**QUESTION 119**
Which statement describes a traffic profile on a Cisco Next Generation Intrusion Prevention System?

A. It allows traffic if it does not meet the profile.
B. It defines a traffic baseline for traffic anomaly deduction.
C. It inspects hosts that meet the profile with more intrusion rules.
D. It blocks traffic if it does not meet the profile.

**Answer:** B

**QUESTION 120**
Which two are valid suppression types on a Cisco Next Generation Intrusion Prevention System?

A. Port
B. Rule
C. Source
D. Application
E. Protocol

**Answer:** BC

**QUESTION 121**
Which license is required for Cisco Security Intelligence to work on the Cisco Next Generation Intrusion Prevention System?

A. control
B. matware
C. URL filtering
D. protect

**Answer:** D

**QUESTION 122**
Which policy is used to capture host information on the Cisco Next Generation Intrusion Prevention System?

A. network discovery
B. correlation
C. intrusion
D. access control

**Answer:** A

**QUESTION 123**
On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed devices?

A. health policy
B. system policy
C. correlation policy
D. access control policy
E. health awareness policy

**Answer:** A

**QUESTION 124**
Which CLI command is used to register a Cisco FirePOWER sensor to Firepower Management Center?

A. configure system add <host><key>
B. configure manager <key> add host
C. configure manager delete
D. configure manager add <host><key>

**Answer:** D

**QUESTION 125**
Which Cisco AMP file disposition valid?

A. pristine
B. malware
C. dirty
D. nonmalicios

**Answer:** B

**QUESTION 126**
Which capability is exclusive to a Cisco AMP public cloud instance as compared to a private cloud instance?

A. RBAC
B. ETHOS detection engine
C. SPERO detection engine
D. TETRA detection engine

**Answer:** B

**QUESTION 127**
Which function is the primary function of Cisco AMP threat Grid?

A. automated email encryption
B. applying a real-time URI blacklist
C. automated malware analysis
D. monitoring network traffic

**Answer:** C

**QUESTION 128**

Which two characteristics of messenger protocols make data exfiltration difficult to detect and prevent? (Choose two.)

A. Malware infects the messenger application on the user endpoint to send company data.
B. Outgoing traffic is allowed so users can communicate with outside organizations.
C. An exposed API for the messaging platform is used to send large amounts of data.
D. Traffic is encrypted, which prevents visibility on firewalls and IPS systems.
E. Messenger applications cannot be segmented with standard network controls.

**Answer:** BE

**QUESTION 129**
How many interfaces per bridge group does an ASA bridge group deployment support?

A. up to 16
B. up to 8
C. up to 4
D. up to 2

**Answer:** B

**QUESTION 130**
Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?

A. It adds endpoints to identity groups dynamically.
B. It verifies that the endpoint has the latest Microsoft security patches installed.
C. It allows the endpoint to authenticate with 802.1xor MAB.
D. It allows CoA to be applied if the endpoint status is compliant.

**Answer:** C

**QUESTION 131**
What is a feature of the open platform capabilities of Cisco DNA Center?

A. domain integration
B. intent-based APIs
C. automation adapters
D. application adapters

**Answer:** B

**QUESTION 132**
Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?

A. process details variation
B. flow insight variation
C. interpacket variation
D. software package variation

**Answer:** C

**QUESTION 133**
In which two ways does a system administrator send web traffic transparently to the Web Security Appliance? (Choose two.)

A. configure policy-based routing on the network infrastructure
B. reference a Proxy Auto Config file
C. use Web Cache Communication Protocol
D. configure the proxy IP address in the web-browser settings
E. configure Active Directory Group Policies to push proxy settings

**Answer:** BC

**QUESTION 134**
Which form of attack is launched using botnets?

A. virus
B. EIDDOS
C. TCP flood
D. ODOS

**Answer:** B

**QUESTION 135**
How is DNS tunneling used to exfiltrate data out of a corporate network?

A. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.
B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.
C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network.
D. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.

**Answer:** B

**QUESTION 136**
Which Cisco security solution protects remote users against phishing attacks when they are not connected to the VPN?

A. Cisco Firepower
B. Cisco Umbrella
C. Cisco Stealthwatch
D. NGIPS

**Answer:** C

**QUESTION 137**
Which two tasks allow NetFlow on a Cisco ASA 5500 Series firewall? (Choose two.)

A. Create an ACL to allow UDP traffic on port 9996.
B. Enable NetFlow Version 9.
C. Create a class map to match interesting traffic.
D. Apply NetFlow Exporter to the outside interface in the inbound direction.
E. Define a NetFlow collector by using the flow-export command.

**Answer:** DE