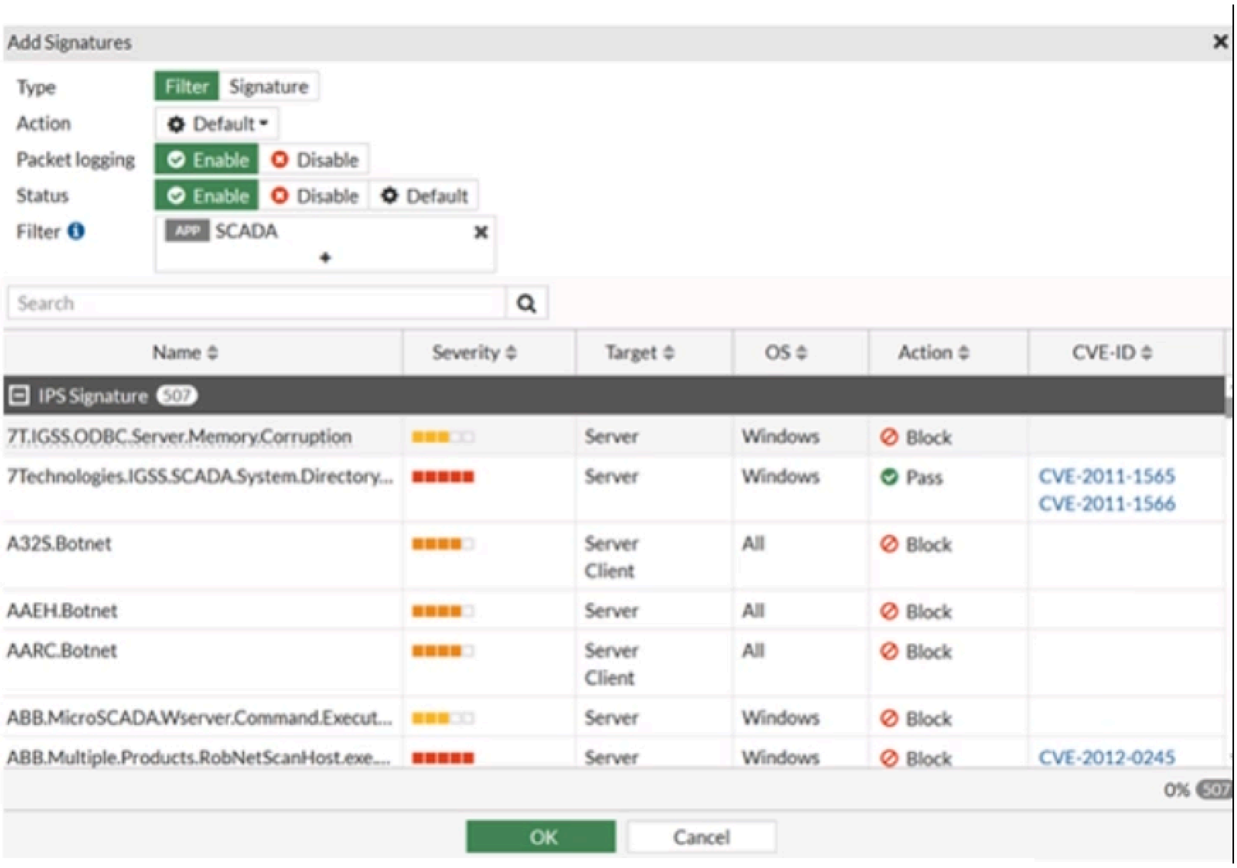
Question #1 *Topic 1*

Refer to the exhibit.



Add Signatures

Type	**Filter** Signature
Action	Default
Packet logging	**Enable** Disable
Status	**Enable** Disable Default
Filter	APP SCADA

Search

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 507					
7T.IGSS.ODBC.Server.Memory.Corruption	■■■□□	Server	Windows	⊘ Block	
7Technologies.IGSS.SCADA.System.Directory...	■■■■■	Server	Windows	✓ Pass	CVE-2011-1565 CVE-2011-1566
A32S.Botnet	■■■■□	Server Client	All	⊘ Block	
AAEH.Botnet	■■■■□	Server	All	⊘ Block	
AARC.Botnet	■■■■□	Server Client	All	⊘ Block	
ABB.MicroSCADA.Wserver.Command.Execut...	■■■□□	Server	Windows	⊘ Block	
ABB.Multiple.Products.RobNetScanHost.exe...	■■■■■	Server	Windows	⊘ Block	CVE-2012-0245

0% 507

The IPS profile is added on all of the security policies on FortiGate.

For an OT network, which statement of the IPS profile is true?

A. FortiGate has no IPS industrial signature database enabled.

B. The listed IPS signatures are classified as SCADA applications.

C. All IPS signatures are overridden and must block traffic match signature patterns.

D. The IPS profile inspects only traffic originating from SCADA equipment.

Suggested Answer: *B*

Community vote distribution

B (100%)

datomb74 5 months, 1 week ago

Selected Answer: B

Studyguide P188

upvoted 2 times

zufyozirke 8 months ago

Selected Answer: B

Agree with B

upvoted 1 times

Question #2 *Topic 1*

Which two statements are true when you deploy FortiGate as an offline IDS? (Choose two.)

A. Network traffic goes through FortiGate.

B. Network attacks can be detected and blocked.

C. FortiGate acts as network sensor.

D. FortiGate receives traffic from configured port mirroring.

Suggested Answer: *CD*

Community vote distribution

CD (100%)

hem82 3 weeks, 3 days ago

Selected Answer: CD

correct ans C & D

upvoted 1 times

flbcobra 4 months, 1 week ago

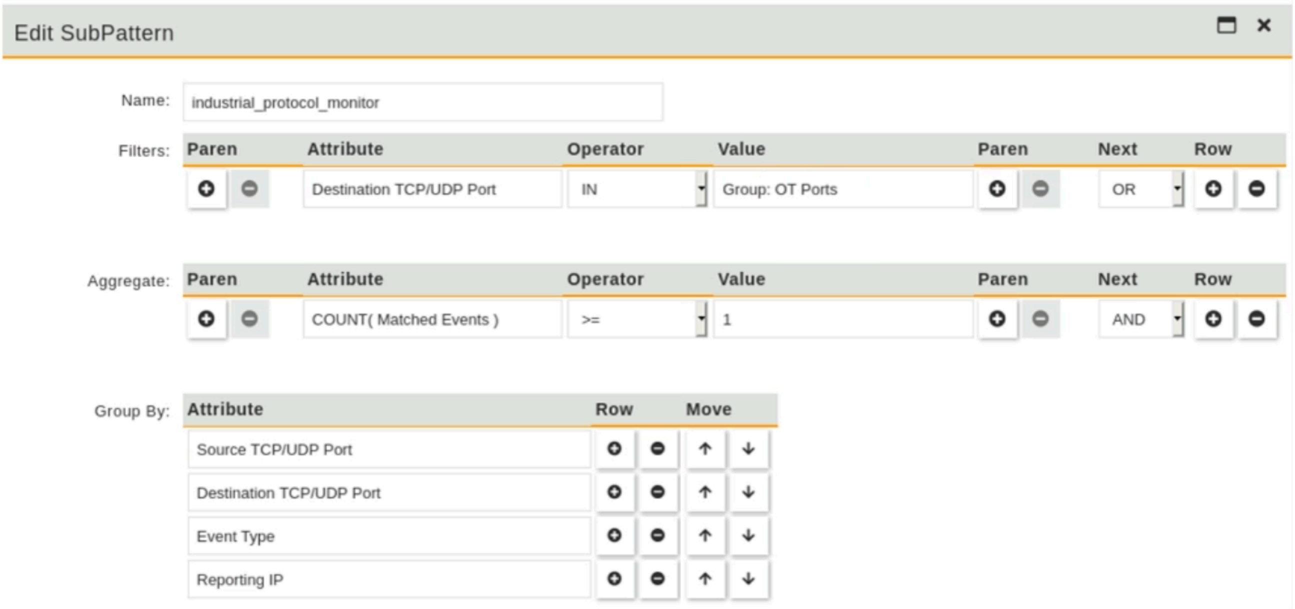
Selected Answer: CD

Page 190

upvoted 2 times

Question #3 *Topic 1*

Refer to the exhibit.



Edit SubPattern

Name: industrial_protocol_monitor

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	Destination TCP/UDP Port	IN	Group: OT Ports	⊕ ⊖	OR	⊕ ⊖

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
⊕ ⊖	COUNT(Matched Events)	>=	1	⊕ ⊖	AND	⊕ ⊖

Group By:

Attribute	Row	Move
Source TCP/UDP Port	⊕ ⊖	↑ ↓
Destination TCP/UDP Port	⊕ ⊖	↑ ↓
Event Type	⊕ ⊖	↑ ↓
Reporting IP	⊕ ⊖	↑ ↓

A new operational technology rule is being created to monitor Modbus protocol traffic on FortiSIEM.
Which action will ensure all Modbus messages on the network match the rule?

A. Set the Aggregate attribute value to equal to or greater than zero.

B. Add a new condition to filter Modbus traffic based on the Source TCP/UDP port.

C. This rule is valid and requires no additional changes.

D. Remove attributes in the Group By section that are not configured in the Filter section.

Suggested Answer: *B*

Community vote distribution

B (100%)

⊟ **Dogbert** 5 months, 1 week ago

Selected Answer: B

Page 242

upvoted 1 times

Question #4 *Topic 1*

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 protocols from PLCs.
Which security sensor must you implement to detect protocols on the OT network?

A. Antivirusinspection

B. Intrusion prevention system (IPS)

C. Application control

D. Deep packet inspection (DPI)

Suggested Answer: *C*

Community vote distribution

C (71%) 14% 14%

⊟ **L_U_P_I_N** 5 months, 2 weeks ago

Selected Answer: D

Deep Packet Inspection (DPI) is required to analyze industrial protocols such as Modbus, DNP3, IEC 60870-5-104, etc., by inspecting packet contents beyond the headers.

This allows FortiGate to recognize and classify OT protocols, even if they use non-standard ports.

upvoted 1 times

⊟ **ali_red** 8 months ago

Selected Answer: C

page 192 of course

upvoted 1 times

⊟ **joetorres10** 8 months, 3 weeks ago

Selected Answer: C

pg 192 of study guide

upvoted 2 times

⊟ **6bee64f** 10 months, 2 weeks ago

Selected Answer: C

From the study guide, IPS is related to exploit vulnerabilities, while app control is related to have OT protocols visibility

upvoted 1 times

⊟ **j0hn_cena** 11 months, 3 weeks ago

Selected Answer: C

Correct answer is C

OT_ Security_7.2_Study_Guide

upvoted 1 times

⊟ **Melina_amira** 11 months, 4 weeks ago

Selected Answer: B

I think the right answer is B

upvoted 1 times

Question #5 *Topic 1*

You are investigating a series of incidents that occurred in the OT network over past 24 hours in FortiSIEM.
Which three FortiSIEM options can you use to investigate these incidents? (Choose three.)

A. Risk

B. IPS

C. List

D. Security

E. Overview

Suggested Answer: *ACE*

Community vote distribution

ACE (100%)

ali_red 8 months ago

Selected Answer: ACE

Page 244 of Study guide, you can see the complete list of INCIDENT views

upvoted 1 times

Question #6 *Topic 1*

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

A. Two-factor authentication is not configured with the RADIUS authentication method.

B. The user was determined by the Security Fabric.

C. FortiGate determined the user by passive authentication.

D. FortiNAC determined the user by the DHCP fingerprint method.

Suggested Answer: *C*

Community vote distribution

C (100%)

ali_red 8 months ago

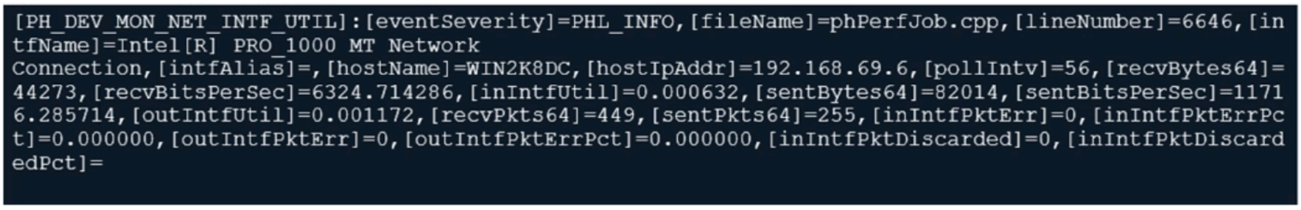
Selected Answer: C

C for sure, page 97 of study guide

upvoted 1 times

Question #7 *Topic 1*

Refer to the exhibit.



```
[PH_DEV_MON_NET_INTF_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=6646,[in
tfName]=Intel[R] PRO_1000 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,[inIntfPktErrPc
t]=0.000000,[outIntfPktErr]=0,[outIntfPktErrPct]=0.000000,[inIntfPktDiscarded]=0,[inIntfPktDiscard
edPct]=
```

From your analysis of the output, which statement about the output is true?

A. This is a sample of an SNMP temperature control event log.

B. This is a sample of a FortiAnalyzer system interface event log.

C. This is a sample of a PAM event type.

D. This is a sample of FortiGate interface statistics.

Suggested Answer: *C*

Community vote distribution

C (100%)

ali_red 8 months ago

Selected Answer: C

PAM event type, page 231 Study guide

upvoted 2 times

fortilearner 10 months ago

Selected Answer: C

I think D is wrong. Study guide p. 231. ph_dev_mon is a PAM event. Hostname is WIN2K8DC (a win server) not Fortigate.

upvoted 3 times

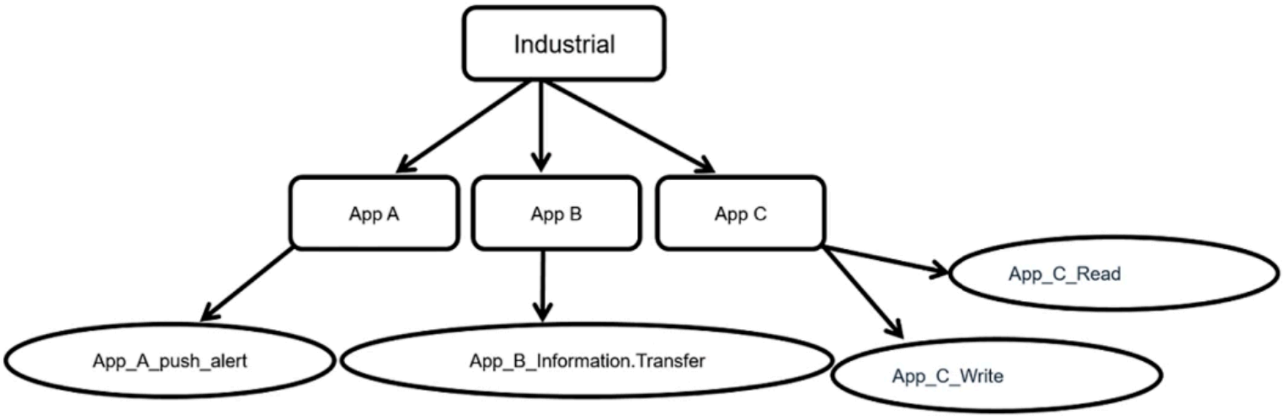
pereirarj 9 months ago

You're right. It's a PAM event.

upvoted 1 times

Question #8 Topic 1

Refer to the exhibit.



Which statement is true about application control inspection?

A. The industrial application control inspection process is unique among application categories.

B. Security actions cannot be applied on the lowest level of the hierarchy.

C. You can control security actions only on the parent-level application signature.

D. The parent signature takes precedence over the child application signature.

Suggested Answer: *D*

Community vote distribution

D (100%)

datomb74 5 months, 1 week ago

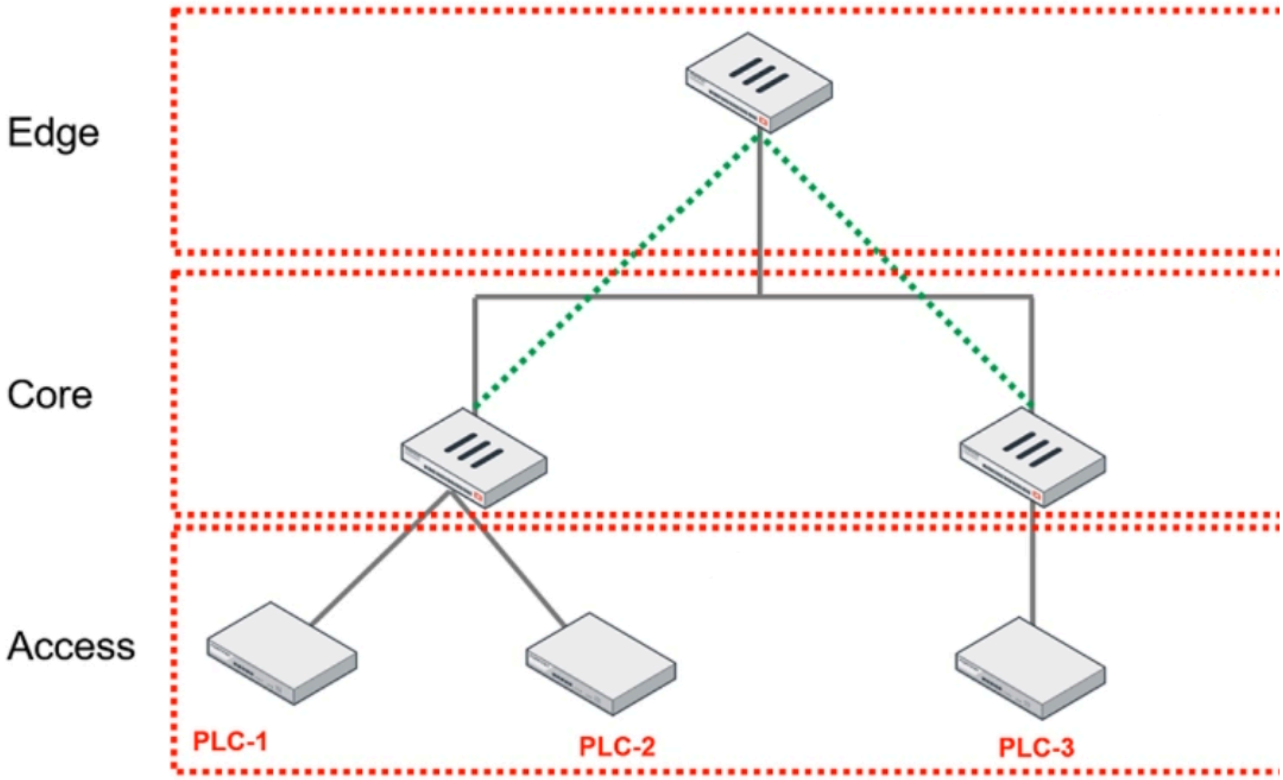
Selected Answer: D

Studyguide P195

upvoted 2 times

Question #9 *Topic 1*

Refer to the exhibit.



You are assigned to implement a remote authentication server in the OT network.
Which part of the hierarchy should the authentication server be part of?

A. Edge

B. Cloud

C. Core

D. Access

Suggested Answer: *A*

Community vote distribution

A (67%) C (33%)

L_U_P_I_N 5 months, 2 weeks ago

Selected Answer: A

Answer (C) if using Fortigate as an authentication server, but in this question they are referring to remote authentication server, so the answer is (A) according to the study guide page 101

upvoted 1 times

f9e691d 6 months ago

Selected Answer: A

Edge device

upvoted 1 times

ali_red 8 months ago

Selected Answer: C

Page 95 Study guide, "Fortigate can be used as an authentication server"

upvoted 1 times

pereirarj 9 months ago

Selected Answer: A

Page 101 shows it clearly that you're supposed to have it on the Edge

upvoted 1 times

edu1718 10 months ago

Selected Answer: A

OT Security 7.2 Study Guide P101 -> Edge

upvoted 1 times

6bee64f 10 months, 2 weeks ago

Selected Answer: C

From the exam guide it refers to Core, while standards talk about iDMZ which should be close to OT core (IT/OT segmentation)

upvoted 1 times

Question #10 *Topic 1*

With the limit of using one firewall device, the administrator enables multi-VDOM on FortiGate to provide independent multiple security domains to each ICS network.
Which statement ensures security protection is in place for all ICS networks?

A. Each traffic VDOM must have a direct connection to FortiGuard services to receive the required security updates.

B. The management VDOM must have access to all global security services.

C. Each VDOM must have an independent security license.

D. Traffic between VDOMs must pass through the physical interfaces of FortiGate to check for security incidents.

Suggested Answer: *B*

Community vote distribution

B (75%) D (25%)

hem82 3 weeks, 3 days ago

Selected Answer: B

B, page 162 Study guide. Question ask about management vdom

upvoted 1 times

4efd50b 2 months, 2 weeks ago

Selected Answer: D

Management is just used to managed the other VDOMs, not to inspect the traffic that flows between the virtual firewalls.

upvoted 1 times

ali_red 8 months ago

Selected Answer: B

B, page 162 Study guide

upvoted 2 times

Question #11

Topic 1

What are two critical tasks the OT network auditors must perform during OT network risk assessment and management? (Choose two.)

A. Implementing strategies to automatically bring PLCs offline

B. Planning a threat hunting strategy

C. Creating disaster recovery plans to switch operations to a backup plant

D. Evaluating what can go wrong before it happens

Suggested Answer: *BD*

Community vote distribution

BD (100%)

⊟ **L_U_P_I_N** 5 months, 2 weeks ago

Selected Answer: BD

Study guide page 257

upvoted 1 times

Question #12 *Topic 1*

Which type of attack posed by skilled and malicious users of security level 3 (SL 3) of IEC 62443 is designed to defend against intentional attacks?

A. Unintentional operator error

B. Access to moderate resources

C. Low access to resources

D. Substantial resources

Suggested Answer: *B*

Community vote distribution

B (100%)

L_U_P_I_N 5 months, 2 weeks ago

Selected Answer: B

Study guide page 26

upvoted 1 times

Question #13 *Topic 1*

The OT network analyst run different level of reports to quickly explore failures that could put the network at risk. Such reports can be about device performance.

Which FortiSIEM reporting method helps to identify device failures?

A. Business service reports

B. Device inventory reports

C. CMDB operational reports

D. Active dependent rules reports

Suggested Answer: *C*

Community vote distribution

C (100%)

BetoHernandezz 3 months, 1 week ago

Selected Answer: C

page 278

upvoted 1 times

Question #14 *Topic 1*

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

A. MAC notification traps

B. Link traps

C. RADIUS

D. End station traffic monitoring

Suggested Answer: *C*

Community vote distribution

C (100%)

053eb20 2 months, 1 week ago

Selected Answer: C

It is absolutely C, as in a wireless network, endpoints connect via access points, which often requires authentication, in this case FortiNAC would rely on RADIUS auth messages from the AP/Controller to identify the MAC address

upvoted 1 times

L_U_P_I_N 5 months, 2 weeks ago

Selected Answer: C

But A also is correct reffering to the study guide page 48

upvoted 1 times

Question #15 *Topic 1*

What can you assign using network access control policies?

A. Layer 3 polling intervals

B. FortiNAC device polling methods

C. Profiling rules

D. Logical networks

Suggested Answer: *C*

Community vote distribution

D (100%)

79ba84e 4 months, 2 weeks ago

Selected Answer: D

Pg 124 of the Study Guide -

upvoted 1 times

Inceptenet 5 months ago

Selected Answer: D

D is correct. A profiling rule helps to assign the Logical network.

upvoted 1 times

Question #16 *Topic 1*

FortiAnalyzer is implemented in the OT network to receive logs from responsible FortiGate devices. The logs must be processed by FortiAnalyzer. In this scenario, which statement is correct about the purpose of FortiAnalyzer receiving and processing multiple log messages from a given PLC or RTU?

A. To isolate PLCs or RTUs in the event of external attacks

B. To configure event handlers and take further action on FortiGate

C. To determine which type of messages from the PLC or RTU causes issues in the plant

D. To help OT administrators configure the network and prevent breaches

Suggested Answer: *C*

Community vote distribution

D (50%) C (50%)

053eb20 2 months, 1 week ago

Selected Answer: C

I believe the correct answer is C because multiple log messages help FortiAnalyzer reveal operational patterns, these logs contain function codes and timestamps the help trace event sequences

upvoted 1 times

BetoHernandezz 3 months, 1 week ago

Selected Answer: D

page 212

upvoted 1 times

Question #17 *Topic 1*

How can you achieve remote access and internet availability in an OT network?

A. Add additional internal firewalls to access OT devices.

B. Implement SD-WAN to manage traffic on each ISP link.

C. Create more access policies to prevent unauthorized access.

D. Create a back-end backup network as a redundancy measure.

Suggested Answer: *B*

Community vote distribution

B (100%)

BetoHernandezz 3 months, 1 week ago

Selected Answer: B

page 156

upvoted 1 times

Question #18 *Topic 1*

What are two benefits of a Nozomi integration with FortiNAC? (Choose two.)

A. Importation and classification of hosts

B. Enhanced point of connection details

C. Adapter consolidation for multi-adapter hosts

D. Direct VLAN assignment

Suggested Answer: *AC*

Community vote distribution

AC (100%)

hem82 3 weeks, 1 day ago

Selected Answer: AC

Study guide page 87

upvoted 1 times

L_U_P_I_N 5 months, 2 weeks ago

Selected Answer: AC

Study guide page 87

upvoted 1 times

datomb74 5 months, 2 weeks ago

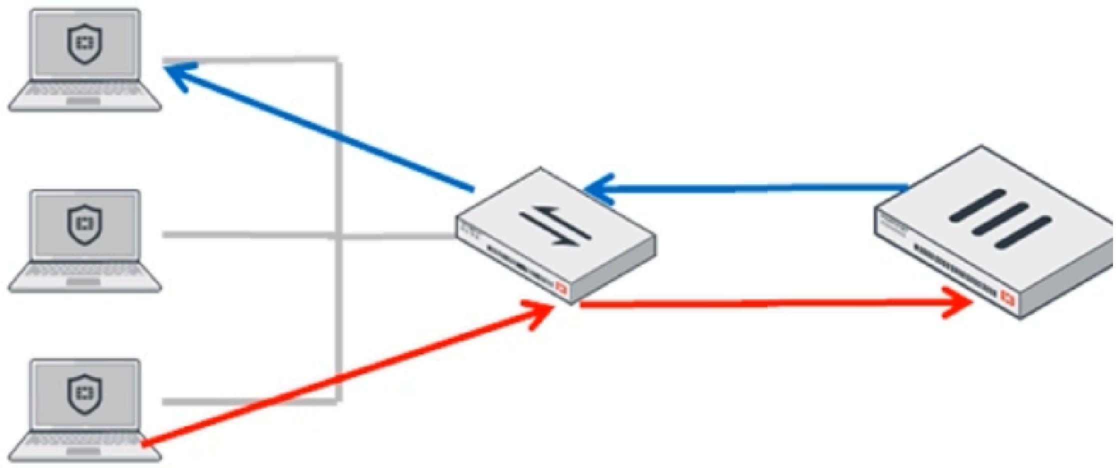
Selected Answer: AC

Study Guide Page 87

upvoted 1 times

Question #19 *Topic 1*

Refer to the exhibit.



In order for a FortiGate device to act as router on a stick, what configuration must an OT network architect implement on FortiGate to achieve inter-VLAN routing?

A. Set a unique forward domain on each interface on the network.

B. Set FortiGate to operate in transparent mode.

C. Set a software switch on FortiGate to handle inter-VLAN traffic.

D. Set a FortiGate interface with the switch to operate as an 802.1q trunk.

Suggested Answer: *D*

Community vote distribution

D (100%)

7b702a7 3 months, 4 weeks ago

Selected Answer: D

Page 139 of the study guide

upvoted 1 times

Question #20 *Topic 1*

Which three Fortinet products can you use for device identification in an OT industrial control system (ICS)? (Choose three.)

A. FortiSIEM

B. FortiManager

C. FortiAnalyzer

D. FortiGate

E. FortiNAC

Suggested Answer: *ADE*

Community vote distribution

ADE (100%)

ali_red 8 months ago

Selected Answer: ADE

Page 17 study guide

upvoted 1 times

Question #21 *Topic 1*

An OT architect has deployed a Layer 2 switch in the OT network at Level 1 in 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.

Which statement about the traffic between PLC1 and PLC2 is true?

A. In order to communicate, PLC1 must be in the same VLAN as PLC2.

B. The Layer 2 switch 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. The Layer 2 switch rewrites VLAN tags before sending traffic to the FortiGate device.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which statement is correct about processing matched rogue devices by FortiNAC?

A. FortiNAC cannot revalidate matched devices.

B. FortiNAC remembers the matching rule of the rogue device.

C. FortiNAC disables matching rule of previously-profiled rogue devices.

D. FortiNAC matches the rogue device with only one device profiling rule.

Suggested Answer: *B*

Community vote distribution

B (100%)

datomb74 5 months, 1 week ago

Selected Answer: B

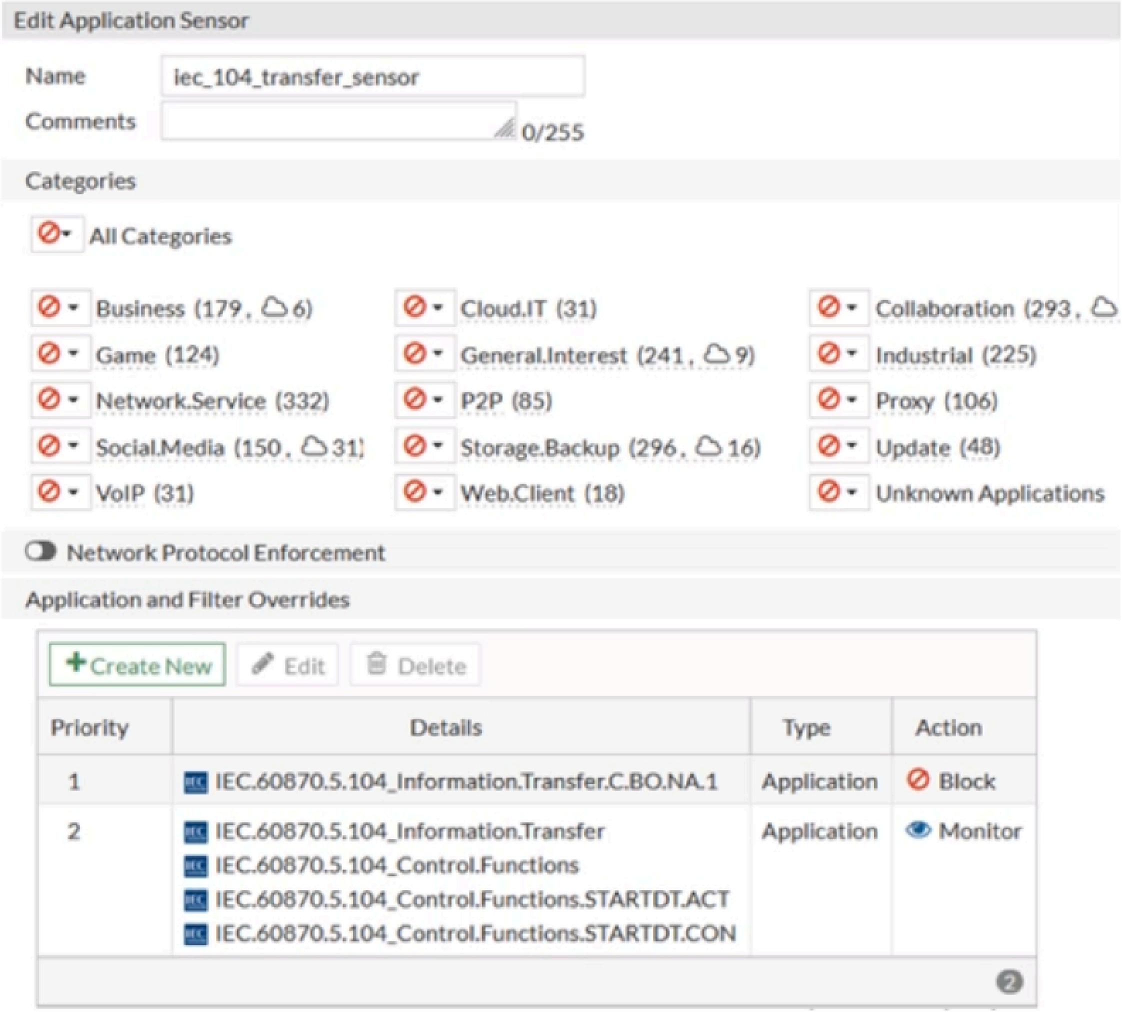
Studyguide P66

upvoted 1 times

Question #23

Topic 1

Refer to the exhibits.



Edit Application Sensor

Name	iec_104_transfer_sensor
Comments	0/255

Categories

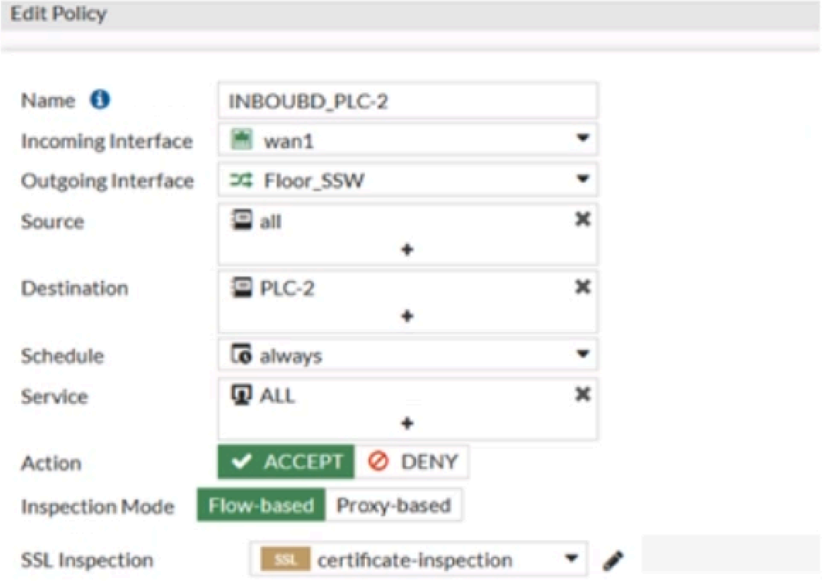
⊘ All Categories

⊘ Business (179, ☁6)	⊘ Cloud.IT (31)	⊘ Collaboration (293, ☁
⊘ Game (124)	⊘ General.Interest (241, ☁9)	⊘ Industrial (225)
⊘ Network.Service (332)	⊘ P2P (85)	⊘ Proxy (106)
⊘ Social.Media (150, ☁31)	⊘ Storage.Backup (296, ☁16)	⊘ Update (48)
⊘ VoIP (31)	⊘ Web.Client (18)	⊘ Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	IEC.60870.5.104_Information.Transfer.C.BO.NA.1	Application	⊘ Block
2	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



Edit Policy

Name	INBOUBD_PLC-2
Incoming Interface	wan1
Outgoing Interface	Floor_SSW
Source	all
Destination	PLC-2
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY
Inspection Mode	Flow-based Proxy-based
SSL Inspection	SSL certificate-inspection

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. SSL inspection must be set to deep-inspection to correctly apply application control.

D. IEC 104 signatures are all allowed except the C.BO.NA.1 signature.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Which two advantages does FortiNAC provide in the OT network? (Choose two.)

A. It can be used for device profiling.

B. It can be used for industrial intrusion detection and prevention.

C. It can be used for IoT device detection.

D. It can be used for network micro-segmentation.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Which statement about the IEC 104 protocol is true?

A. IEC 104 is used for telecontrol SCADA in electrical engineering applications.

B. IEC 104 is IEC 101 compliant in old SCADA systems.

C. IEC 104 protects data transmission between OT devices and services.

D. IEC 104 uses non-TCP/IP standards.

Suggested Answer: *A*

Community vote distribution

A (100%)

L_U_P_I_N 5 months, 2 weeks ago

Selected Answer: A

Study guide page 181

upvoted 1 times

ali_red 8 months ago

Selected Answer: A

page 181 study guide

upvoted 1 times

Question #26 Topic 1

A FortiGate device is newly deployed as the edge gateway of an OT network security fabric. The downstream FortiGate devices are also newly deployed as Security Fabric leafs to protect the control area zone.
With no additional essential networking devices, and to implement micro-segmentation on this OT network, what configuration must the OT network architect apply to control intra-VLAN traffic?

A. Enable transparent mode on the edge FortiGate device.

B. Enable security profiles on all interfaces connected in the control area zone.

C. Set up VPN tunnels between downstream and edge FortiGate devices.

D. Create a software switch on each downstream FortiGate device.

Suggested Answer: *D*

Community vote distribution

D (100%)

ali_red 8 months ago

Selected Answer: D

page 144 study guide

upvoted 2 times

Question #27 *Topic 1*

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. FortiSOAR and FortiSIEM

C. A syslog server and FortiSIEM

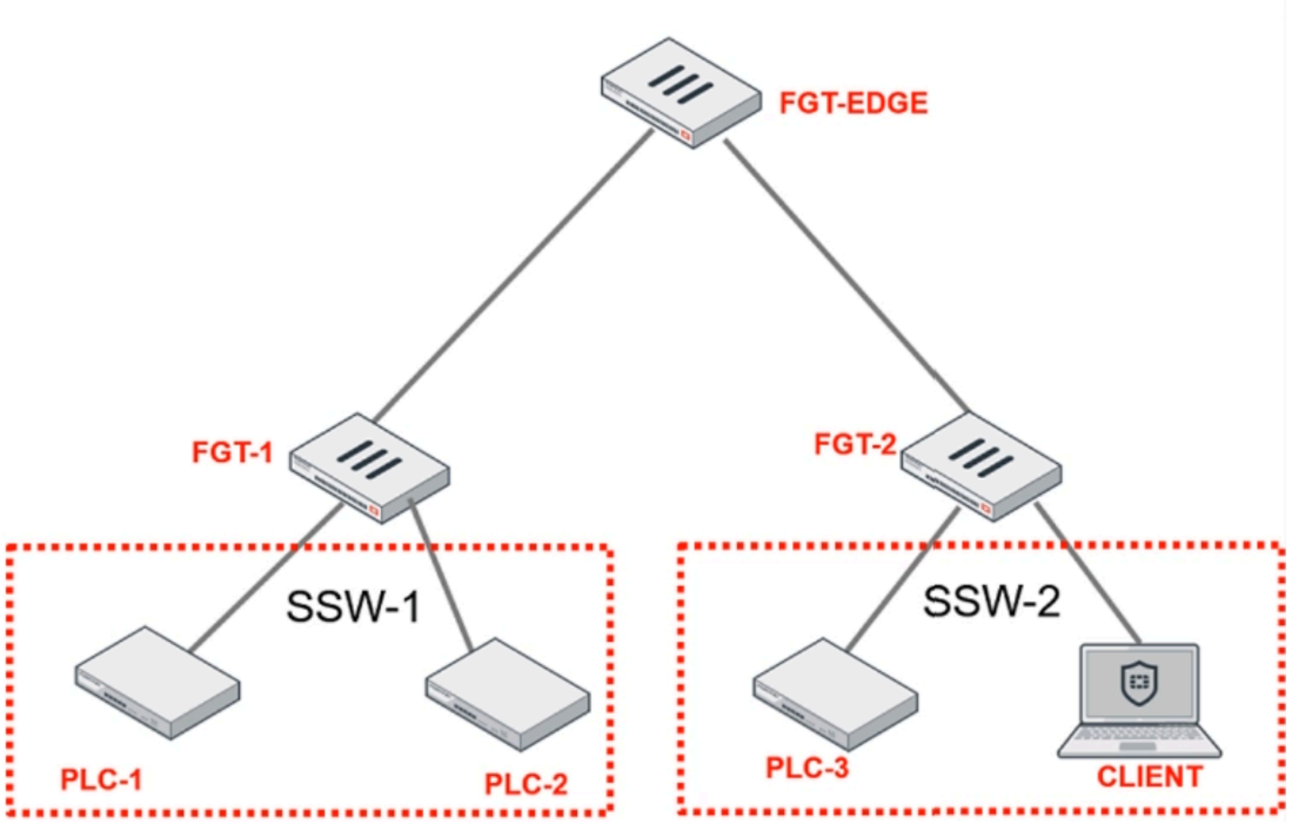
D. FortiSandbox and FortiSIEM

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #28 Topic 1

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 cannot send traffic to each other.

Which two statements about the traffic between PCL-1 and PLC-2 are true? (Choose two.)

A. The switch on FGT-2 must be hardware to implement micro-segmentation.

B. Micro-segmentation on FGT-2 prevents direct device-to-device communication.

C. Traffic must be inspected by FGT-EDGE in OT networks.

D. FGT-2 controls intra-VLAN traffic through firewall policies.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

ali_red 8 months ago

Selected Answer: BD

page 149 study guide

upvoted 1 times

Question #29 *Topic 1*

Which two frameworks are common to secure ICS industrial processes, including SCADA and DCS? (Choose two.)

A. Modbus

B. NIST Cybersecurity

C. IEC 104

D. IEC 62443

Suggested Answer: *BD*

Community vote distribution

BD (100%)

datomb74 5 months, 1 week ago

Selected Answer: BD

Study Guide P25

upvoted 1 times

Question #30 *Topic 1*

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 protocols from PLCs.

Which security sensor must you implement to detect protocols on the OT network?

A. Application control (AC)

B. Endpoint Detection and Response (EDR)

C. Deep packet inspection (DPI)

D. Intrusion prevention system (IPS)

Suggested Answer: *A*

Community vote distribution

A (80%) D (20%)

hem82 3 weeks, 1 day ago

Selected Answer: A

Page 192. It mentions application detection not exploits

upvoted 1 times

fb66ad3 4 months, 2 weeks ago

Selected Answer: A

Page 192 of the study guide. Application control is tied to protocol detection.

upvoted 3 times

79ba84e 4 months, 3 weeks ago

Selected Answer: D

Page 187 of the study guide

upvoted 1 times