

What is the function of Cisco Cloudlock for data security?

- A. data loss prevention
- B. controls malicious cloud apps
- C. detects anomalies
- D. user and entity behavior analytics

Correct Answer: A

QUESTION 20

When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

- A. Application Control
- B. Security Category Blocking
- C. Content Category Blocking
- D. File Analysis

Correct Answer: B

QUESTION 21

Which two activities can be done using Cisco DNA Center? (Choose two.)

- A. DHCP
- B. design
- C. accounting
- D. DNS
- E. provision

Correct Answer: BE

QUESTION 22

Where are individual sites specified to be blacklisted in Cisco Umbrella?

- A. application settings
- B. content categories
- C. security settings
- D. destination lists

Correct Answer: D

QUESTION 23

Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

- A. transparent
- B. redirection
- C. forward
- D. proxy gateway

Correct Answer: A

QUESTION 24

What is the primary role of the Cisco Email Security Appliance?

- A. Mail Submission Agent
- B. Mail Transfer Agent
- C. Mail Delivery Agent
- D. Mail User Agent

Correct Answer: B

QUESTION 25

How does Cisco Umbrella archive logs to an enterprise-owned storage?

- A. by using the Application Programming Interface to fetch the logs
- B. by sending logs via syslog to an on-premises or cloud-based syslog server
- C. by the system administrator downloading the logs from the Cisco Umbrella web portal
- D. by being configured to send logs to a self-managed AWS S3 bucket

Correct Answer: D

QUESTION 26

What are two list types within AMP for Endpoints Outbreak Control? (Choose two.)

- A. blocked ports
- B. simple custom detections
- C. command and control
- D. allowed applications
- E. URL

Correct Answer: BD

QUESTION 27

Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?

- A. group policy
- B. access control policy
- C. device management policy
- D. platform service policy

Correct Answer: D

QUESTION 28

On which part of the IT environment does DevSecOps focus?

- A. application development
- B. wireless network
- C. data center
- D. perimeter network

Correct Answer: A

QUESTION 29

How does Cisco Stealthwatch Cloud provide security for cloud environments?

- A. It delivers visibility and threat detection.
- B. It prevents exfiltration of sensitive data.
- C. It assigns Internet-based DNS protection for clients and servers.
- D. It facilitates secure connectivity between public and private networks.

Correct Answer: A

QUESTION 30

Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

- A. File Analysis
- B. SafeSearch
- C. SSL Decryption
- D. Destination Lists

Correct Answer: C

QUESTION 31

Which two preventive measures are used to control cross-site scripting? (Choose two.)

- A. Enable client-side scripts on a per-domain basis.
- B. Incorporate contextual output encoding/escaping.
- C. Disable cookie inspection in the HTML inspection engine.
- D. Run untrusted HTML input through an HTML sanitization engine.
- E. SameSite cookie attribute should not be used.

Correct Answer: AB

QUESTION 32

DRAG DROP

Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.

PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

Correct Answer:

PortScan Detection	Distributed PortScan
Port Sweep	Decoy PortScan
Decoy PortScan	Port Sweep
Distributed PortScan	PortScan Detection

QUESTION 33

An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?

- A. SAT
- B. BAT
- C. HAT
- D. RAT

Correct Answer: D

QUESTION 34

Which information is required when adding a device to Firepower Management Center?

- A. username and password
- B. encryption method
- C. device serial number
- D. registration key

Correct Answer: D

QUESTION 35

Refer to the exhibit. Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

Interface	MAC Address	Method	Domain	Status	Fg Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth	0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth	0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth	0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth	0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth	0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth	0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth	0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth	0A02198200000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth	0A02198200001
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth	0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth	0A02198200000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth	0A02198200000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth	0A02198200001
Gi7/4	54ee.75db.d766	dot1x	DATA	Auth	0A02198200001
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth	0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth	0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth	0A02198200000

- A. show authentication registrations
- B. show authentication method
- C. show dot1x all
- D. show authentication sessions

Correct Answer: B

QUESTION 36

Which technology is used to improve web traffic performance by proxy caching?

- A. WSA
- B. Firepower
- C. FireSIGHT
- D. ASA

Correct Answer: A

QUESTION 37

The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

- A. SDN controller and the cloud
- B. management console and the SDN controller
- C. management console and the cloud
- D. SDN controller and the management solution

Correct Answer: D

QUESTION 38

Which technology must be used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

- A. DMVPN
- B. FlexVPN