Fortinet

Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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.
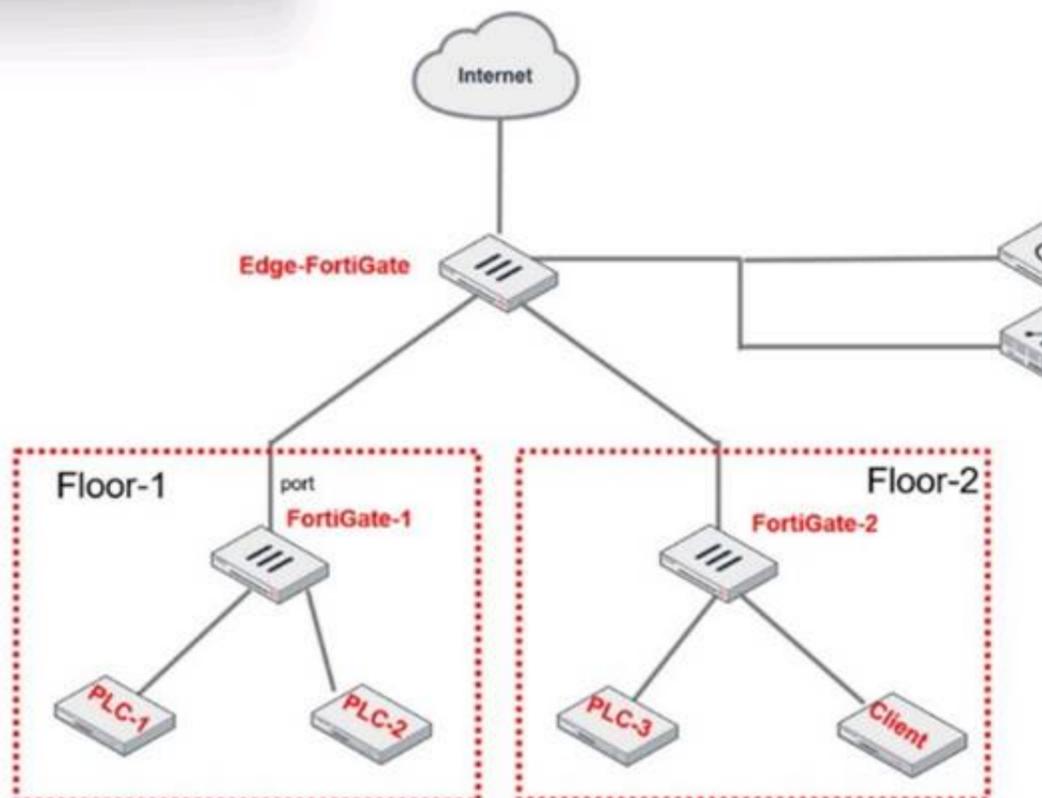
Answer: C

NEW QUESTION 4

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 5

Refer to the exhibit.

PLC-3 and CLIENT can send traffic to PLC-1 and PLC-2. FGT-2 has only one software switch (SSW-1) connecting both PLC-3 and CLIENT. PLC-3 and CLIENT can send traffic to each other at the Layer 2 level.
What must the OT admin do to prevent Layer 2-level communication between PLC-3 and CLIENT?

A. Set a unique forward domain for each interface of the software switch.
B. Create a VLAN for each device and replace the current FGT-2 software switch members.
C. Enable explicit intra-switch policy to require firewall policies on FGT-2.
D. Implement policy routes on FGT-2 to control traffic between devices.

Answer: AB

NEW QUESTION 6
Which three Fortinet products can be used for device identification in an OT industrial control system (ICS)? (Choose three.)

A. FortiNAC
B. FortiManager
C. FortiAnalyzer
D. FortiSIEM
E. FortiGate

Answer: ADE

Explanation:
 A. FortiNAC - FortiNAC is a network access control solution that provides visibility and control over network devices. It can identify devices, enforce access policies, and automate threat response.
* D. FortiSIEM - FortiSIEM is a security information and event management solution that can collect and analyze data from multiple sources, including network devices and servers. It can help identify potential security threats, as well as monitor compliance with security policies and regulations.
* E. FortiAnalyzer - FortiAnalyzer is a central logging and reporting solution that collects and analyzes data from multiple sources, including FortiNAC and FortiSIEM. It can provide insights into network activity and help identify anomalies or security threats.
Reference:
Fortinet NSE 7 - OT Security 6.4 Study Guide, Chapter 4: OT Security Devices, page 4-20.

NEW QUESTION 7
Which three common breach points can be found in a typical OT environment? (Choose three.)

A. Global hat
B. Hard hat
C. VLAN exploits
D. Black hat
E. RTU exploits

Answer: BDE

NEW QUESTION 8
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 9
An OT architect has deployed a Layer 2 switch in the OT network at Level 1 the Purdue model-process control. The purpose of the Layer 2 switch is to segment traffic between PLC1 and PLC2 with two VLANs. All the traffic between PLC1 and PLC2 must first flow through the Layer 2 switch and then through the FortiGate device in the Level 2 supervisory control network.
What statement about the traffic between PLC1 and PLC2 is true?

A. The Layer 2 switch rewrites VLAN tags before sending traffic to the FortiGate device.
B. The Layer 2 switches routes any traffic to the FortiGate device through an Ethernet link.
C. PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.
D. In order to communicate, PLC1 must be in the same VLAN as PLC2.

Answer: C

Explanation:
The statement that is true about the traffic between PLC1 and PLC2 is that PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.

NEW QUESTION 10
......

Relate Links

100% Pass Your NSE7_OTS-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/NSE7_OTS-7.2-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/