Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2

https://www.2passeasy.com/dumps/NSE7_OTS-7.2/

NEW QUESTION 1
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 2
How can you achieve remote access and internel availability in an OT network?

A. Create a back-end backup network as a redundancy measure.
B. Implement SD-WAN to manage traffic on each ISP link.
C. Add additional internal firewalls to access OT devices.
D. Create more access policies to prevent unauthorized access.

Answer: B

NEW QUESTION 3
To increase security protection in an OT network, how does application control on ForliGate 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 two frameworks are common to secure ICS industrial processes, including SCADA and DCS? (Choose two.)

A. Modbus
B. NIST Cybersecurity
C. IEC 62443
D. IEC104

Answer: CD

NEW QUESTION 5
Refer to the exhibit.

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 andnetwork 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
Which two statements about the Modbus protocol are true? (Choose two.)

A. Modbus uses UDP frames to transport MBAP and function codes.
B. Most of the PLC brands come with a built-in Modbus module.
C. You can implement Modbus networking settings on internetworking devices.
D. Modbus is used to establish communication between intelligent devices.

Answer: BC

NEW QUESTION 7
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

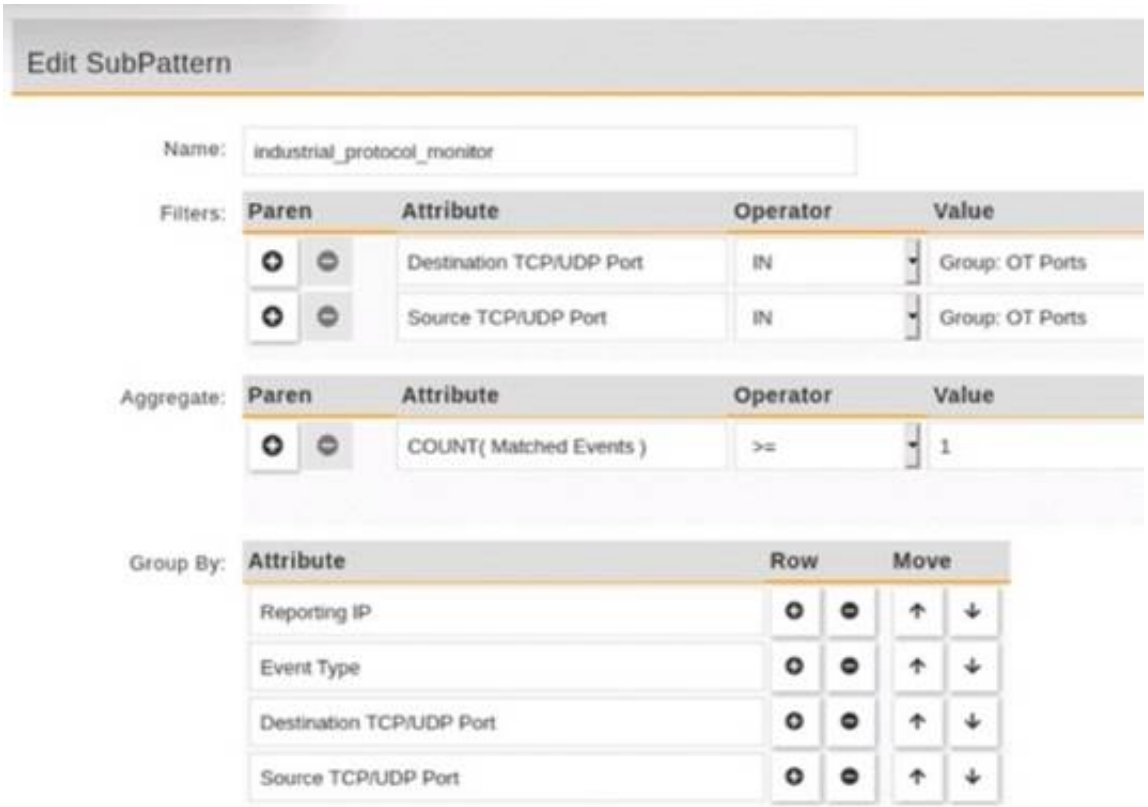
Answer: AD

NEW QUESTION 8
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 9
Refer to the exhibit.



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 10
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 10
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 11
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 16
An OT administrator has configured FSSO and local firewall authentication. A user who is part of a user group is not prompted from credentials during authentication.
What is a possible reason?

A. FortiGate determined the user by passive authentication
B. The user was determined by Security Fabric
C. Two-factor authentication is not configured with RADIUS authentication method
D. FortiNAC determined the user by DHCP fingerprint method

Answer: A

NEW QUESTION 21
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 24
What two advantages does FortiNAC provide in the OT network? (Choose two.)

A. It can be used for IoT device detection.
B. It can be used for industrial intrusion detection and prevention.
C. It can be used for network micro-segmentation.
D. It can be used for device profiling.

Answer: AD

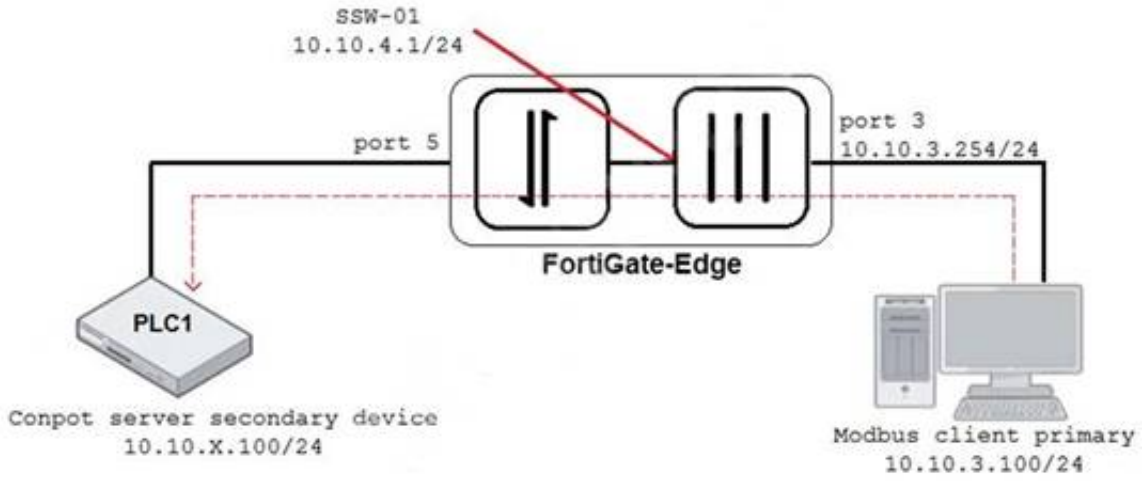
Explanation:
Typically, in a microsegmented network, NGFWs are used in conjunction with VLANs to implement security policies and to inspect and filter network communications. Fortinet FortiSwitch and FortiGate NGFW offer an integrated approach to microsegmentation.

NEW QUESTION 27
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 31
Refer to the exhibit.

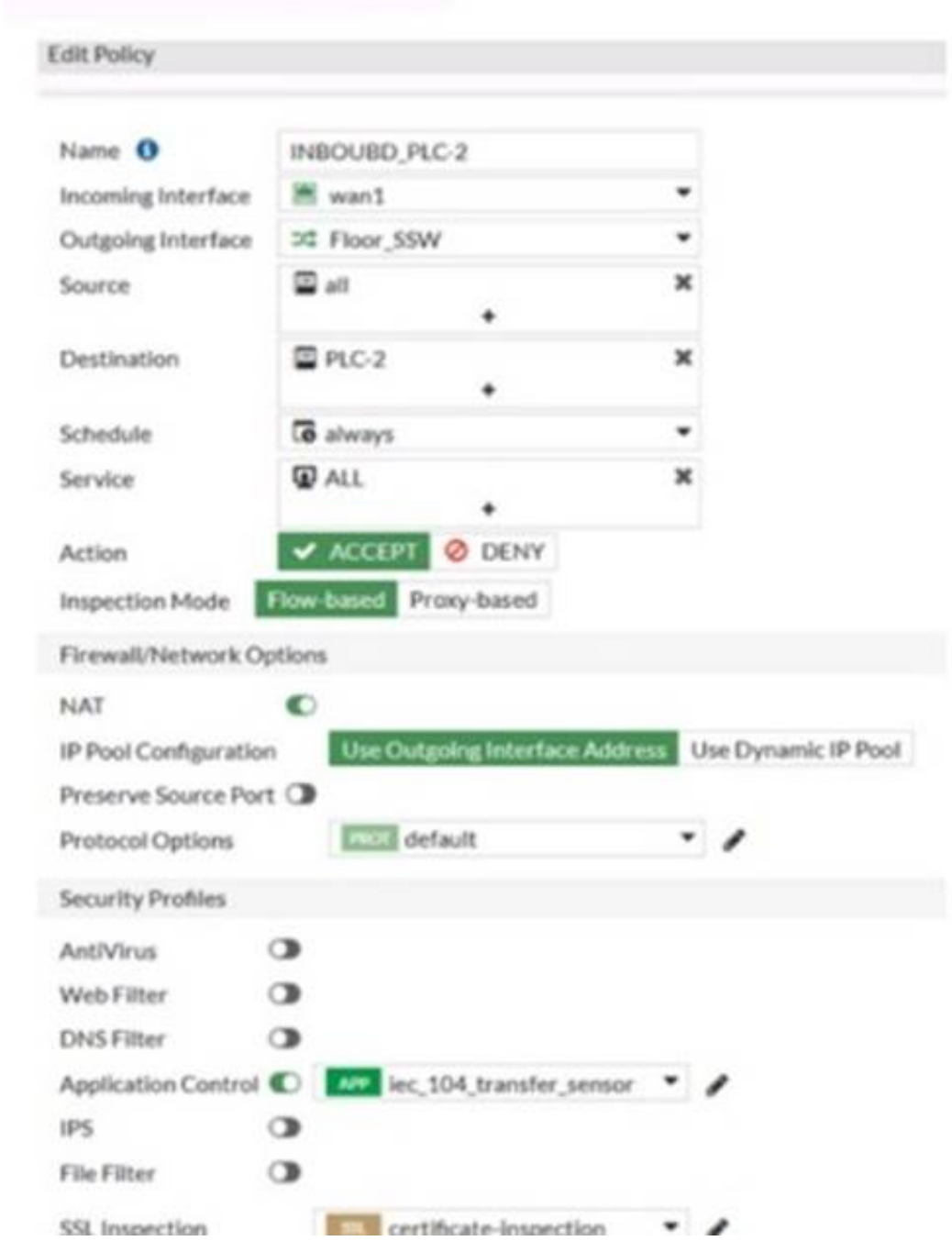


An OT architect has implemented a Modbus TCP with a simulation server Conpot to identify and control the Modus traffic in the OT network. The FortiGate-Edge device is configured with a software switch interface ssw-01.
Based on the topology shown in the exhibit, which two statements about the successful simulation of traffic between client and server are true? (Choose two.)

A. The FortiGate-Edge device must be in NAT mode.
B. NAT is disabled in the FortiGate firewall policy from port3 to ssw-01.
C. The FortiGate devices is in offline IDS mode.
D. Port5 is not a member of the software switch.

Answer: AB

NEW QUESTION 35
Refer to the exhibits.



Which statement is true about the traffic passing through to PLC-2?

A. IPS must be enabled to inspect application signatures.
B. The application filter overrides the default action of some IEC 104 signatures.
C. IEC 104 signatures are all allowed except the C.BO.NA 1 signature.
D. SSL Inspection must be set to deep-inspection to correctly apply application control.

Answer: B

NEW QUESTION 40
Refer to the exhibit.

```
config system interface
     edit VLAN101_dmz
          set forward-domain 101
next
     edit VLAN101_internal
          set forward-domain 101
end
```

Given the configurations on the FortiGate, which statement is true?

A. FortiGate is configured with forward-domains to reduce unnecessary traffic.
B. FortiGate is configured with forward-domains to forward only domain controller traffic.
C. FortiGate is configured with forward-domains to forward only company domain website traffic.
D. FortiGate is configured with forward-domains to filter and drop non-domain controller traffic.

Answer: A

NEW QUESTION 41

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_OTS-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_OTS-7.2 Product From:

https://www.2passeasy.com/dumps/NSE7_OTS-7.2/

Money Back Guarantee

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