



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.



NSE7_OTS-7.2 Dumps
NSE7_OTS-7.2 Braindumps
NSE7_OTS-7.2 Real Questions
NSE7_OTS-7.2 Practice Test
NSE7_OTS-7.2 Actual Questions



killexams.com

Fortinet

NSE7_OTS-7.2

Trustworthy for Fortinet Certified Solution Specialist (FCSS)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/NSE7_OTS-7.2



Question: 255

An OT administrator is troubleshooting device detection in a Security Fabric with FortiGate and FortiNAC. A new PLC using IEC 61850 is not detected. Which steps resolve this?

- A. Configure FortiGate to log IEC 61850 traffic with set application-list iec61850; set logtraffic all
- B. Enable FortiNAC's passive discovery for IEC 61850 with set protocol iec61850 enable
- C. Update FortiNAC's protocol database to include IEC 61850 signatures
- D. Use FortiGate CLI to enable IEC 61850 detection with set iec61850-detection enable
- E. Integrate FortiSIEM to forward IEC 61850 logs to FortiNAC

Answer: A,C

Explanation: Logging IEC 61850 traffic on FortiGate (set application-list iec61850; set logtraffic all) ensures detection data is available. Updating FortiNAC's protocol database with IEC 61850 signatures enables accurate detection.

Question: 256

An Operational Technology network uses FortiAnalyzer to log all traffic from a specific VLAN (100). Which filter ensures only VLAN 100 traffic is logged?

- A. logid=10 AND vlan=100
- B. logid=1 AND vlan_id=100
- C. logid=10 AND vlan_id=100
- D. logid=1 AND vlan=100

Answer: A

Explanation: The correct FortiAnalyzer filter is logid=10 AND vlan=100, as logid=10 targets traffic logs and vlan is the field for VLAN ID) Other options use incorrect fields (vlan_id) or incorrect logid values (logid=1).

Question: 257

In an OT environment, a FortiGate is deployed to protect a SCADA network using the IEC 61850 protocol. The administrator needs to identify and log all MMS (Manufacturing Message Specification)

traffic for compliance auditing. Which two FortiGate features should be configured to achieve this?

- A. Application control profile with IEC 61850 MMS signatures enabled
- B. Deep packet inspection (DPI) with a custom MMS filter
- C. Firewall policy with protocol inspection for IEC 61850
- D. IPS sensor with MMS-specific signatures enabled
- E. Traffic logging with a filter for MMS protocol

Answer: A, E

Explanation: To identify and log MMS traffic in an IEC 61850 SCADA network, the administrator should enable an application control profile with MMS signatures (part of IEC 61850) to identify the traffic and configure traffic logging with a filter for the MMS protocol to capture logs for auditing.

Question: 258

An Operational Technology network uses FortiSIEM to monitor IEC 61850 traffic for anomalies. Which query detects devices sending GOOSE messages with invalid sequence numbers?

- A. `SELECT source, seq_num FROM $log WHERE type="GOOSE" AND seq_num IS INVALID`
- B. `SELECT src_ip, goose_seq FROM $log WHERE protocol="IEC61850" AND goose_seq NOT IN (SELECT valid_seq FROM goose_table)`
- C. `SELECT src_ip, sequence FROM $log WHERE protocol="IEC61850" AND sequence != VALID`
- D. `SELECT device, goose_seq FROM $log WHERE proto="GOOSE" AND goose_seq NOT VALID`

Answer: B

Explanation: The correct FortiSIEM query is `SELECT src_ip, goose_seq FROM $log WHERE protocol="IEC61850" AND goose_seq NOT IN (SELECT valid_seq FROM goose_table)`. It targets IEC 61850 GOOSE messages and checks for invalid sequence numbers by comparing against a valid sequence table. Other options use incorrect fields (type, proto, sequence, seq_num) or invalid syntax (IS INVALID, NOT VALID).

Question: 259

An Operational Technology network uses FortiAnalyzer to monitor S7comm traffic. You need to configure a filter to log only S7comm write requests. Which filter syntax is correct?

- A. `set filter "protocol=s7comm action=write"`
- B. `set filter "app=s7comm write"`

- C. set filter "s7comm.write"
- D. set filter "app=s7comm-write"

Answer: B

Explanation: To log S7comm write requests, the filter must specify the S7comm application and write action. "set filter "app=s7comm write"" is correct. "protocol=s7comm action=write" uses incorrect syntax. "s7comm.write" is invalid. "app=s7comm-write" assumes a hyphenated name, so it's incorrect.

Question: 260

An Operational Technology network uses a FortiSwitch ring topology with MRP for redundancy. A link failure causes a 300ms recovery delay. Which configuration achieves a 100ms recovery time?

- A. Enable RSTP as a fallback protocol
- B. Set the MRP recovery time to 100ms
- C. Configure a static LAG for redundancy
- D. Increase the MRP ring check interval to 50ms
- E. Set the MRP priority to 8192

Answer: B

Explanation: Setting the MRP recovery time to 100ms configures the protocol to recover within the desired timeframe, as MRP supports ultra-fast recovery in ring topologies. RSTP is not compatible with MRP. A static LAG doesn't support ring topologies. Increasing the ring check interval slows recovery. MRP priority affects role assignment, not recovery time.

Question: 261

An Operational Technology network uses FortiNAC to enforce network access control. A new device using PROFINET (EtherType 0x8892) fails to connect to the production VLAN. The FortiNAC log shows a profiling failure. Which steps should you take to resolve this issue?

- A. Add a custom profiling rule in FortiNAC for EtherType 0x8892
- B. Configure the Industrial Ethernet switch to send LLDP packets to FortiNAC
- C. Verify the FortiGate firewall allows PROFINET traffic to the VLAN
- D. Enable SNMP traps on the switch to update FortiNAC's device inventory
- E. Manually assign the device to the production VLAN in FortiNAC

Answer: A,B,C

Explanation: Adding a custom profiling rule for EtherType 0x8892 allows FortiNAC to recognize PROFINET devices. Configuring the switch to send LLDP packets provides additional device information for profiling. Verifying the FortiGate allows PROFINET traffic ensures connectivity to the VLAN. SNMP traps help with inventory but are less specific to PROFINET profiling. Manually assigning the VLAN bypasses profiling and is not scalable.

Question: 262

An OT administrator is configuring FortiGate to detect a new PLC using DNP3 protocol in a Security Fabric environment. Which command enables FortiGate to identify and log DNP3 traffic for device detection?

- A. config firewall service custom; set protocol DNP3; set logtraffic all; end
- B. config system settings; set dnp3-detection enable; end
- C. config firewall policy; set application-list DNP3; set logtraffic all; end
- D. config system interface; set dnp3 enable; set logtraffic enable; end

Answer: C

Explanation: To detect and log DNP3 traffic, the administrator configures a firewall policy with an application control list for DNP3 and enables logging (config firewall policy; set application-list DNP3; set logtraffic all; end). This integrates with the Security Fabric for device detection.

Question: 263

An OT environment uses FortiGate to segment SCADA devices on VLAN 400 from IT devices on VLAN 500. The administrator needs to allow specific OPC UA traffic (port 4840) from a SCADA server (172.16.1.10) to a client in VLAN 500 (172.16.2.20). Which firewall policy is correct?

- A. config firewall policy edit 1 set srcintf "vlan400" set dstintf "any" set srcaddr "all" set dstaddr "all" set service "OPCUA" set action accept next end
- B. config firewall policy edit 1 set srcintf "vlan400" set dstintf "vlan400" set srcaddr "172.16.1.10" set dstaddr "172.16.2.20" set service "OPCUA" set action accept next end
- C. config firewall policy edit 1 set srcintf "vlan500" set dstintf "vlan400" set srcaddr "172.16.2.20" set dstaddr "172.16.1.10" set service "OPCUA" set action accept next end
- D. config firewall policy edit 1 set srcintf "vlan400" set dstintf "vlan500" set srcaddr "172.16.1.10" set dstaddr "172.16.2.20" set service "OPCUA" set action accept next end

Answer: D

Explanation: To allow OPC UA traffic (port 4840) from the SCADA server (172.16.1.10) in VLAN 400 to a client (172.16.2.20) in VLAN 500, the firewall policy must specify the correct source and destination interfaces and addresses.

Question: 264

An Operational Technology network uses a FortiGate to secure a Profibus network. The administrator needs to implement an IPS policy to detect and block Profibus packets with unauthorized master-slave communication attempts. Which two CLI commands are required to enable this protection?

- A. `config ips sensor edit "Profibus_Protection" set action block next end`
- B. `config ips sensor edit "Profibus_Protection" config entries edit 1 set protocol PROFIBUS set signature "Profibus.Unauthorized_Master" set action block next end next end`
- C. `config firewall policy edit 1 set ips-sensor "Profibus_Protection" set service "PROFIBUS" set action deny next end`
- D. `config ips sensor edit "Profibus_Protection" config entries edit 1 set protocol TCP set signature "Profibus.Generic" set action block next end next end`
- E. `config firewall policy edit 1 set service "PROFIBUS" set action deny next end`

Answer: B, C

Explanation: To detect and block unauthorized Profibus master-slave communication attempts, the administrator must configure an IPS sensor with a specific signature and apply it to a firewall policy.

Question: 265

An Operational Technology network uses FortiGate with FortiNAC for device authentication. The administrator wants to ensure that only devices with valid digital certificates issued by the internal CA can access the control network. Which configuration on FortiGate is required to enforce this?

- A. Configure a firewall policy with deep packet inspection and certificate validation
- B. Set `set auth-cert` in the firewall policy configuration
- C. Enable certificate-based authentication in the FortiGate SSL-VPN settings
- D. Use `set ssl-ocsp enable` in the FortiGate global configuration

Answer: B

Explanation: To enforce certificate-based authentication on FortiGate, the administrator must configure a firewall policy with the certificate validation setting using the command `set auth-cert` (Set `set auth-cert` in the firewall policy configuration). This ensures only devices with valid certificates issued by the specified CA are allowed. Deep packet inspection does not specifically handle certificate authentication, SSL-VPN

settings are irrelevant for OT device access, and OCSP enables certificate revocation checking but does not enforce authentication.

Question: 266

To ensure OT availability, you configure a FortiGate high-availability (HA) cluster in an Industrial Ethernet network. The cluster uses VRRP for redundancy. Which command verifies that the secondary FortiGate is synchronizing correctly with the primary?

- A. `diagnose sys ha status`
- B. `get router info vrrp`
- C. `show system ha`
- D. `diagnose sys vrrp status`
- E. `get system ha status`

Answer: E

Explanation: The `get system ha status` command displays the HA synchronization status, including whether the secondary FortiGate is properly synchronized with the primary. `diagnose sys ha status` provides detailed HA diagnostics but is less straightforward. `show system ha` displays configuration, not real-time status. `diagnose sys vrrp status` and `get router info vrrp` relate to VRRP but don't confirm HA synchronization.

Question: 267

A FortiSIEM rule needs to detect OT devices with memory utilization above 90% for 10 minutes. Which condition is correct?

- A. `EventType = "System" AND memory > 90 INTERVAL 10m`
- B. `EventType = "Performance" AND mem_usage > 90 INTERVAL 600s`
- C. `EventType = "Performance" AND mem_load > 90 INTERVAL 600s`
- D. `EventType = "System" AND mem_usage > 90 INTERVAL 10m`

Answer: B

Explanation: The correct FortiSIEM rule condition is `EventType = "Performance" AND mem_usage > 90 INTERVAL 600s`, as `EventType = "Performance"` targets performance metrics, `mem_usage` is the standard field, and `INTERVAL 600s` specifies 10 minutes. Other options use incorrect fields (`memory`, `mem_load`) or event types (`System`).

Question: 268

An OT administrator needs to configure FortiSIEM to detect devices sending excessive ICMP packets. Which query identifies devices with over 1000 ICMP packets in 5 minutes?

- A. `SELECT source, SUM(packets) FROM $log WHERE type="ICMP" GROUP BY source HAVING SUM(packets) > 1000 INTERVAL 5m`
- B. `SELECT src_ip, COUNT(*) AS pkt_count FROM $log WHERE protocol="ICMP" GROUP BY src_ip HAVING pkt_count > 1000 INTERVAL 300s`
- C. `SELECT src_ip, COUNT(packets) FROM $log WHERE protocol="ICMP" GROUP BY src_ip HAVING COUNT(packets) > 1000 INTERVAL 300s`
- D. `SELECT device, SUM(pkt) FROM $log WHERE proto="ICMP" GROUP BY device HAVING SUM(pkt) > 1000 INTERVAL 5m`

Answer: B

Explanation: The correct FortiSIEM query is `SELECT src_ip, COUNT(*) AS pkt_count FROM $log WHERE protocol="ICMP" GROUP BY src_ip HAVING pkt_count > 1000 INTERVAL 300s`. It filters ICMP traffic, counts packets with `COUNT(*)`, groups by source IP, and uses a 300-second (5-minute) interval. Other options use incorrect fields (`type`, `proto`, `packets`, `pkt`) or aggregation methods.

Question: 269

An Operational Technology network uses FortiAnalyzer to monitor IEC 61850 traffic. You need to configure a filter to log only GOOSE messages. Which filter syntax is correct?

- A. `set filter "app=goose"`
- B. `set filter "protocol=iec61850 type=goose"`
- C. `set filter "iec61850.goose"`
- D. `set filter "app=iec61850.goose"`

Answer: D

Explanation: To log GOOSE messages, the filter must specify the IEC 61850 application and GOOSE type. `"set filter "app=iec61850.goose""` is correct. `"protocol=iec61850 type=goose"` uses incorrect syntax. `"iec61850.goose"` is invalid. `"app=goose"` does not specify IEC 61850, so it's incorrect.

Question: 270

In an OT environment, a FortiGate is used to secure a network with S7comm protocol traffic. The administrator needs to allow only specific S7comm function codes. Which CLI command is used to configure this?

- A. config system settings
- B. config firewall policy
- C. config application list
- D. config ips sensor

Answer: C

Explanation: The config application list command is used to create an application control profile to filter specific S7comm function codes. The config firewall policy command applies the profile but does not configure it. The config system settings command is unrelated. The config ips sensor command is for IPS, not application control.

Question: 271

In a FortiSIEM deployment, an OT administrator wants to prioritize alerts for devices with a criticality score above 7. Which configuration ensures this?

- A. Set Priority = Criticality * Severity in the FortiSIEM rule
- B. Configure an event handler with filter: Criticality > 7
- C. Adjust the FortiSIEM global policy to weight Criticality > 7
- D. Use a CMDB query to tag devices with Criticality > 7

Answer: B

Explanation: To prioritize alerts for devices with a criticality score above 7 in FortiSIEM, configure an event handler with the filter Criticality > 7 to directly target high-criticality devices. Setting Priority = Criticality * Severity modifies priority but does not ensure prioritization of alerts. Adjusting the global policy is too broad and not specific to criticality. A CMDB query for tagging is a prerequisite, not a prioritization mechanism.

Question: 272

In a FortiNAC deployment, an OT administrator wants to enforce 802.1X authentication for PLCs using

EAP-TLS. The FortiSwitch ports must dynamically assign VLAN 500 for authenticated devices and VLAN 600 for guest devices. Which configuration is correct?

- A. config switch-controller 802-1x-settings set guest-vlan 600 set auth-vlan 500 set auth-type eap-tls end
- B. config switch-controller port-security set port1 auth-mode 802.1x set guest-vlan 600 set auth-vlan 500 set eap-tls enable end
- C. config switch-controller security-policy 802-1x set guest-vlanid 600 set auth-vlanid 500 set security-mode eap-tls end
- D. config switch-controller vlan-policy set vlan 500 set guest-vlan 600 set auth-method eap-tls end

Answer: C

Explanation: To configure 802.1X authentication with EAP-TLS on FortiSwitch for PLCs, the correct command is under the switch-controller security-policy 802-1x context.

Question: 273

In an Operational Technology network, a FortiGate is used to secure a Modbus TCP network. The administrator needs to block packets with function code 23 (Read/Write Multiple Registers) from a specific VLAN (VLAN 100). Which configuration achieves this?

- A. config application control edit "Modbus_Restrict" set protocol MODBUS set function "Read_Write" set action block next end
- B. config firewall policy edit 1 set vlanid 100 set service "MODBUS" set action deny next end
- C. config ips sensor edit "Modbus_Restrict" config entries edit 1 set protocol TCP set signature "Modbus.Generic" set action block next end next end
- D. config ips sensor edit "Modbus_Restrict" config entries edit 1 set protocol MODBUS set signature "Modbus.Read_Write" set action block set vlan 100 next end next end
- E. config firewall policy edit 1 set vlanid 100 set service "TCP/502" set action deny next end

Answer: D

Explanation: To block Modbus function code 23 packets from VLAN 100, an IPS sensor with a specific signature and VLAN filter is required.

Question: 274

An Operational Technology network administrator configures FortiGate to segment a control network (VLAN 900) to allow only S7comm traffic (port 102) to a server at 192.168.90.10. Which CLI configuration is correct?

- A. config firewall policy edit 1 set srcintf "VLAN900" set dstintf "Server" set srcaddr "all" set dstaddr "192.168.90.10" set service "ALL" set action accept next end
- B. config firewall policy edit 1 set srcintf "VLAN900" set dstintf "Server" set srcaddr "192.168.90.0/24" set dstaddr "192.168.90.10" set service "S7comm" set action accept next end
- C. config firewall policy edit 1 set srcintf "VLAN900" set dstintf "Server" set srcaddr "192.168.90.0/24" set dstaddr "all" set service "S7comm" set action accept next end
- D. config firewall policy edit 1 set srcintf "VLAN900" set dstintf "Server" set srcaddr "all" set dstaddr "all" set service "ALL" set action accept next end

Answer: B

Explanation: To allow only S7comm traffic from VLAN 900 to the server at 192.168.90.10, the firewall policy must specify the source interface (VLAN900), destination interface (Server), source address (192.168.90.0/24), destination address (192.168.90.10), and service (S7comm) with an accept action (config firewall policy with specific source, destination, and S7comm service). Other options allow broader addresses or services, failing to meet the requirement.

Question: 275

In an OT environment, a FortiGate administrator is configuring internal segmentation to isolate ICS devices on VLAN 200 from corporate devices on VLAN 300. The goal is to prevent lateral movement while allowing specific Modbus TCP traffic (port 502) from a SCADA server (10.0.2.10) to ICS devices. Which firewall policy configuration is correct?

- A. config firewall policy edit 1 set srcintf "vlan200" set dstintf "vlan300" set srcaddr "10.0.2.10" set dstaddr "all" set service "MODBUS" set action accept next end
- B. config firewall policy edit 1 set srcintf "vlan300" set dstintf "vlan200" set srcaddr "all" set dstaddr "10.0.2.10" set service "MODBUS" set action accept next end
- C. config firewall policy edit 1 set srcintf "vlan200" set dstintf "vlan200" set srcaddr "10.0.2.10" set dstaddr "all" set service "MODBUS" set action accept next end
- D. config firewall policy edit 1 set srcintf "vlan200" set dstintf "any" set srcaddr "all" set dstaddr "all" set service "MODBUS" set action accept next end

Answer: C

Explanation: To allow specific Modbus TCP traffic (port 502) from the SCADA server (10.0.2.10) in VLAN 200 to ICS devices within the same VLAN while preventing lateral movement to VLAN 300, the firewall policy must be configured with srcintf and dstintf set to "vlan200" to restrict traffic within VLAN 200. The srcaddr should be "10.0.2.10" to specify the SCADA server, and the service should be "MODBUS" to allow port 502 traffic.

Question: 276

An Operational Technology network administrator needs to restrict SCADA server access to only categorized PLCs using FortiNAC) Which configuration achieves this?

- A. Configure FortiGate to enforce PLC access with set application-list plc-only
- B. Create a network access policy in FortiNAC to allow only PLC device profiles
- C. Set up FortiNAC to use VLAN segmentation for PLCs with set vlan plc
- D. Enable FortiNAC's access control with set access-control plc
- E. Integrate FortiSIEM to enforce PLC access policies

Answer: B

Explanation: Creating a network access policy in FortiNAC to allow only PLC device profiles restricts SCADA server access effectively.

Question: 277

An Operational Technology network administrator configures a FortiGate to protect a BACnet network. They need to log all BACnet WriteProperty requests for auditing. Which configuration achieves this?

- A. Use FortiAnalyzer to log all BACnet traffic
- B. Configure a firewall policy for BACnet port 47808 with logging enabled
- C. Enable logging in an application control profile with a custom BACnet signature
- D. Enable IPS logging for BACnet traffic
- E. Set up packet capture for BACnet port 47808

Answer: C

Explanation: To log BACnet WriteProperty requests, Enable logging in an application control profile with a custom BACnet signature is correct, as it targets specific BACnet requests. Configure a firewall policy for BACnet port 47808 with logging enabled logs all BACnet traffic, not specific requests. Use FortiAnalyzer to log all BACnet traffic is too broad. Enable IPS logging for BACnet traffic may log anomalies but not specific requests. Set up packet capture for BACnet port 47808 is inefficient, requiring manual analysis.



KILLEXAMS.COM

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:



Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.