

# **Fortinet NSEI\_OTS\_AR-7.6**

## **Fortinet NSE I - OT Security 7.6 Architect**

**Thank You for Downloading NSEI\_OTS\_AR-7.6 Updated Exam Questions**

[https://certs4sale.com/fortinet/nsei\\_ots\\_ar-7.6-pdf-exam-dumps](https://certs4sale.com/fortinet/nsei_ots_ar-7.6-pdf-exam-dumps)

### Fortinet NSE I - OT Security 7.6 Architect

This practice guide contains technical evaluation questions for architects and engineers responsible for designing, securing, and operating Operational Technology (OT) and Critical Infrastructure networks adhering to the IEC 62443 standard using Fortinet Security Fabric solutions.

#### VENDOR

**Fortinet**

#### EXAM CODE

**NSEI\_OTS\_AR-7.6**

#### TARGET CERTIFICATION

**NSE Industry  
Certification: OT Security**

#### Core Architecture Domains Assessed

- OT Device Detection & Fingerprinting (Modbus TCP, Profinet) via FortiNAC
- Purdue Model Zone Segmentation & Ultra-Low Latency Policies on FortiGate
- Hybrid Contractor Authentication & PKI Integration via SSL VPN
- Virtual Patching & Custom IPS Signatures for Legacy PLCs
- FortiAnalyzer Risk Assessments & IEC 62443 Compliance Enforcement

# Fortinet NSEI\_OTS\_AR-7.6

## PRACTICE ASSESSMENT

---

### Question 1

SINGLE CHOICE

Your organization operates a manufacturing facility with legacy SCADA systems running Modbus TCP and Profinet protocols. You need to deploy device detection capabilities to identify and monitor these industrial devices on your FortiGate firewall. Which combination of Fortinet solutions would provide comprehensive device detection for OT environments while maintaining compliance with IEC 62443 standards?

**A. FortiGate device detection with FortiNAC integration to profile industrial devices and enforce segmentation policies based on device type**

B. FortiAnalyzer alone configured with raw syslog collection from network switches to manually categorize OT devices

C. FortiClient endpoint agents deployed on all SCADA workstations with centralized reporting to FortiManager

D. FortiDDoS protection configured to isolate Modbus and Profinet traffic from standard IT networks

**Answer: A**

#### Explanation:

The correct answer is FortiGate device detection with FortiNAC integration. FortiNAC provides device fingerprinting and profiling capabilities specifically designed for OT environments, allowing identification of industrial protocol devices like Modbus and Profinet controllers. It integrates with FortiGate to enforce network segmentation and access policies, directly supporting IEC 62443 compliance frameworks. FortiAnalyzer is primarily a logging and reporting tool and cannot perform active device detection. FortiClient is an endpoint solution not suited for non-traditional OT devices like PLCs and controllers. FortiDDoS is a DDoS mitigation tool unrelated to device detection or compliance requirements.

### Question 2

SINGLE CHOICE

You are designing network segmentation for a critical infrastructure facility using a combination of Ethernet VLANs and industrial switches. The facility has safety-critical zones, operational zones, and administrative zones. When configuring network segmentation schemas in FortiGate, what is the primary consideration for isolating these zones while maintaining OT operational requirements?

**A. Implement zone-based policies with strict deny-by-default rules, ensuring only explicitly allowed industrial protocols between zones, while maintaining ultra-low latency requirements for time-sensitive communications**

B. Create a flat network topology across all three zones to ensure optimal protocol performance and eliminate any latency-induced device failures

C. Segment zones only at Layer 2 using VLAN tagging, avoiding any Layer 3 firewall rules that might introduce packet inspection delays

D. Deploy separate FortiGate instances for each zone with no inter-zone communication to guarantee complete isolation

# Fortinet NSEI\_OTS\_AR-7.6

## PRACTICE ASSESSMENT

---

**Answer: A**

### Explanation (Question 2):

The correct answer acknowledges that zone-based policies with explicit allow rules and denial defaults are essential for OT security while recognizing the critical operational constraint of ultra-low latency. FortiGate supports this through granular policy definitions for industrial protocols. A flat network topology introduces unacceptable security risks in critical infrastructure. Layer 2-only segmentation without Layer 3 inspection fails to enforce meaningful access controls and violates defense-in-depth principles. Complete isolation with separate devices would break operational functionality.

### Question 3

**SINGLE CHOICE**

Your organization is implementing network access authentication for contractor access to your OT network. You want to use certificate-based authentication for technical staff and password-based authentication for occasional visitors. Which FortiGate authentication method would best support this hybrid approach while integrating with your existing Public Key Infrastructure (PKI)?

A. FortiToken hardware token combined with RADIUS server backend supporting both certificate and LDAP lookups

**B. Client certificate authentication via FortiGate SSL VPN with fallback to Active Directory password authentication for non-certificate users**

C. Kerberos authentication exclusively, as it is the only method supporting hybrid credential types in OT environments

D. TACACS+ protocol with manual certificate import for each user account

**Answer: B**

### Explanation:

The correct answer is FortiGate SSL VPN with client certificate authentication and Active Directory fallback. This approach provides certificate-based authentication for technical staff (leveraging PKI) while allowing password-based authentication for others, all through a single FortiGate infrastructure. FortiToken is primarily for multi-factor authentication, not hybrid authentication methods. Kerberos does not natively support certificate authentication, and TACACS+ does not provide the flexible certificate/password hybrid method required.

# Fortinet NSEI\_OTS\_AR-7.6

## PRACTICE ASSESSMENT

---

### Question 4

SINGLE CHOICE

You are configuring security inspections on your FortiGate for industrial protocols including Modbus TCP, DNP3, and Profinet. A critical requirement is to apply virtual patching rules to prevent known exploits targeting PLCs without requiring immediate firmware updates. What approach would best meet this requirement while maintaining protocol functionality?

**A. Create custom IPS signatures for known PLC vulnerabilities and apply them in a monitoring-only mode initially, then transition to block mode after validation to ensure operational continuity**

B. Block all Modbus, DNP3, and Profinet traffic entirely until all devices receive vendor-supplied firmware patches

C. Deploy FortiSandbox analysis to detonate all industrial protocol packets for real-time threat detection

D. Enable Deep Packet Inspection on all industrial traffic and rely solely on signature-based detection with no customization

**Answer: A**

#### Explanation:

The correct answer describes the proper virtual patching approach: creating custom IPS signatures for known vulnerabilities and using monitoring mode before blocking. This allows security protection against specific exploits while preserving device functionality during validation. Completely blocking industrial protocols is operationally infeasible. FortiSandbox is designed for malware detection, not industrial protocol exploitation patterns. Standard DPI with no customization cannot detect industry-specific zero-days or known vulnerabilities specific to your environment's PLCs.

# Fortinet NSEI\_OTS\_AR-7.6

## PRACTICE ASSESSMENT

---

### Question 5

SINGLE CHOICE

Your facility has experienced a targeted attack on its water treatment OT network. You are tasked with performing a comprehensive risk assessment using FortiAnalyzer security reports to identify vulnerabilities, threat exposure, and compliance gaps. After collecting data, you discover that 15% of devices are running unsupported firmware versions and 30% lack proper network segmentation. What should be your primary recommendation based on this risk assessment?

**A. Prioritize firmware updates for the 15% of devices and immediately implement network segmentation controls for the 30% gap, then conduct a follow-up assessment to validate risk reduction**

B. Accept the current risk level as acceptable since the facility is still operational without known breaches

C. Request that all devices be replaced with newer models to eliminate technical debt

D. Focus exclusively on the network segmentation issue and defer firmware updates until the next maintenance window in 12 months

**Answer: A**

#### Explanation:

The correct answer prioritizes both firmware patching and segmentation implementation with follow-up validation, reflecting a risk management approach appropriate for critical OT infrastructure. Unsupported firmware and lack of segmentation are both significant risk factors in critical environments. Accepting current risk without mitigation is inappropriate for water treatment facilities subject to regulatory standards. Device replacement is not practical or cost-effective. Deferring firmware updates leaves exploitable vulnerabilities exposed for an unacceptable duration.

# Fortinet NSEI\_OTS\_AR-7.6

## ARCHITECTURE DOMAIN SUMMARY

---

### Fortinet OT Security Architectural Principles

| Purdue Level / Component            | Fortinet Security Solution   | Security Function & Compliance                                                    |
|-------------------------------------|------------------------------|-----------------------------------------------------------------------------------|
| Level 0–2 (Field Devices / Control) | FortiNAC & Rugged FortiGate  | Active device profiling and protocol-aware virtual patching for legacy PLCs.      |
| Level 3 (Operations Management)     | FortiGate & Custom IPS       | Ultra-low latency zone-based firewalling for Modbus, DNP3, and Profinet.          |
| DMZ / Remote Access                 | FortiGate SSL VPN & PKI      | Hybrid certificate/password contractor authentication and secure access controls. |
| Centralized Management              | FortiAnalyzer & FortiManager | IEC 62443 risk auditing, threat reporting, and central configuration control.     |

#### Practice Assessment Completed

You have reviewed all standard sample items for the Fortinet NSE I - OT Security 7.6 Architect examination module.



# THANK YOU FOR DOWNLOADING NSEI\_OTS\_AR-7.6 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our NSEI\_OTS\_AR-7.6 Exam Product

Visit Our Site to Purchase the Full Set of Actual NSEI\_OTS\_AR-7.6 Exam Questions With Answers.

## Money Back Guarantee



**Click The Link Below**

[https://certs4sale.com/fortinet/nsei\\_ots\\_ar-7.6-pdf-exam-dumps](https://certs4sale.com/fortinet/nsei_ots_ar-7.6-pdf-exam-dumps)