PassQueen
a.k.a dumpsqueen.com

Implementing Cisco Connected Physical Security 2 Exam

Cisco 648-247

Version Demo

Total Demo Questions: 7

Total Premium Questions: 77

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Cisco Physical Access Control	77
Total	77

QUESTION NO: 1

Which two design practices help protect Cisco Physical Access Control Gateway traffic on a converged network? (Choose two.)

A. Place physical-access devices in a dedicated VLAN.

B. Apply ACL or firewall policy to restrict inter-VLAN communications.

C. Connect Cisco Access Gateways to the same unrestricted VLAN as user workstations.

D. Disable NTP to reduce physical-access network traffic.

E. Allow unrestricted management access from every user subnet.

ANSWER: A B

Explanation:

Placing physical-access devices in a dedicated VLAN provides Layer 2 separation from normal user traffic. Restricting routed traffic with ACLs or firewall policy provides a controlled Layer 3 boundary so that gateways can communicate only with required systems, such as Cisco PAM, NTP, DNS when used, and approved management workstations.

Connecting a gateway to an unrestricted user VLAN removes the intended traffic separation. Disabling time synchronization also reduces the reliability of event correlation and can affect secure communications and troubleshooting.

QUESTION NO: 2

Refer to the exhibit.

One or more expansion modules is connected to the Cisco Access Gateway via a CAN bus. How should the CAN bus wires be connected after the last module in the chain?

A. The CAN bus wires should be looped back to the Cisco Access Gateway.

B. The CAN bus wires should be twisted together and tucked away.

C. The CAN bus wires should be plugged into a Layer 2 Ethernet switch.

D. The CAN bus wires should be terminated with a high-impedance resistor.

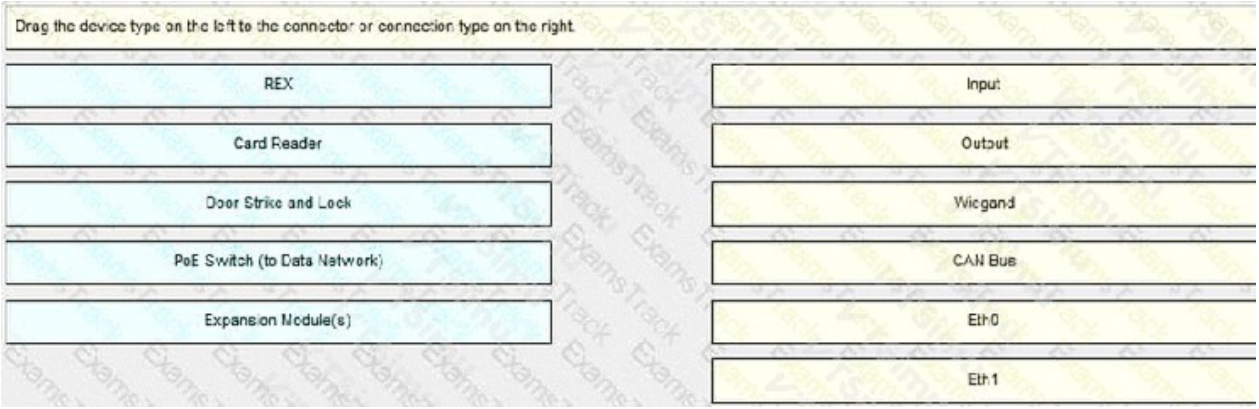
E. The CAN bus wires should be terminated with a 120-ohm resistor.

ANSWER: E

Explanation:

The CAN bus wires should be terminated with a 120-ohm resistor. A CAN network is a linear differential bus, and proper end-of-line termination is required at the physical ends of the bus to match the cable's characteristic impedance. In a Cisco Access Gateway installation with expansion modules connected in a daisy chain, the final module is the far physical end of that CAN segment. Installing a 120-ohm terminating resistor across the CAN High and CAN Low conductors at that point prevents signal reflections, preserves differential-signal integrity, and supports reliable communication between the gateway and all attached expansion modules. This termination is especially important as cable length and the number of connected modules increase, because reflected signals can otherwise distort CAN frames and cause communication errors. CAN physical-layer guidance specifies 120-ohm termination at each end of a high-speed CAN bus; one termination is normally present at or near the gateway side, while the other is fitted at the last module in the chain. See the CAN in Automation physical-layer overview and Cisco's Cisco Access Gateway Installation Guide.

QUESTION NO: 3 - (SIMULATION)



ANSWER: See the explanation for the answer

Explanation:

Make the following device-to-connection assignments:

Eth1 is not used for these listed device connections.

The REX is a dry-contact input, the strike/lock is controlled by an output relay, and a conventional card reader uses the Wiegand interface. Expansion modules communicate over the CAN bus, while the upstream data-network PoE switch connects to Ethernet 0.

QUESTION NO: 4

Which two statements are true regarding Cisco Physical Access Control Gateway field-device connectivity? (Choose two.)

A. Wiegand-compatible readers can be connected to the gateway or Reader Module.

B. The gateway provides a total of 650 mA for supported connected field devices.

C. Only Cisco-branded readers are supported.

D. The Eth1 port supplies PoE to locks and readers.

E. Cisco supplies the locks and door hardware used with the gateway.

ANSWER: A B

Explanation:

Cisco Physical Access Control Gateways and Reader Modules support Wiegand-compatible readers, allowing compatible third-party reader hardware to communicate credential data to the access-control system. The gateway also provides a total of 650 mA of available power for supported readers, locks, and other connected field devices, subject to the design power budget. Cisco does not manufacture readers and locks, and the Eth1 interface is not used to pass PoE to field devices. See the Cisco Physical Access Gateway data sheet.

QUESTION NO: 5

A gateway is reporting unstable or flapping connectivity. INPUT 1 is rapidly flapping between "up" and "down." What is the most likely cause?

A. The input is configured as supervised, when it should be unsupervised.

B. The wires are dirty or improperly seated in the termination block.

C. The gateway is defective and should be RMA.

D. The input on the gateway is configured as supervised, and the wires could be dirty or improperly seated in the termination block.

ANSWER: D

Explanation:

The input on the gateway is configured as supervised, and the wires could be dirty or improperly seated in the termination block. This is the most likely cause because a supervised physical-access input continuously monitors the electrical state of its field circuit, not merely whether a contact appears open or closed. The gateway expects the circuit's specified end-of-line resistance values and stable terminal connections. A loose conductor, contamination on a terminal, a marginal crimp, or an incompletely seated wire can intermittently alter resistance or interrupt continuity. The supervision logic then repeatedly interprets the changing electrical condition as alternating normal and fault states, producing rapid up/down flapping. This behavior is especially characteristic when the input mode is set to supervised, because minor connection instability is detected and reported rather than being masked as a simple contact-state change. Checking that the configured supervision mode matches the installed field wiring, then inspecting, cleaning, and firmly reseating the termination-block conductors, is the appropriate first troubleshooting action. Cisco's Physical Access Gateway support resources and product documentation describe gateway input wiring and configuration considerations: Cisco Physical Access Gateway support and Cisco Physical Access Gateway product information.

QUESTION NO: 6 - (DRAG DROP)

Select & Place:

ANSWER:

Explanation:

Creating a new door in Cisco Physical Access Manager follows the dependency flow of the physical-security configuration model. First, create the location. A location provides the organizational and physical context in which the door is defined, such as a site, building, floor, or other placement in the access-control hierarchy. Establishing that context first keeps the later door configuration attached to the correct part of the deployment.

Next, create the door template. The template defines the reusable door behavior and configuration characteristics that will be applied when a logical door is created. Templates allow consistent configuration across doors that share operational requirements, which is especially useful when an installation contains multiple similar entry points.

After both the location and template exist, create the logical door. The logical door is the PAM representation of the controlled opening. It combines the door's placement with the template-based configuration, making it the appropriate object to receive the hardware association. Cisco physical-access designs use logical representations to separate the administrative door definition from the controller-connected hardware.

Finally, associate devices to the logical door. At this point, the logical object already exists and can be linked to the applicable access-control hardware, such as the controller interface and door-related devices. This completes the relationship between the configured door definition and the physical equipment that operates it. This sequencing reflects the configuration approach described in Cisco's physical-security documentation and product resources, including the Cisco Physical Security product information and the Cisco Physical Access Manager support documentation.

QUESTION NO: 7

How many licenses are included with Cisco PAM, and how are licenses allocated?

A. Cisco PAM does not come with any licenses. Licenses are allocated for every logical door.

B. Cisco PAM comes with 1 license. It is allocated for the admin user.

C. Cisco PAM comes with 32 licenses. Each module requires 1 license.

D. Cisco PAM comes with 64 licenses. Only gateways require licenses.

ANSWER: C

Explanation:

Cisco PAM comes with 32 licenses. Each module requires 1 license. This describes the base licensing model for Cisco Physical Access Manager: the system includes a pool of 32 licenses, and capacity is consumed on a one-license-per-module basis. In practical deployment planning, an administrator inventories the access-control modules to be managed and ensures that the available license count covers the required module count. This model makes the license requirement directly proportional to the physical access-control infrastructure being added to the Cisco PAM deployment, rather than being based on an administrator account or a gateway alone. The included 32-license entitlement therefore provides an initial supported capacity without requiring a separate license allocation for each individual user account. Cisco's Physical Access Manager documentation and installation resources describe the product's deployment architecture and licensing-related planning requirements; see the Cisco Physical Access Manager installation guides and Cisco's Physical Access Manager product information. When sizing a system, count modules first, then verify that the 32 included licenses, plus any additional entitlement if needed, meet that count.