

Fortinet

Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2



NEW QUESTION 1

An OT administrator configured and ran a default application risk and control report in FortiAnalyzer to learn more about the key application crossing the network. However, the report output is empty despite the fact that some related real-time and historical logs are visible in the FortiAnalyzer. What are two possible reasons why the report output was empty? (Choose two.)

- A. The administrator selected the wrong logs to be indexed in FortiAnalyzer.
- B. The administrator selected the wrong time period for the report.
- C. The administrator selected the wrong devices in the Devices section.
- D. The administrator selected the wrong hcache table for the report.

Answer: BC

Explanation:

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/32cb817d-a307-11eb-b70b-00505692583a/FortiAnalyzer-7.0.0-Administration_Guide.pdf

NEW QUESTION 2

When device profiling rules are enabled, which devices connected on the network are evaluated by the device profiling rules?

- A. Known trusted devices, each time they change location
- B. All connected devices, each time they connect
- C. Rogue devices, only when they connect for the first time
- D. Rogue devices, each time they connect

Answer: C

NEW QUESTION 3

To increase security protection in an OT network, how does application control on FortiGate detect industrial traffic?

- A. By inspecting software and software-based vulnerabilities
- B. By inspecting applications only on nonprotected traffic
- C. By inspecting applications with more granularity by inspecting subapplication traffic
- D. By inspecting protocols used in the application traffic

Answer: B

NEW QUESTION 4

Which three methods of communication are used by FortiNAC to gather visibility information? (Choose three.)

- A. SNMP
- B. ICMP
- C. API
- D. RADIUS
- E. TACACS

Answer: ACD

NEW QUESTION 5

Refer to the exhibit.

110 Cloud Applications require deep inspection
0 policies are using this profile.

Name: Allow_IEC-104_Transfer
Comments: 0/255

Categories

All Categories

Business (153, 6)

Game (86)

Network.Service (333)

Social.Media (117, 30)

VoIP (23)

Cloud.IT (67, 1)

GeneralInterest (236, 9)

P2P (56)

Storage.Backup (161, 19)

Web.Client (24)

Collaboration (267, 16)

Industrial (225)

Proxy (180)

Update (49)

Unknown Applications

☒ Network Protocol Enforcement

Application and Filter Overrides

Create New

Edit

Delete

| Priority | Details | Type | Action |
|----------|---|-------------|---------|
| 1 | IEC.60870.5.104_Information.Transfer IEC.60870.5.104_Control.Functions IEC.60870.5.104_Control.Functions.STARTDT.ACT IEC.60870.5.104_Control.Functions.STARTDT.CON | Application | Monitor |
| 2 | IEC.60870.5.104_Information.Transfer.C.BO.NA.1 | Application | Block |

An OT network security audit concluded that the application sensor requires changes to ensure the correct security action is committed against the overrides filters.

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. Set the priority of the C.BO.NA.1 signature override to 1.

D. Remove IEC.60870.5.104 Information.Transfer from the first filter override.

Answer: C

Explanation:

According to the Fortinet NSE 7 - OT Security 6.4 exam guide1, the application sensor settings allow you to configure the security action for each application category and network protocol override. The security action determines how the FortiGate unit handles traffic that matches the application category or network protocol override. The security action can be one of the following:

- ? Allow: The FortiGate unit allows the traffic without any further inspection.
- ? Monitor: The FortiGate unit allows the traffic and logs it for monitoring purposes.
- ? Block: The FortiGate unit blocks the traffic and logs it as an attack.

The priority of the network protocol override determines the order in which the FortiGate unit applies the security action to the traffic. The lower the priority number, the higher the priority. For example, a priority of 1 is higher than a priority of 10.

In the exhibit, the application sensor has the following settings:

- ? The industrial category has a security action of allow, which means that the FortiGate unit will not inspect or log any traffic that belongs to this category.
- ? The IEC.60870.5.104 Information.Transfer network protocol override has a security action of block, which means that the FortiGate unit will block and log any traffic that matches this protocol.
- ? The IEC.60870.5.104 Control.Functions network protocol override has a security action of monitor, which means that the FortiGate unit will allow and log any traffic that matches this protocol.
- ? The IEC.60870.5.104 Start/Stop network protocol override has a security action of allow, which means that the FortiGate unit will not inspect or log any traffic that matches this protocol.
- ? The IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override has a security action of block, which means that the FortiGate unit will block and log any traffic that matches this protocol.

The problem with these settings is that the IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override has a lower priority than the IEC.60870.5.104 Information.Transfer network protocol override. This means that if the traffic matches both protocols, the FortiGate unit will apply the security action of the higher priority override, which is block. However, the IEC.60870.5.104 Transfer.C.BO.NA.1 protocol is used to transfer binary outputs, which are essential for controlling OT devices. Therefore, blocking this protocol could have negative consequences for the OT network.

To fix this issue, the OT network administrator must set the priority of the IEC.60870.5.104 Transfer.C.BO.NA.1 network protocol override to 1, which is higher than the priority of the IEC.60870.5.104 Information.Transfer network protocol override. This way, the FortiGate unit will apply the security action of the lower priority override, which is allow, to the traffic that matches both protocols. This will ensure that the FortiGate unit does not block the traffic that is used to transfer binary outputs, while still blocking the traffic that is used to transfer information.

1: NSE 7 Network Security Architect - Fortinet

NEW QUESTION 6

An OT administrator is defining an incident notification policy using FortiSIEM and would like to configure the system with a notification policy. If an incident occurs, the administrator would like to be able to intervene and block an IP address or disable a user in Active Directory from FortiSIEM.

Which step must the administrator take to achieve this task?

A. Configure a fabric connector with a notification policy on FortiSIEM to connect with FortiGate.

B. Create a notification policy and define a script/remediation on FortiSIEM.

C. Define a script/remediation on FortiManager and enable a notification rule on FortiSIEM.

D. Deploy a mitigation script on Active Directory and create a notification policy on FortiSIEM.

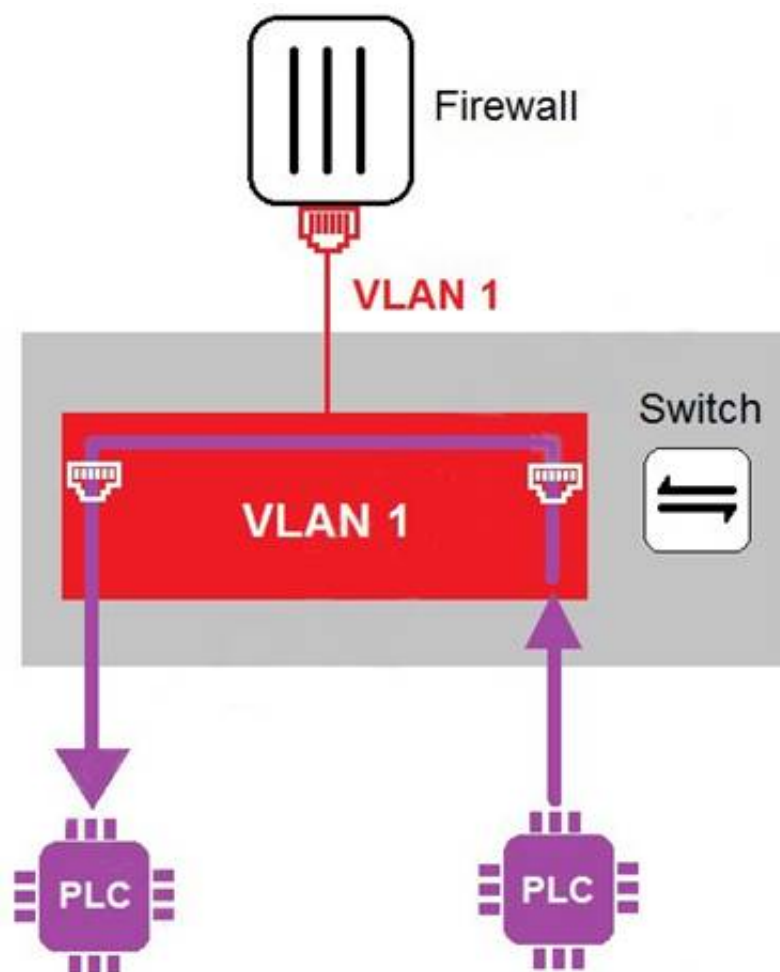
Answer: B

Explanation:

<https://fusecommunity.fortinet.com/blogs/silviu/2022/04/12/fortisiempublishingscript>

NEW QUESTION 7

Refer to the exhibit



In the topology shown in the exhibit, both PLCs can communicate directly with each other, without going through the firewall. Which statement about the topology is true?

- A. PLCs use IEEE802.1Q protocol to communicate each other.
- B. An administrator can create firewall policies in the switch to secure between PLCs.
- C. This integration solution expands VLAN capabilities from Layer 2 to Layer 3.
- D. There is no micro-segmentation in this topology.

Answer: D

NEW QUESTION 8

An OT network architect must deploy a solution to protect fuel pumps in an industrial remote network. All the fuel pumps must be closely monitored from the corporate network for any temperature fluctuations.

How can the OT network architect achieve this goal?

- A. Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature security rule on the corporate network.
- B. Configure a fuel server on the corporate network, and deploy a FortiSIEM with a single pattern temperature performance rule on the remote network.
- C. Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature performance rule on the corporate network.
- D. Configure both fuel server and FortiSIEM with a single-pattern temperature performance rule on the corporate network.

Answer: C

Explanation:

This way, FortiSIEM can discover and monitor everything attached to the remote network and provide security visibility to the corporate network

NEW QUESTION 9

An OT network administrator is trying to implement active authentication.

Which two methods should the administrator use to achieve this? (Choose two.)

- A. Two-factor authentication on FortiAuthenticator
- B. Role-based authentication on FortiNAC
- C. FSSO authentication on FortiGate
- D. Local authentication on FortiGate

Answer: AD

NEW QUESTION 10

An OT network consists of multiple FortiGate devices. The edge FortiGate device is deployed as the secure gateway and is only allowing remote operators to access the ICS networks on site.

Management hires a third-party company to conduct health and safety on site. The third- party company must have outbound access to external resources.

As the OT network administrator, what is the best scenario to provide external access to the third-party company while continuing to secure the ICS networks?

- A. Configure outbound security policies with limited active authentication users of the third- party company.
- B. Create VPN tunnels between downstream FortiGate devices and the edge FortiGate to protect ICS network traffic.
- C. Split the edge FortiGate device into multiple logical devices to allocate an independent VDOM for the third-party company.
- D. Implement an additional firewall using an additional upstream link to the internet.

Answer: C

NEW QUESTION 10

Refer to the exhibit.

Edit SubPattern

Name:industrial_protocol_monitor

Filters:

| Paren | Attribute | Operator | Value |
|-----------------------------------|--------------------------|----------|-----------------|
| <div><div></div><div></div></div> | Destination TCP/UDP Port | IN | Group: OT Ports |
| <div><div></div><div></div></div> | Source TCP/UDP Port | IN | Group: OT Ports |

Aggregate:

| Paren | Attribute | Operator | Value |
|-----------------------------------|-------------------------|----------|-------|
| <div><div></div><div></div></div> | COUNT(Matched Events) | >= | 1 |

Group By:

| Attribute | Row | Move |
|--------------------------|-----------------------------------|-----------------------------------|
| Reporting IP | <div><div></div><div></div></div> | <div><div></div><div></div></div> |
| Event Type | <div><div></div><div></div></div> | <div><div></div><div></div></div> |
| Destination TCP/UDP Port | <div><div></div><div></div></div> | <div><div></div><div></div></div> |
| Source TCP/UDP Port | <div><div></div><div></div></div> | <div><div></div><div></div></div> |

An operational technology rule is created and successfully activated to monitor the Modbus protocol on FortiSIEM. However, the rule does not trigger incidents despite Modbus traffic and application logs being received correctly by FortiSIEM. Which statement correctly describes the issue on the rule configuration?

- A. The first condition on the SubPattern filter must use the OR logical operator.
- B. The attributes in the Group By section must match the ones in Fitters section.
- C. The Aggregate attribute COUNT expression is incompatible with the filters.
- D. The SubPattern is missing the filter to match the Modbus protocol.

Answer: B

NEW QUESTION 14

Refer to the exhibit and analyze the output.

```
[PH_DEV_MON_NET_INTF_UTIL] : [eventSeverity] =PHL_INFO, [filename] =phPerfJob.cpp,
[lineNumber] =6646, [intfName]= Intel [R] PRO_100 MT Network
Connection, [intfAlias] =, [hostname] =WIN2K8DC, [hostIpAddr] = 192.168.69.6,
[pollIntv] =56, [recvBytes64] =
44273, [recvBitsPerSec] = 6324.714286, [inIntfUtil] = 0.000632, [sentBytes64] =
82014, [sentBitsPerSec] = 1171
6.285714, [outIntfUtil] = 0.001172, [recvPkts64] = 449, [sentPkts64] = 255,
[inIntfPktErr] = 0, [inIntfPktErrPct] = 0.000000, [outIntfPktErr] =0,
[outIntfPktErrPct] = 0.000000, [inIntfPktDiscarded] =0, [inIntfPktDiscardedPct] =
```

Which statement about the output is true?

- A. This is a sample of a FortiAnalyzer system interface event log.
- B. This is a sample of an SNMP temperature control event log.
- C. This is a sample of a PAM event type.
- D. This is a sample of FortiGate interface statistics.

Answer: C

NEW QUESTION 18

What triggers Layer 2 polling of infrastructure devices connected in the network?

- A. A failed Layer 3 poll
- B. A matched security policy
- C. A matched profiling rule
- D. A linkup or linkdown trap

Answer: D

NEW QUESTION 19

Which three criteria can a FortiGate device use to look for a matching firewall policy to process traffic? (Choose three.)

- A. Services defined in the firewall policy.
- B. Source defined as internet services in the firewall policy
- C. Lowest to highest policy ID number
- D. Destination defined as internet services in the firewall policy
- E. Highest to lowest priority defined in the firewall policy

Answer:

ADE

Explanation:

The three criteria that a FortiGate device can use to look for a matching firewall policy to process traffic are:

- * A. Services defined in the firewall policy - FortiGate devices can match firewall policies based on the services defined in the policy, such as HTTP, FTP, or DNS.
- * D. Destination defined as internet services in the firewall policy - FortiGate devices can also match firewall policies based on the destination of the traffic, including destination IP address, interface, or internet services.
- * E. Highest to lowest priority defined in the firewall policy - FortiGate devices can prioritize firewall policies based on the priority defined in the policy. The device will process traffic against the policy with the highest priority first and move down the list until it finds a matching policy.

Reference:

Fortinet NSE 7 - Enterprise Firewall 6.4 Study Guide, Chapter 4: Policy Implementation, page 4-18.

NEW QUESTION 24

As an OT network administrator, you are managing three FortiGate devices that each protect different levels on the Purdue model. To increase traffic visibility, you are required to implement additional security measures to detect exploits that affect PLCs.

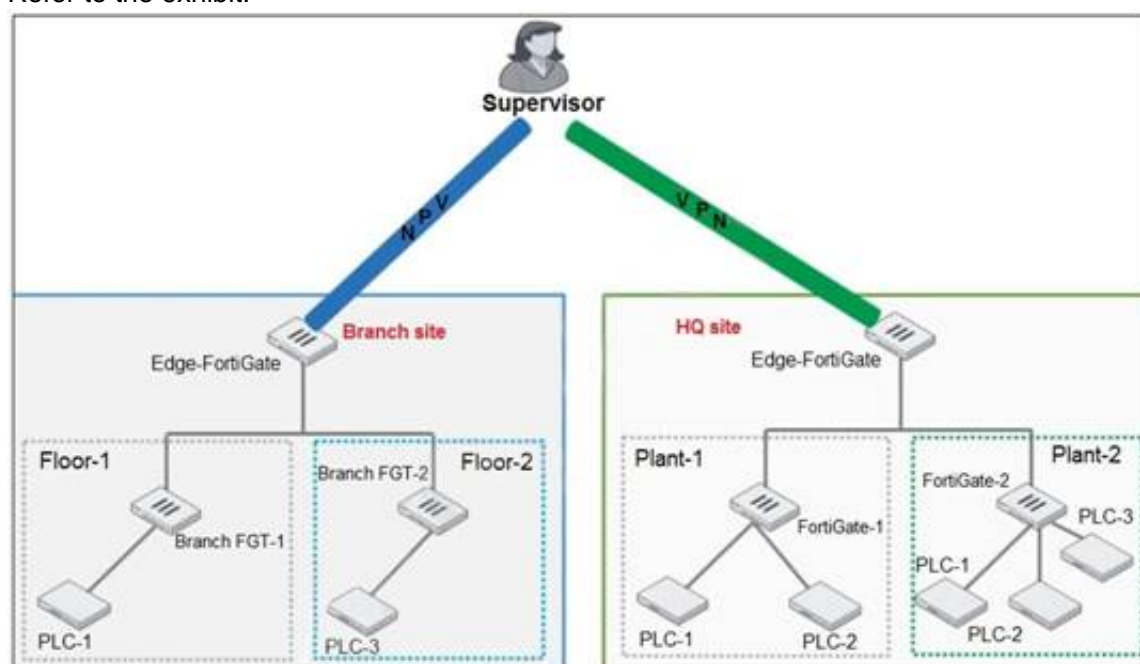
Which security sensor must implement to detect these types of industrial exploits?

- A. Intrusion prevention system (IPS)
- B. Deep packet inspection (DPI)
- C. Antivirus inspection
- D. Application control

Answer: B

NEW QUESTION 25

Refer to the exhibit.



You need to configure VPN user access for supervisors at the branch and HQ sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must you do to achieve this objective?

- A. You must use a FortiAuthenticator.
- B. You must register the same FortiToken on more than one FortiGate.
- C. You must use the user self-registration server.
- D. You must use a third-party RADIUS OTP server.

Answer: A

NEW QUESTION 29

An OT network architect needs to secure control area zones with a single network access policy to provision devices to any number of different networks. On which device can this be accomplished?

- A. FortiGate
- B. FortiEDR
- C. FortiSwitch
- D. FortiNAC

Answer: A

Explanation:

An OT network architect can accomplish the goal of securing control area zones with a single network access policy to provision devices to any number of different networks on a FortiGate device.

NEW QUESTION 31

An administrator wants to use FortiSoC and SOAR features on a FortiAnalyzer device to detect and block any unauthorized access to FortiGate devices in an OT network.

Which two statements about FortiSoC and SOAR features on FortiAnalyzer are true? (Choose two.)

- A. You must set correct operator in event handler to trigger an event.
- B. You can automate SOC tasks through playbooks.
- C. Each playbook can include multiple triggers.

D. You cannot use Windows and Linux hosts security events with FortiSoC.

Answer: AB

Explanation:

Ref: <https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/268882/fortisoc>

NEW QUESTION 35

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: BC

NEW QUESTION 39

An OT administrator deployed many devices to secure the OT network. However, the SOC team is reporting that there are too many alerts, and that many of the alerts are false positive. The OT administrator would like to find a solution that eliminates repetitive tasks, improves efficiency, saves time, and saves resources. Which products should the administrator deploy to address these issues and automate most of the manual tasks done by the SOC team?

- A. FortiSIEM and FortiManager
- B. FortiSandbox and FortiSIEM
- C. FortiSOAR and FortiSIEM
- D. A syslog server and FortiSIEM

Answer: C

NEW QUESTION 42

In a wireless network integration, how does FortiNAC obtain connecting MAC address information?

- A. RADIUS
- B. Link traps
- C. End station traffic monitoring
- D. MAC notification traps












Answer: A

Explanation:

FortiNAC can integrate with RADIUS servers to obtain MAC address information for wireless clients that authenticate through the RADIUS server. Reference: Fortinet NSE 7 - OT Security 6.4 Study Guide, Chapter 4: OT Security Devices, page 4-28.

NEW QUESTION 45

Refer to the exhibit.

| Maint | Device | Type | Organization | Avail Status | Perf Status | Security Status |
|---|------------------|---------------------|--------------|---|--|---|
|  | FG240D3913800441 | Fortinet FortiOS | Super |  |  |  |
|  | SJ-QA-F-Lnx-CHK | Checkpoint FireWall | Super |  |  |  |
|  | FAPS321C-default | Fortinet FortiAP | Super | |  |  |

You are navigating through FortiSIEM in an OT network.

How do you view information presented in the exhibit and what does the FortiGate device security status tell you?

- A. In the PCI logging dashboard and there are one or more high-severity security incidents for the FortiGate device.
- B. In the summary dashboard and there are one or more high-severity security incidents for the FortiGate device.
- C. In the widget dashboard and there are one or more high-severity incidents for the FortiGate device.
- D. In the business service dashboard and there are one or more high-severity security incidents for the FortiGate device.

Answer: B

NEW QUESTION 46

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE7_OTS-7.2 Practice Exam Features:

- * NSE7_OTS-7.2 Questions and Answers Updated Frequently
- * NSE7_OTS-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_OTS-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_OTS-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_OTS-7.2 Practice Test Here](#)