management? (Choose two.)
A. Planning a threat hunting strategy
B. Implementing strategies to automatically bring PLCs offline
C. Creating disaster recovery plans to switch operations to a backup plant
D. Evaluating what can go wrong before it happens
Answer: AD
Explanation:
Planning a threat hunting strategy is essential for proactively searching for threats and vulnerabilities in the OT environment before they manifest into attacks.
Evaluating what can go wrong before it happens is a core part of risk assessment, involving the identification and analysis of potential risks and their impacts on OT systems.
Implementing strategies to automatically bring PLCs offline is generally not a responsible or safe approach in OT environments because it could disrupt critical industrial processes.
Creating disaster recovery plans is important for overall business continuity but is not primarily a task of auditors during risk assessment-it is more of a broader business continuity or incident response responsibility.

NO.6 Refer to the exhibit. An operational technology (OT) network security audit concluded that the application sensor does not block the IEC.60870.5.104_Information.Trasfer.C.BO.NA.1 signature.
Which change must the OT network administrator make?



A. Set all application categories to apply default actions.
B. Change the security action of the industrial category to monitor.
C. Update the priority of the C.BO.NA.1 signature override to 1.
D. Remove IEC.60870.5.104_Information.Transfer.C.BO.NA.1 from the first filter override.
Answer: C
Explanation:
The current configuration assigns priority 2 to the IEC.60870.5.104_Information.Transfer.C.BO.NA.1 application signature and sets it to Block. Priority 1 contains broader IEC.60870.5.104_Information.Transfer entries set to Monitor, which overrides the block action due to higher priority. To ensure that the C.BO.NA.1 signature is blocked, it must have higher priority than the general monitoring rule.

NO.7 What is the main difference between real-time logs and historical logs on FortiAnalyzer?
A. Historical logs are indexed in the SQL database, but real-time logs are not.
B. Real-time logs are indexed in the SQL database, but historical logs are not.
C. Historical logs are compressed and real-time logs are indexed in the SQL database.
D. Real-time logs are indexed while historical logs are compressed in the SQL database.
Answer: A

NO.8 As an OT administrator, it is important to understand how industrial protocols work in an OT network. Which communication method is used by the Modbus protocol?

A. It uses OSI Layer 2 and the primary device sends data based on request from secondary device.
B. It uses OSI Layer 2 and both the primary/secondary devices always send data during the communication.
C. It uses OSI Layer 2 and both the primary/secondary devices send data based on a matching token ring.
D. It uses OSI Layer 2 and the secondary device sends data based on request from primary device.
Answer: D
Explanation:
Modbus is master/slave: the master (primary) polls; a slave (secondary) replies only when requested. That fits "secondary sends data based on request from primary device."

NO.9 Which two statements are true when you deploy FortiGate as an offline IDS? (Choose two.)
A. FortiGate receives traffic from configured port mirroring.
B. Network traffic goes through FortiGate.
C. FortiGate acts as network sensor.
D. Network attacks can be detected and blocked.
Answer: AC
Explanation:
FortiGate receives traffic from configured port mirroring
In an offline IDS configuration, a FortiGate is typically set up to receive a copy of network traffic from specific ports or VLANs through port mirroring, allowing it to analyze the data without impacting the normal network flow.
FortiGate acts as a network sensor
Since it is passively monitoring the traffic, FortiGate can detect malicious activity based on its pre-defined intrusion detection signatures without blocking the traffic.