Fortinet

NSE7_OTS-6.4 Exam

Fortinet NSE 7 - OT Security 6.4

Questions & Answers
Demo

Version: 4.0

Question: 1

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

A. Enhanced point of connection details
B. Direct VLAN assignment
C. Adapter consolidation for multi-adapter hosts
D. Importation and classification of hosts

Answer: A, B

Explanation:

Question: 2

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: A, B, D

Explanation:

Question: 3

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: A

Explanation:

Question: 4

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

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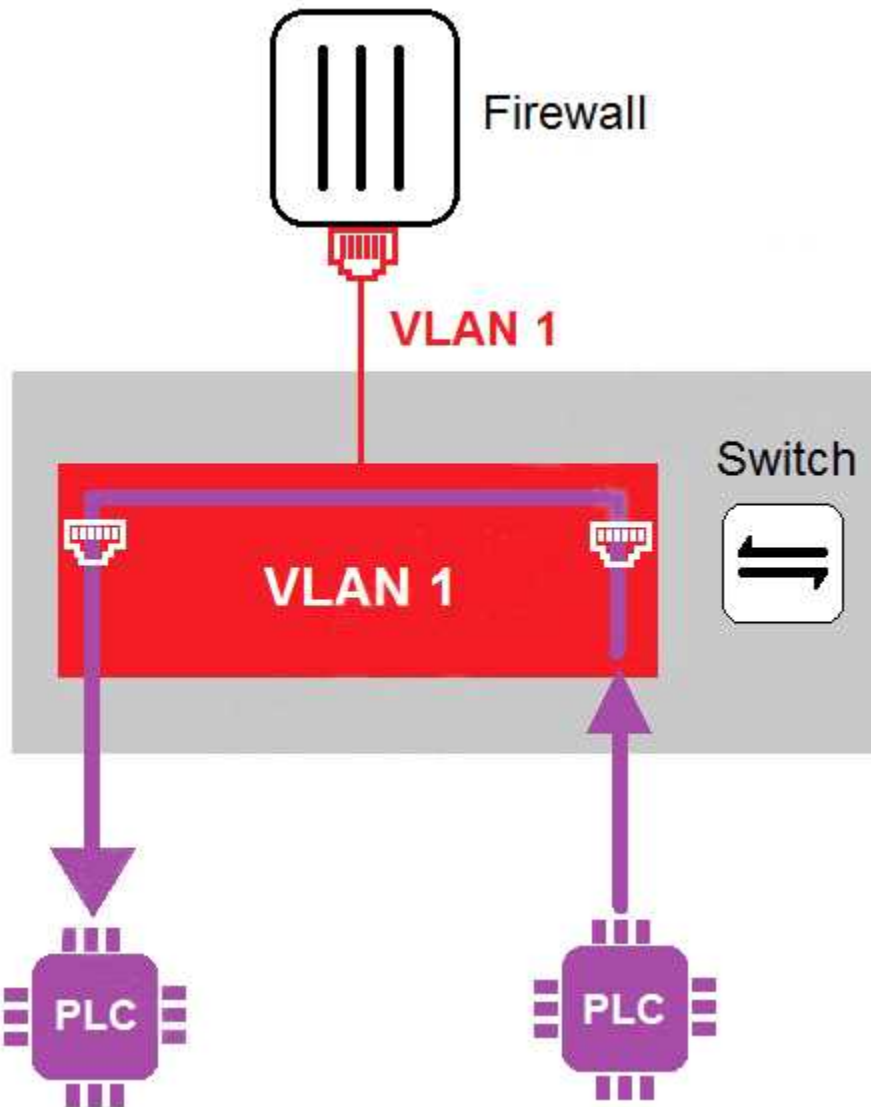C. FortiAnalyzer
D. FortiSIEM
E. FortiGate

Answer: A, C, D

Explanation:

Question: 5

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

Explanation: