Chapter 25: Quiz – Secure Network Access Control (Answers) CCNPv8 ENCOR

itexamanswers.net/chapter-25-quiz-secure-network-access-control-answers-ccnpv8-encor.html

January 11, 2021

1. Which Cisco security architectural framework helps design secure solutions for the various places in the network (PINs)?

- **Cisco SAFE**
- Cisco DNA
- Cisco ENFV
- Cisco NGFW

Explanation: Cisco developed the Cisco SAFE security architecture to help design secure solutions for various places in the network (PINs) such as: the branch, campus, data center, edge, cloud, and WAN.

2. Which Cisco SAFE secure domain is concerned with the technologies involving access control, VPNs, and encryption?

- **secure services**
- security intelligence
- threat defense
- compliance

Explanation: Secure services is a Cisco SAFE security architectural framework concept primarily concerned with the technologies that include access control, VPNs, and encryption.

3. Which component in the AMP architecture makes the intelligent decisions on whether a file is clean, malicious, or unknown?

- **AMP Cloud**
- Cisco Talos
- AMP Connector
- Cisco Threat Grid

Explanation: There are three major components in the AMP architecture: AMP Cloud, AMP Connector, and threat intelligence from Cisco Talos and Cisco Threat Grid. The AMP Cloud is the most important component of the architecture, making intelligent decisions in real time to identify malware.

4. According to Gartner, Inc., what are three IPS functions that should be included in a next-generation IPS? (Choose three.)

- **real-time contextual awareness**
- **advanced threat protection**
- **intelligent security automation**
- application-level inspection
- stateful firewall protection
- advanced malware protection

Explanation: In addition to IPS functions, Gartner, Inc. states a next-generation IPS should include following capabilities:

- Real-time contextual awareness
- Advanced threat protection
- Intelligent security automation
- Unparalleled performance and scalability
- Application visibility and control (AVC) and URL filtering

5. Which security service is provided by 802.1x?

- **port-based network access control**
- malware analysis and protection across the full attack continuum
- malware analysis of files
- protection against emerging threats for Cisco products

Explanation: 802.1x is an industry standard for providing port-based network access control. It provides a mechanism to authenticate devices onto the local-area networks and WLANs.

6. Which three security concepts in the Cisco SAFE framework are used to evaluate each PIN? (Choose three.)

- **compliance**
- **threat defense**
- **segmentation**
- threat grid
- malware protection
- intrusion prevention

Explanation: The Cisco SAFE framework identifies six security concepts to evaluate PINs.

- Management
- Security intelligence
- Compliance
- Segmentation
- Threat defense

- Secure services

7. Which component of the Cisco SAFE framework consists of a team of security experts who develop threat intelligence that protects against threats for Cisco products?

- **Cisco Talos**
- Cisco Umbrella
- Cisco Stealthwatch
- Cisco ISE

Explanation: Cisco Talos is a threat intelligence organization made up of a team of security experts who create intelligence that detects, analyzes, and protects against both known and emerging threats for Cisco products.

8. What is a solution for identifying malware through file analysis performed in a controlled and monitored sandbox environment?

- **Cisco Threat Grid**
- Cisco Umbrella
- Cisco Stealthwatch
- Cisco ISE

Explanation: Cisco Threat Grid performs file analysis in a controlled and monitored sandbox environment to observe and analyze the behavior against millions of samples to determine whether a file is malware.

9. Which security function is provided by a firewall?

- **allows or blocks trafic by performing packet filtering and stateful inspection**
- passively monitors network traffic and logs intrusion attacks for security analysis
- passively monitors network traffic and automatically blocks intrusion attacks
- aggregates and correlates threat events, contextual information, and network device performance data

Explanation: A firewall monitors incoming and outgoing network traffic and allows or blocks traffic based on filtering and stateful inspection of packets.

10. What is the default timeout period for initiation of 802.1x authentication before the authenticator with MAB enabled proceeds with MAC authentication bypass?

- 30 seconds
- **90 seconds**

- 120 seconds
- 180 seconds

Explanation: The MAB authentication process is initiated by the authenticator by sending an EAPoL identity request message to the endpoint every 30 seconds to determine if it has a supplicant. After three timeouts (90 seconds) the authenticator proceeds to authenticate via MAB.

11. Which two Cisco solutions are used by Cisco Web Security Appliance for real-time threat intelligence to protect against the latest threats? (Choose two.)

- **Cisco Talos**
- **Cisco AMP**
- Cisco Umbrella
- Cisco ISE
- Cisco Threat Grid

Explanation: Cisco Web Security Appliance (WSA) is a web gateway that offers a wide range of security protection. It makes use of Cisco AMP and Cisco Talos for real-time intelligence so that it can stay ahead of the evolving threat landscape and protect against the latest exploits.

12. Which place in the network (PIN) typically contains the critical information assets and intellectual property of an organization?

- **data center**
- edge
- branch
- WAN

Explanation: Data centers house the servers containing the critical information assets and intellectual property of an organization.

13. Which three threat protection capabilities are provided by Cisco ESA? (Choose three.)

- **spam protection**
- **forged email detection**
- **phishing protection**
- cloud access security
- Layer 4 traffic monitoring
- web filtering

Explanation: Email is a top attack vector for security breaches. Cisco Email Security Appliance (ESA) includes many threat protection capabilities for email, including protection against spam, forged email, and advanced phishing.