Q1.

An engineer is implementing Cisco CES in an existing Microsoft Office 365 environment and must route inbound email to Cisco CES addresses Which DNS record must be modified to accomplish this task?

A. MX
B. SPF
C. CNAME
D. DKIM

Q2.

Which component of Cisco Umbrella architecture increases reliability of the service?

A. anycast IP
B. AMP Threat Grid
C. BGP route reflector
D. Cisco Tales

Q3.

Which feature is leveraged by advanced antimalware capabilities to be an effective endpoint protection platform?

A. storm centers
B. big data
C. sandboxing
D. blocklisting

Q4.

An engineer is adding a Cisco DUO solution to the current TACACS+ deployment using Cisco ISE The engineer wants to authenticate users using their account when they log into network devices Which action accomplishes this task?

A. Create an identity policy within Cisco ISE to send all authentication requests to Cisco DUO
B. Modify the current policy with the condition MFA: Source Sequence DUO=true in the authorization conditions within Cisco ISE
C. Configure Cisco DUO with the external Active Directory connector and tie it to the policy set within Cisco ISE.
D. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE.

Q5.

An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices The default management port conflicts with other communications on the network and must be changed. What must be done to ensure that all devices can communicate together?

A. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices.
B. Set the sftunnel port to 8305
C. Manually change the management port on Cisco FMC and all managed Cisco FTD devices
D. Set the sftunnel to go through the Cisco FTD

Q6.

What are two characteristics of Cisco DNA Center APIs? (Choose two.)

A. They quickly provision new devices
B. They are Cisco proprietary
C. Postman is required to utilize Cisco DNA Center API calls.
D. They view the overall health of the network.
E. They do not support Python scripts

Q7.

Why is it important to have a patching strategy for endpoints?

A. so that patching strategies can assist with disabling nonsecure protocols in applications
B. so that known vulnerabilities are targeted and having a regular patch cycle reduces risks
C. to take advantage of new features released with patches
D. so that functionality is increased on a faster scale when it is used

Q8.

Cisco SensorBase gathers threat information from a variety of Cisco products and services and performs analytics to find patterns on threats. Which term describes this process?

A. consumption
B. authoring
C. sharing
D. Deployment

Q9.

```
import http.client
import base64
import ssl
import sys

host = sys.argv[1] # "10.10.10.240"
user = sys.argv[2] # "ersad"
password = sys.argv[3] # "Password1"

conn = http.client.HTTPSConnection("{}:9060".format(host),
context=ssl.SSLContext(ssl.PROTOCOL_TLSv1_2))

creds = str.encode(':'.join((user, password)))
encodedAuth = bytes.decode(base64.b64encode(creds))

headers = {
   'accept': "application/json",
   'authorization': " ".join(("Basic",encodedAuth)),
   'cache-control': "no-cache",
   }

conn.request("GET", "/ers/config/internaluser/", headers=headers)

res = conn.getresponse()
data = res.read()

print("Status: {}".format(res.status))
print("Header:\n{}".format(res.headers))
print("Body:\n{}".format(data.decode("utf-8")))
```

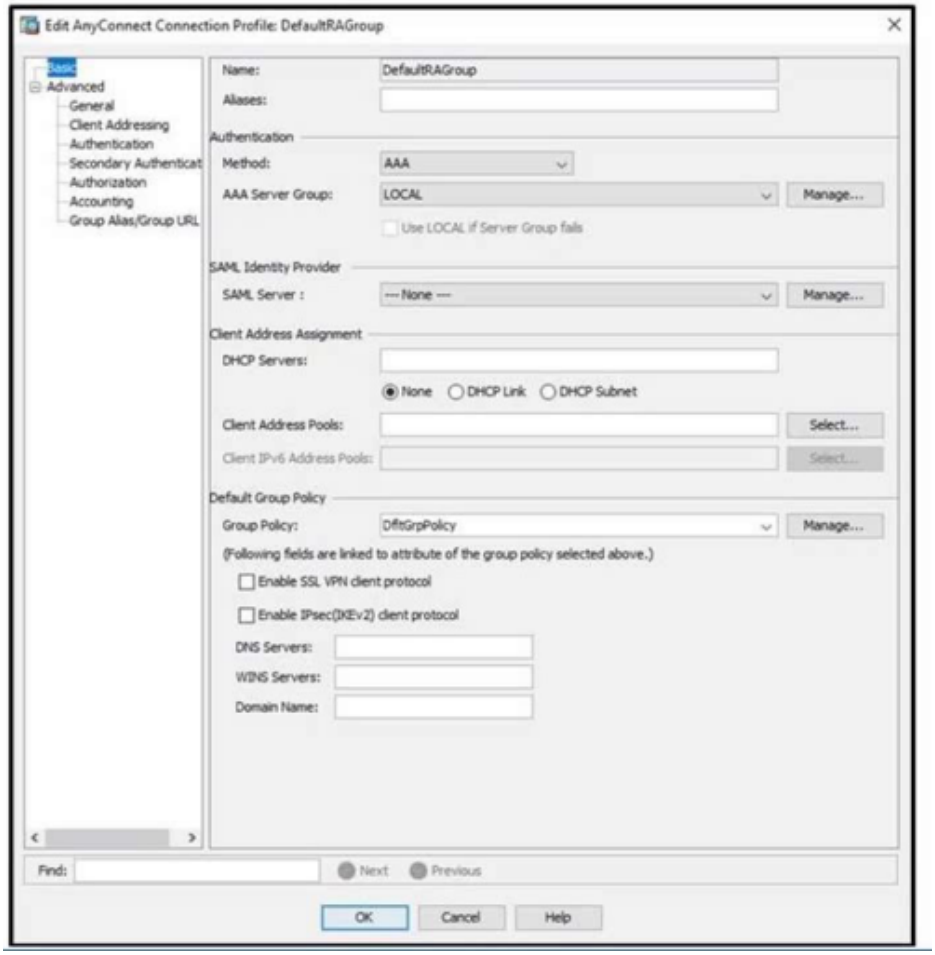
Refer to the exhibit What does this Python script accomplish?

A. It authenticates to a Cisco ISE with an SSH connection
B. It allows authentication with TLSv1 SSL protocol
C. It authenticates to a Cisco ISE server using the username of ersad
D. It lists the LDAP users from the external identity store configured on Cisco ISE.

Q10.

What is a description of microsegmentation?
A. Environments apply a zero-trust model and specify how applications on different servers or containers can communicate
B. Environments deploy centrally managed host-based firewall rules on each server or container
C. Environments implement private VLAN segmentation to group servers with similar applications
D. Environments deploy a container orchestration platform, such as Kubernetes. to manage the application delivery.

Q11.



Refer to the exhibit. When configuring a remote access VPN solution terminating on the Cisco ASA. an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication using machine certificates Which configuration item must be modified to allow this?

A. AAA Server Group
B. Group Policy
C. SAML Server
D. Method

Q12.

Which method of attack is used by a hacker to send malicious code through a web application to an unsuspecting user to request that the victim's web browser executes the code?

A. buffer overflow
B. browser WGET
C. cross-site scripting
D. SQL injection

Q13.

```
crypto ikev2 name-mangler MANGLER
 dn organization-unit
```

Refer to the exhibit An engineer is implementing a certificate based VPN What is the result of the existing configuration?

A. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.
B. Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully
C. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER.
D. The OU of the IKEv2 peer certificate is set to MANGLER

Q14.

What is a commonality between DMVPN and FlexVPN technologies?
A. IOS routers run the same NHRP code for DMVPN and FlexVPN.
B. FlexVPN and DMVPN use the same hashing algorithms
C. FlexVPN and DMVPN use IS-IS routing protocol to communicate with spokes
D. FlexVPN and DMVPN use the new key management protocol, IKEv2.

Q15.

An organization wants to improve its cybersecurity processes and to add intelligence to its data. The organization wants to utilize the most current intelligence data for URL filtering. reputations, and vulnerability information that can be integrated with the Cisco FTD and Cisco WSA What must be done to accomplish these objectives?
A. Download the threat intelligence feed from the IETF and import it into the Cisco FTD and Cisco WSA databases
B. Configure the integrations with Talos Intelligence to take advantage of the threat intelligence that it provides.
C. Create a Cisco pxGrid connection to NIST to import this information into the security products for policy use
D. Create an automated download of the Internet Storm Center intelligence feed into the Cisco FTD and Cisco WSA databases to tie to the dynamic access control policies

Q16.

A customer has various external HTTP resources available including Intranet Extranet, and Internet, with a proxy configuration running in explicit mode. Which method allows the client desktop browsers to be configured to select when to connect direct or when to use the proxy?

A. Transparent mode
B. PAC file
C. Forward file
D. Bridge mode

Q17.

What is an advantage of network telemetry over SNMP pulls?

A. scalability
B. encapsulation
C. accuracy
D. security

Q18.

A company discovered an attack propagating through their network via a file. A custom file detection policy was created in order to track this in the future and ensure no other endpoints execute the infected file. In addition, it was discovered during testing that the scans are not detecting the file as an indicator of compromise. What must be done in order to ensure that the policy created is functioning as it should?

A. Block the application that the file was using to open.
B. Create an IP block list for the website from which the file was downloaded.
C. Send the file to Cisco Threat Grid for dynamic analysis.
D. Upload the hash for the file into the policy

Q19.

An organization wants to use Cisco FTD or Cisco ASA devices Specific URLs must be blocked from being accessed via the firewall, which requires that the administrator input the bad URL categories that the organization wants blocked into the access policy. Which solution should be used to meet this requirement?

A. Cisco FTD because it includes URL filtering in the access control policy capabilities, whereas Cisco ASA does not.
B. Cisco ASA because it includes URL filtering in the access control policy capabilities, whereas Cisco FTD does not
C. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not

D. Cisco ASA because it enables URL filtering and blocks malicious URLs by default whereas Cisco FTD does not

Q20.

An administrator configures new authorization policies within Cisco ISE and has difficulty profiling the devices Attributes for the new Cisco IP phones that are profiled based on the RADIUS authentication are seen; however, the attributes for CDP or DHCP are not. What should the administrator do to address this issue?

A. Configure a service template within the switch to standardize the port configurations so that the correct information is sent to Cisco ISE
B. Configure the authentication port-control auto feature within Cisco ISE to identify the devices that are trying to connect
C. Configure the device sensor feature within the switch to send the appropriate protocol information
D. Configure the ip dhcp snooping trust command on the DHCP interfaces to get the information to Cisco ISE

Q21.

Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?

A. Lambda
B. Docker
C. SDLC
D. Contiv

Q22.

What does Cisco AMP for Endpoints use to help an organization detect different families of malware"?

A. Ethos Engine to perform fuzzy fingerprinting
B. Tetra Engine to detect malware when the endpoint is connected to the cloud
C. Spero Engine with machine learning to perform dynamic analysis
D. ClamAV Engine to perform email scanning

Q23.

An engineer is implementing NTP authentication within the network and has configured the client and server devices with the command ntp authentication-key 1 md5 Cisc409674397.The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however is unable to do so Which command is required to resolve this issue?

A. ntp peer 1.1.1.1 key 1

B. ntp server 1.1.1.2 key 1 correct

ntp peer 1.1.1.2 key 1

D. ntp server 1.1.1.1 key 1

Q24.

An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA Which Cisco ASA command must be used?

A. flow-export destination inside 1.1.1.1 2055
B. flow exporter <name>
C. ip flow monitor<name> input
D. ip flow-export destination 1.1.1.1 2055

Q25.

A Cisco FTD engineer is creating a new IKEv2 policy called s2s00409674397 to allow for additional protocols to terminate network devices. They currently only have one policy established and need the new policy to be a backup in case some devices cannot support the stronger algorithms listed in the primary policy. Which action will accomplish this goal?

A. Change the encryption to AES* to support all AES algorithms in the primary policy.
B. Make the priority for the primary policy 10 and the new policy 1
C. Change the integrity algorithms to SHA* to support all SHA algorithms in the primary policy.
D. Make the priority for the new policy 5 and the primary policy 1.

Q26.

What is a functional difference between a Cisco ASA and a Cisco IOS router with Zone-Based Policy Firewall?

A. The Cisco ASA denies all traffic by default, whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces
B. The Cisco IOS router with Zone-Based Policy Firewall can be configured for high availability whereas the Cisco ASA cannot.
C. The Cisco ASA can be configured for high availability, whereas the Cisco IOS router with Zone-Based Policy Firewall cannot.

D. The Cisco IOS router with Zone-Based Policy Firewall denies all traffic by default, whereas the Cisco ASA starts out by allowing all traffic until rules are added.

Q27.

An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation What must be understood before choosing a solution?

A. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701.
B. GRE over IPsec cannot be used as a standalone protocol, and L2TP can
C. L2TP is an IP packet encapsulation protocol, and GRE over IPsec is a tunneling protocol
D. GRE over IPsec adds its own header, and L2TP does not.

Q28.

Which posture assessment requirement provides options to the client for remediation and requires the remediation within a certain timeframe?

A. optional
B. visibility
C. audit
D. Mandatory

Q29.

How does Cisco Workload Optimization Manager help mitigate application performance issues?

A. It deploys an AWS Lambda system
B. It sets up a workload forensic score
C. It optimizes a flow path
D. It automates resource resizing.

Q30.

What is a benefit of conducting device compliance checks?

A. It validates if anti-virus software is installed
B. It scans endpoints to determine if malicious activity is taking place
C. It indicates what type of operating system is connecting to the network.
D. It detects email phishing attacks

Q31.

How is data sent out to the attacker during a DNS tunneling attack?

A. as part of the domain name
B. as part of the UDP/53 packet pay load
C. as part of the DNS response packet
D. as part of the TCP/53 packet header

Q32.

A network engineer must monitor user and device behavior within the on-premises network. This data must be sent to the Cisco Stealthwatch Cloud analytics platform for analysis What must be done to meet this requirement using the Ubuntu-based VM appliance deployed in a VMware-based hypervisor?

A. Deploy a Cisco FTD sensor to send network events to Cisco Stealthwatch Cloud.
B. Configure a Cisco FMC to send NetFlow to Cisco Stealthwatch Cloud
C. Configure a Cisco FMC to send syslogs to Cisco Stealthwatch Cloud
D. Deploy the Cisco Stealthwatch Cloud PNM sensor that sends data to Cisco Stealthwatch Cloud

Q33.

An organization is trying to implement micro-segmentation on the network and wants to be able to gam visibility on the applications within the network. The solution must be able to maintain and force compliance. Which product should be used to meet these requirements?

A. Cisco Tetration
B. Cisco AMP
C. Cisco Umbrella
D. Cisco Stealthwatch

Q34.

Which endpoint solution protects a user from a phishing attack?

A. Cisco AnyConnect with Umbrella Roaming Security module
B. Cisco Identity Services Engine
C. Cisco AnyConnect with ISE Posture module
D. Cisco AnyConnect with Network Access Manager module

Q35.

Which Cisco platform processes behavior baselines monitors for deviations, and reviews for malicious processes in data center traffic and servers while performing software vulnerability detection?

A. Cisco AMP for Network

B. Cisco AnyConnect
C. Cisco Tetration
D. Cisco ISE

Q36.

An engineer adds a custom detection policy to a Cisco AMP deployment and encounters issues with the configuration The simple detection mechanism is configured, but the dashboard indicates that the hash is not 64 characters and is non-zero. What is the issue?

A. The file being uploaded is incompatible with simple detections and must use advanced detections.
B. The engineer is attempting to upload a file instead of a hash
C. The hash being uploaded is part of a set in an incorrect format.
D. The engineer is attempting to upload a hash created using MD5 instead of SHA-256.

Q37.

Drag and drop the NetFlow export formats from the left onto the descriptions on the right.

Answer.

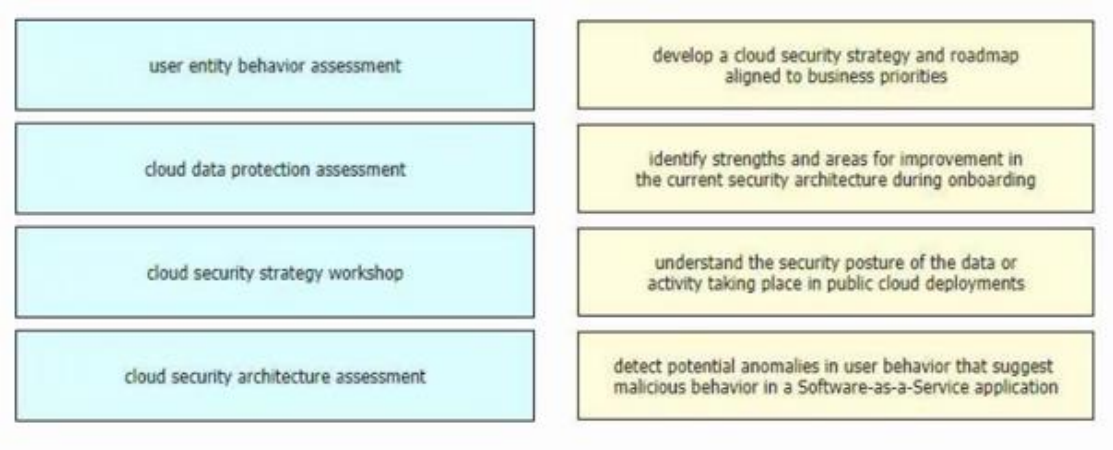
Q38.

In which two ways does Easy Connect help control network access when used with Cisco TrustSec? (Choose two.)

A. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.
B. It allows multiple security products to share information and work together to enhance security posture in the network
C. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).
D. It allows for the assignment of Security Group Tags and does not require 802 1x to be configured on the switch or the endpoint
E. It integrates with third-party products to provide better visibility throughout the network

Q39.

Drag and drop the cloud security assessment components from the left onto the definitions on the right.



Answer:

Q40.

```
ntp authentication-key 10 md5 cisco123
ntp trusted-key 10
```

Refer to the exhibit. A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced. What is the cause of this issue?

A. The key was configured in plain text.
B. The hashing algorithm that was used was MD5. which is unsupported.
C. The router was not rebooted after the NTP configuration updated.
D. NTP authentication is not enabled

Q41.

An administrator enables Cisco Threat Intelligence Director on a Cisco FMC Which process uses STIX and allows uploads and downloads of block lists?

A. editing
B. sharing
C. authoring
D. consumption

Q42.

A Cisco ISE engineer configures Central Web Authentication (CWA) for wireless guest access and must have the guest endpoints redirect to the guest portal for authentication and authorization While testing the policy, the engineer notices that the device is not redirected and instead gets full guest access. What must be done for the redirect to work?

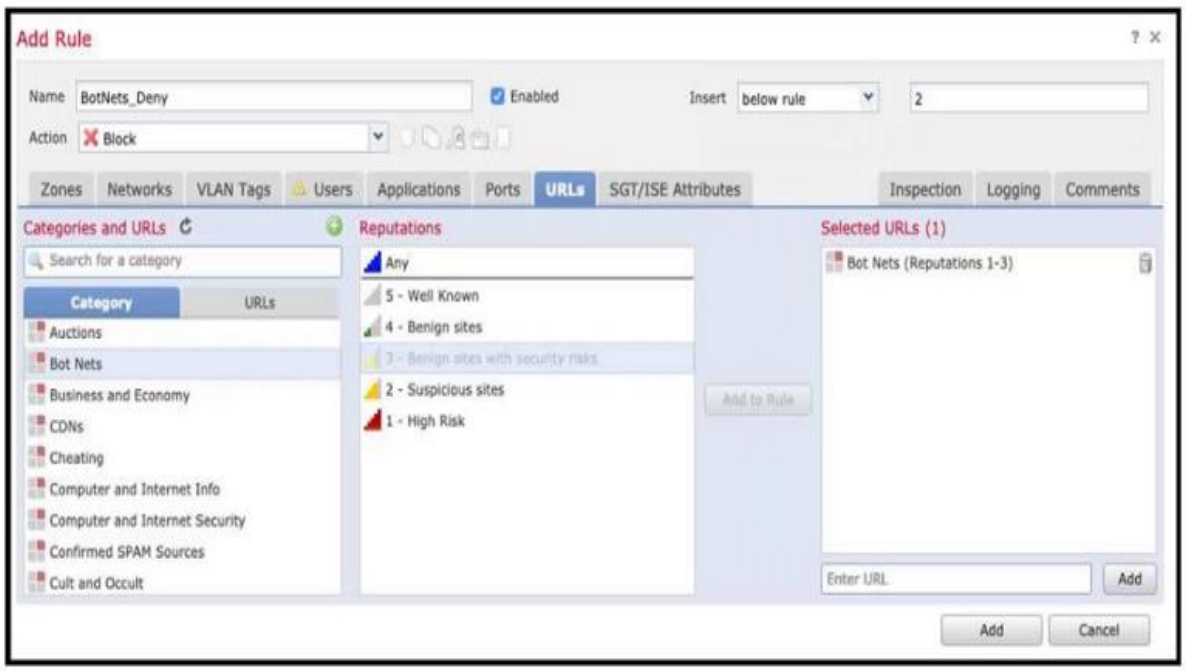
A. Tag the guest portal in the CWA part of the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit
B. Create an advanced attribute setting of Cisco: cisco-gateway-id=guest within the authorization profile for the authorization policy line that the unauthenticated devices hit.
C. Use the track movement option within the authorization profile for the authorization policy line that the unauthenticated devices hit
D. Add the DACL name for the Aire space ACL configured on the WLC in the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.

Q43.

An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems Why should the organization select either Platform as a Service or Infrastructure as a Service for this environment?

A. Infrastructure as a Service because the customer manages the operating system
B. Platform as a Service because the service provider manages the operating system
C. Infrastructure as a Service because the service provider manages the operating system.
D. Platform as a Service because the customer manages the operating system.

Q44.



Refer to the exhibit. When creating an access rule for URL filtering a network engineer adds certain categories and individual URLs to block. What is the result of the configuration?

A. Only URLs for botnets with a reputation score of 3 will be blocked
B. Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked
C. Only URLs for botnets with reputation scores of 3-5 will be blocked
D. Only URLs for botnets with reputation scores of 1-3 will be blocked

Q45.

A network engineer must migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vMotion What is a requirement for both physical hosts?
A. The hosts must use a different datastore than the virtual appliance.
B. The hosts must have access to the same defined network
C. The hosts must run Cisco Async OS 10 0 or greater
D. The hosts must run different versions of Cisco Async OS.

Q46.

An organization has a Cisco ESA set up with DLP policies and would like to customize the action assigned for violations The organization wants a copy of the message to be delivered with a message added to flag it as a DLP violation. Which actions must be performed in order to provide this capability?
A. deliver and add disclaimer text
B. deliver and send copies to other recipients
C. quarantine and alter the subject header with a DLP violation
D. quarantine and send a DLP violation notification

Q47.

What must be enabled to secure SaaS-based applications?
A. two-factor authentication
B. application security gateway
C. modular policy framework
D. end-to-end encryption

Q48.

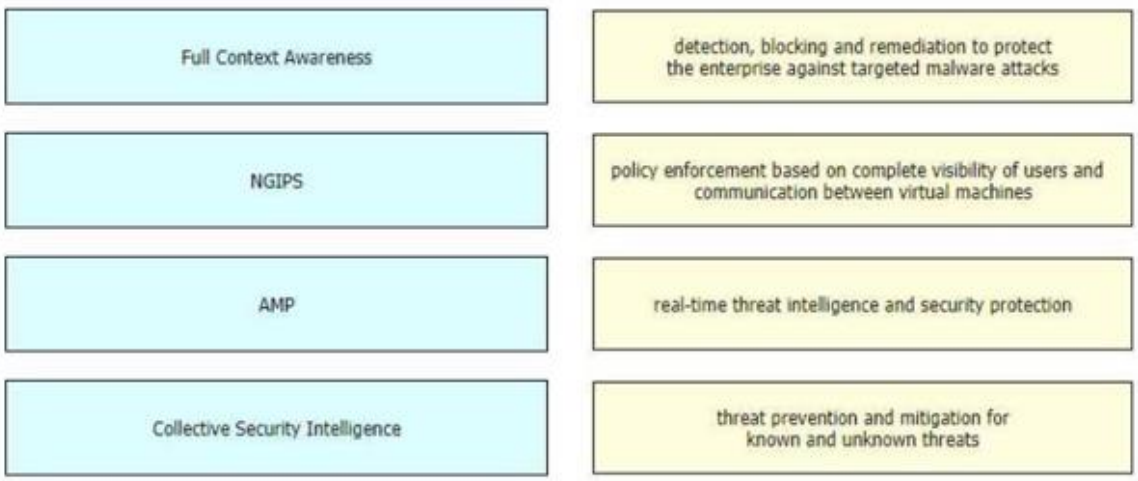
Which type of DNS abuse exchanges data between two computers even when there is no direct connection?
A. command-and-control communication
B. malware installation
C. data exfiltration
D. network foot printing

Q49.

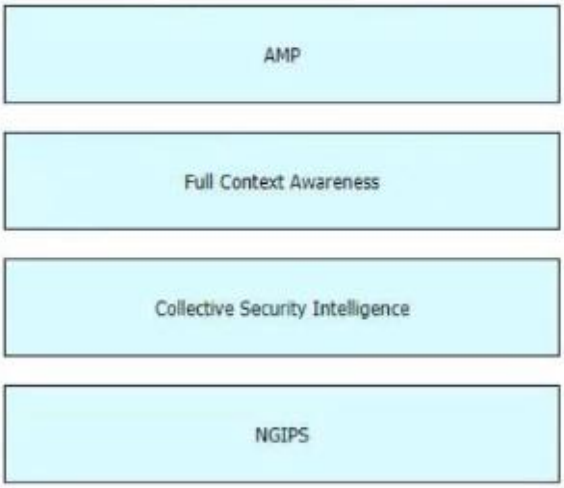
An engineer has been tasked with configuring a Cisco FTD to analyze protocol fields and detect anomalies in the traffic from industrial systems. What must be done to meet these requirements?
A. Implement pre-filter policies for the CIP preprocessor.
B. Enable traffic analysis in the Cisco FTD.
C. Modify the access control policy to trust the industrial traffic
D. Configure intrusion rules for the DNP3 preprocessor.

Q50.

Drag and drop the features of Cisco epower from the left onto the benefits on the right.



Answer:



Q51.

A network engineer must configure a Cisco ESA to prompt users to enter two forms of information before gaining access. The Cisco ESA must also join a cluster machine using preshared keys. What must be configured to meet these requirements?

A. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA CLI.
B. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA GUI
C. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA CLI.
D. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA GUI.

Q52.

What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.)

A. Deploy a separate eDirectory server: the client IP address is recorded in this server.
B. The eDirectory client must be installed on each client workstation
C. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.
D. Create NTLM or Kerberos authentication realm and enable transparent user identification
E. Create an LDAP authentication realm and disable transparent user identification.

Q53.

Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

A. Open IOC
B. OpenC2
C. Cyb OX
D. STIX

Q54.

An administrator is adding a new Cisco ISE node to an existing deployment What must be done to ensure that the addition of the node will be successful when inputting the FQDN?

A. Change the IP address of the new Cisco ISE node to the same network as the others.
B. Make the new Cisco ISE node a secondary PAN before registering it with the primary.
C. Add the DNS entry for the new Cisco ISE node into the DNS server
D. Open port 8905 on the firewall between the Cisco ISE nodes

Q55.

Which method is used to deploy certificates and configure the supplicant on mobile devices to gam access to network resources?

A. Simple Certificate Enrollment Protocol
B. client provisioning
C. MAC authentication bypass
D. BYOD onboarding

Q56.

What is a benefit of using a multifactor authentication strategy?
A. It provides visibility into devices to establish device trust.
B. It protects data by enabling the use of a second validation of identity
C. It provides an easy, single sign-on experience against multiple applications
D. It provides secure remote access for applications.

Q57.

A Cisco ESA administrator has been tasked with configuring the Cisco ESA to ensure there are no viruses before quarantined emails are delivered In addition delivery of mail from known bad mail servers must be prevented. Which two actions must be taken in order to meet these requirements? (Choose two)
A. Deploy the Cisco ESA in the DMZ.
B. Scan quarantined emails using AntiVirus signatures
C. Enable a message tracking service.
D. Use outbreak filters from SenderBase
E. Configure a recipient access table

Q58.

What is the result of the ACME-Router(config)#login block-for 100 attempts 4 within 60 command on a Cisco IOS router?
A. After four unsuccessful log in attempts, the line is blocked for 100 seconds and only permit IP addresses are permitted in ACL 60
B. If four failures occur in 60 seconds, the router goes to quiet mode for 100 seconds.
C. If four log in attempts fail in 100 seconds, wait for 60 seconds to next log in prompt
D. After four unsuccessful log in attempts, the line is blocked for 60 seconds and only permit IP addresses are permitted in ACL 100

Q59.

What is the difference between a vulnerability and an exploit?
A. An exploit is a hypothetical event that causes a vulnerability in the network.
B. A vulnerability is a weakness that can be exploited by an attacker.
C. A vulnerability is a hypothetical event for an attacker to exploit
D. An exploit is a weakness that can cause a vulnerability in the network

Q60.

An organization configures Cisco Umbrella to be used for its DNS services. The organization must be able to block traffic based on the subnet that the endpoint is on, but it sees only the requests from its public IP address instead of each internal IP address. What must be done to resolve this issue?

A. Use the tenant control features to identify each subnet being used and track the connections within the Cisco Umbrella dashboard
B. Configure an internal domain within Cisco Umbrella to help identify each address and create policy from the domains.
C. Install the Microsoft Active Directory Connector to give IP address information stitched to the requests in the Cisco Umbrella dashboard
D. Set up a Cisco Umbrella virtual appliance to internally field the requests and see the traffic of each IP address.

Q61.

An organization has noticed an increase in malicious content downloads and wants to use Cisco Umbrella to prevent this activity for suspicious domains while allowing normal web traffic Which action will accomplish this task?

A. Use destination block lists.
B. Set content settings to High.
C. Configure the intelligent proxy
D. Configure application block lists.

Q62.

Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?

A. selfsigned
B. url
C. terminal
D. profile

Q63.

An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco Firepower Which feature should be used to accomplish this?

A. Access Control
B. Packet Tracer
C. Network Discovery
D. NetFlow

Q64.

An organization has a requirement to collect full metadata information about the traffic going through their AWS cloud services They want to use this information for behavior analytics and statistics. Which two actions must be taken to implement this requirement?

A. Send syslog from AWS to Cisco Stealthwatch Cloud.
B. Configure Cisco ACI to ingest AWS information.
C. Send VPC Flow Logs to Cisco Stealthwatch Cloud.
D. Configure Cisco Thousand Eyes to ingest AWS information.
E. Configure Cisco Stealthwatch Cloud to ingest AWS information

Q65.

What are two functionalities of SDN Northbound APIs? (Choose two)

A. OpenFlow is a standardized northbound API protocol.
B. Northbound APIs use the NETCONF protocol to communicate with applications
C. Northbound APIs form the interface between the SDN controller and business applications.
D. Northbound APIs form the interface between the SDN controller and the network switches or routers
E. Northbound APIs provide a programmable interface for applications to dynamically configure the network

Q66.

A Cisco AMP for Endpoints administrator configures a custom detection policy to add specific MD5 signatures The configuration is created in the simple detection policy section, but it does not work. What is the reason for this failure?

A. The APK must be uploaded for the application that the detection is intended
B. The administrator must upload the file instead of the hash for Cisco AMP to use
C. The MD5 hash uploaded to the simple detection policy is in the incorrect format.
D. Detections for MD5 signatures must be configured in the advanced custom detection policies

Q67.

What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?

A. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA.
B. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA

C. Cisco CWS minimizes the load on the internal .network and security infrastructure as compared to Cisco WSA
D. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not.

Q68.

What is the intent of a basic SYN flood attack?
A. to cause the buffer to overflow
B. to solicit DNS responses
C. to flush the register stack to re-initiate the buffers
D. to exceed the threshold limit of the connection queue

Q69.

```
.... #(code snipped)
...
api_path = "/api/access/global/rules"
url = server + api_path
f = None

post_data = {
"sourceService": {
"kind": serviceKind,
"value": sourceServiceValue
},
"destinationAddress": {
"kind": destinationAddressKind,
"value": destinationAddress
},
"remarks": [],
"destinationService": {
"kind": serviceKind,
"value": destinationServiceValue
},
"permit": trueORfalse,
"active": "true",
"position": "1",
"sourceAddress": {
"kind": sourceAddressKind,
"value": sourceAddress
}
}

req = urllib2.Request(url, json.dumps(post_data), headers)
base64string = base64.encodestring('%s:%s' % (username, password)).replace('\n', '')
req.add_header("Authorization", "Basic %s" % base64string)
try:
f = urllib2.urlopen(req)
status_code = f.getcode()

print "Status code is "+str(status_code)
if status_code == 201:
print "Operation successful"
except urllib2.HTTPError, err:
print "Error received from server. HTTP Status code :"+str(err.code)
try:
json_error = json.loads(err.read())
if json_error:
print json.dumps(json_error,sort_keys=True,indent=4, separators=(',', ': '))
except ValueError:
pass
finally:
if f: f.close()
```

Refer to the exhibit What is the function of the Python script code snippet for the Cisco ASA REST API?

A. obtains the saved configuration of the Cisco ASA firewall
B. deletes a global rule from policies
C. changes the hostname of the Cisco ASA
D. Adds a global rule into policies

Q70.

What is a difference between an XSS attack and an SQL injection attack?

A. XSS is a hacking method used to attack SQL databases whereas SQL injection attacks can exist in many different types of applications.
B. XSS attacks are used to steal information from databases, whereas SQL injection attacks are used to redirect users to websites where attackers can steal data from them
C. SQL injection is a hacking method used to attack SQL databases, whereas XSS attacks can exist in many different types of applications.
D. SQL injection attacks are used to steal information from databases, whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

Q71.

An engineer must modify a policy to block specific addresses using Cisco Umbrella The policy is created already and is actively used by devices, using many of the default policy elements What else must be done to accomplish this task?

A. Use content categories to block or allow specific addresses
B. Add the specified addresses to the identities list and create a block action
C. Modify the application settings to allow only applications to connect to required addresses.
D. Create a destination list for addresses to be allowed or blocked.

Q72.

How does a cloud access security broker function'?

A. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution.
B. It scans other cloud solutions being used within the network and identifies vulnerabilities
C. It is an authentication broker to enable single sign-on and multi-factor authentication for a cloud solution

D. It acts as a security information and event management solution and receives syslog from other cloud solutions.

Q73.

An engineer needs to add protection for data in transit and have headers in the email message Which configuration is needed to accomplish this goal?

A. Map sender IP addresses to a host interface.
B. Provision the email appliance
C. Deploy an encryption appliance.
D. Enable flagged message handling

Q74.

What are two rootkit types? (Choose two)

A. bootloader
B. virtual
C. buffer mode
D. registry
E. user mode

Q75.

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

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

Q76.

An engineer configures new features within the Cisco Umbrella dashboard and wants to identify and proxy traffic that is categorized as risky domains and may contain safe and malicious content Which action accomplishes these objectives?

A. Upload the threat intelligence database to Cisco Umbrella for the most current information on reputations and to have the destination lists block them.
B. Create a new site within Cisco Umbrella to block requests from those categories so they can be sent to the proxy device
C. Configure URL filtering within Cisco Umbrella to track the URLs and proxy the requests for those categories and below,
D. Configure intelligent proxy within Cisco Umbrella to intercept and proxy the requests for only those categories.

Q77.

What are two functions of TAXII in threat intelligence sharing? (Choose two)
A. exchanges trusted anomaly intelligence information
B. supports STIX information
C. determines the "what" of threat intelligence
D. allows users to describe threat motivations and abilities
E. determines how threat intelligence information is relayed

Q78.

An engineer is configuring Cisco Umbrella and has an identity that references two different policies. Which action ensures that the policy that the identity must use takes precedence over the second one?
A. Configure the default policy to redirect the requests to the correct policy.
B. Place the policy with the most-specific configuration last in the policy order
C. Configure only the policy with the most recently changed timestamp.
D. Make the correct policy first in the policy order.

Q79.

What is a characteristic of a bridge group in a Cisco ASA Firewall running in transparent mode?
A. It allows ARP traffic with a single access rule.
B. It is a Layer 3 segment and includes one port and customizable access rules.
C. It includes multiple interfaces and access rules between interfaces are customizable.
D. It has an IP address on its BVI interface and is used for management traffic

Q80.

Which two methods must be used to add switches into the fabric so that administrators can control how switches are added into DCNM for private cloud management? (Choose two)
A. Cisco Cloud Director
B. Cisco Prime Infrastructure
C. CDP Auto Discovery
D. Seed IP
E. Power On Auto Provisioning

Q81.

Which attribute has the ability to change during the RADIUS CoA?
A. membership
B. accessibility
C. authorization
D. NTP

Q82.

What is a difference between Cisco AMP for Endpoints and Cisco Umbrella'?
A. Cisco AMP for Endpoints is a cloud-based service, and Cisco Umbrella is not.
B. Cisco AMP for Endpoints automatically researches indicators of compromise and confirms threats, and Cisco Umbrella does not.
C. Cisco AMP for Endpoints prevents connections to malicious destinations, and Cisco Umbrella works at the file level to prevent the initial execution of malware.
D. Cisco AMP for Endpoints prevents, detects, and responds to attacks before damage can be done and Cisco Umbrella provides the first line of defense against Internet threats

Q83.

What are two functionalities of northbound and southbound APIs within Cisco SDN architecture? (Choose two)
A. Southbound APIs are used to define how SDN controllers integrate with applications.
B. Southbound interfaces utilize device configurations such as VLANs and IP addresses.
C. Northbound APIs utilize RESTful API methods such as GET, POST and DELETE.
D. Northbound interfaces utilize OpenFlow and OpFlex to integrate with network devices.
E. Southbound APIs utilize CLI SNMP, and RESTCONF

Q84.

What are two advantages of using Cisco AnyConnect over DMVPN? (Choose two)
A. It allows multiple sites to connect to the data center
B. It enables VPN access for individual users from their machines
C. It provides spoke-to-spoke communications without traversing the hub
D. It allows different routing protocols to work over the tunnel.
E. It allows customization of access policies based on user identity

Q85.

What is a benefit of performing device compliance?

A. providing multi-factor authentication
B. verification of the latest OS patches
C. device classification and authorization
D. providing attribute-driven policies

Q86.

An administrator is adding a new switch onto the network and has configured AAA for network access control When testing the configuration the RADIUS authenticates to Cisco ISE but is being rejected. Why is the **ip radius source-interface** command needed for this configuration?

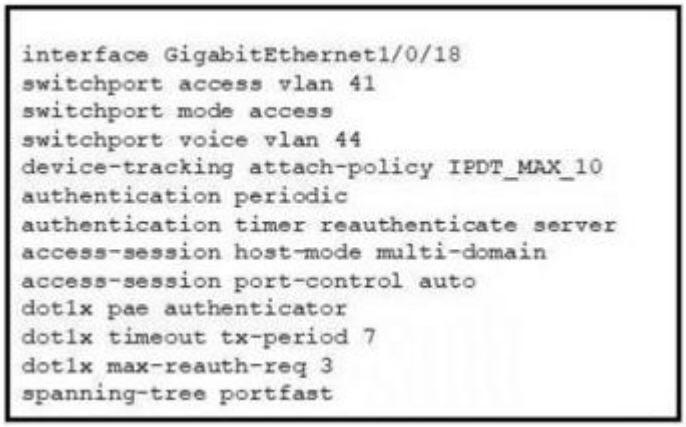
A. Only requests that originate from a configured NAS IP are accepted by a RADIUS server.
B. RADIUS requests are generated only by a router if a RADIUS source interface is defined.
C. Encrypted RADIUS authentication requires the RADIUS source interface be defined
D. The RADIUS authentication key is transmitted only from the defined RADIUS source interface

Q87.

Which security product enables administrators to deploy Kubernetes clusters in air-gapped sites without needing Internet access?

A. Cisco Container Platform
B. Cisco Content Platform
C. Cisco Cloud Platform
D. Cisco Container Controller

Q88.



```
interface GigabitEthernet1/0/18
switchport access vlan 41
switchport mode access
switchport voice vlan 44
device-tracking attach-policy IPDT_MAX_10
authentication periodic
authentication timer reauthenticate server
access-session host-mode multi-domain
access-session port-control auto
dot1x pae authenticator
dot1x timeout tx-period 7
dot1x max-reauth-req 3
spanning-tree portfast
```

Refer to the exhibit. A Cisco ISE administrator adds a new switch to an 802.1X deployment and has difficulty with some endpoints gaming access. Most PCs and IP phones can connect and authenticate using their machine certificate credentials, however printers and video cameras cannot Based on the interface configuration provided, what must be done to get these devices onto the network using Cisco ISE for authentication and authorization while maintaining security controls?

A. Change the default policy in Cisco ISE to allow all devices not using machine authentication
B. Enable insecure protocols within Cisco ISE in the allowed protocols configuration.
C. Add mab to the interface configuration
D. Configure authentication event fail retry 2 action authorize vlan 41 on the interface

Q89.

Which security solution protects users leveraging DNS-layer security?

A. Cisco FTD
B. Cisco ISE
C. Cisco ASA
D. Cisco Umbrella

Q90.

What are two DDoS attack categories? (Choose two)

A. database
B. volume-based
C. source-based
D. sequential
E. protocol

Q91.

Which kind of API that is used with Cisco DNA Center provisions SSIDs QoS policies, and update software versions on switches?
A. multivendor
B. integration
C. event
D. intent

Q92.

What is the benefit of integrating Cisco ISE with a MDM solution'?
A. It provides the ability to add applications to the mobile device through Cisco ISE.
B. It provides compliance checks for access to the network
C. It provides the ability to update other applications on the mobile device.
D. It provides network device administration access.

Q93.

What are two functions of secret key cryptography? (Choose two)
A. utilization of different keys for encryption and decryption
B. utilization of less memory
C. utilization of large prime number iterations
D. key selection without integer factorization
E. provides the capability to only know the key on one side

Q94.

Which role is a default guest type in Cisco ISE?
A. Yearly
B. Monthly
C. Full-Time
D. Contractor

Q95.

Which portion of the network do EPP solutions solely focus on and EDR solutions do not?
A. core
B. perimeter
C. East-West gateways
D. server farm

Q96.

Why is it important to implement MFA inside of an organization?

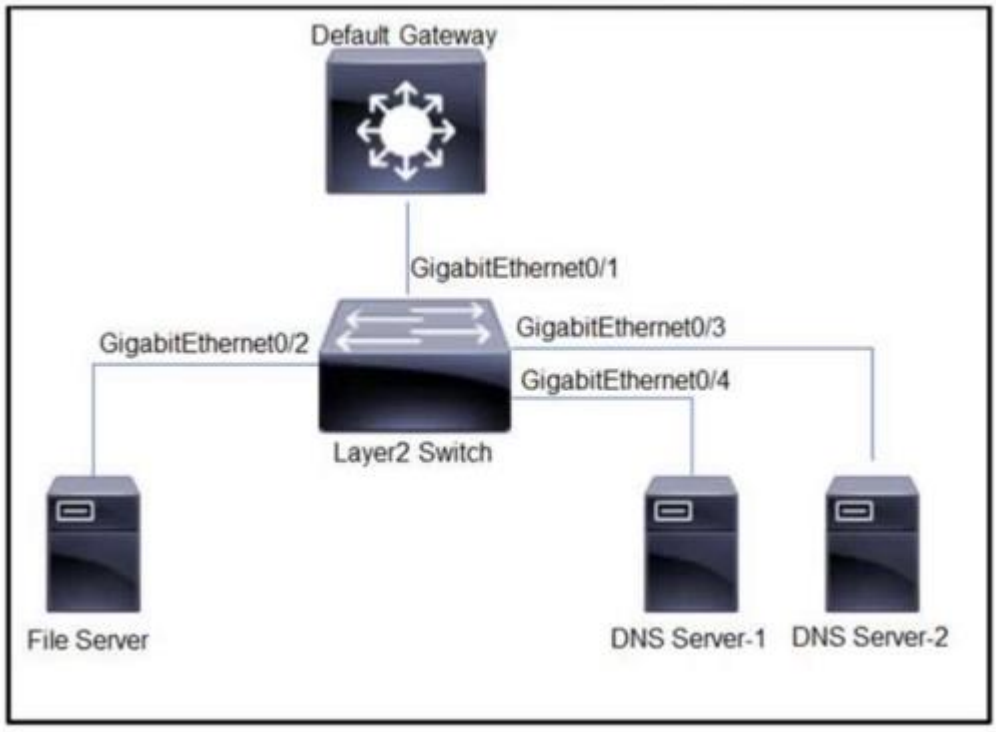
A. To prevent phishing attacks from being successful.
B. To prevent brute force attacks from being successful
C. To prevent DoS attacks from being successful
D. To prevent man-the-middle attacks from being successful

Q97.

An organization has a Cisco Stealthwatch Cloud deployment in their environment. Cloud logging is working as expected but logs are not being received from the on-premise network What action will resolve this issue?

A. Configure security appliances to send NetFlow to Cisco Stealthwatch Cloud
B. Deploy a Cisco FTD sensor to send events to Cisco Stealthwatch Cloud
C. Configure security appliances to send syslogs to Cisco Stealthwatch Cloud
D. Deploy a Cisco Stealthwatch Cloud sensor on the network to send data to Cisco Stealthwatch Cloud.

Q98.



Refer to the exhibit All servers are in the same VLAN/Subnet DNS Server-1 and DNS Server-2 must communicate with each other and all servers must communicate with default gateway multilayer switch Which type of private VLAN

ports should be configured to prevent communication between DNS servers and the file server?

A. Configure GigabitEthernet0/1 as community port. GigabitEthernet0/2 as promiscuous port, GigabitEthernet0/3 and GigabitEthernet0/4 as isolated ports.
B. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as isolated port and GigabitEthernet0/3 and GigabitEthernet0/4 as community ports
C. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as community port, and GigabitEthernet0/3 and GigabitEthernet0/4 as isolated ports
D. Configure GigabitEthernet0/1 as community port GigabitEthernet0/2 as isolated port, and GigabitEthernet0/3 and GigabitEthernet0/4 as promiscuous ports

Q99.

An organization wants to implement a cloud-delivered and SaaS-based solution to etection policy
bility and threat detection across the AWS network The solution must be deployed without software agents and rely on AWS VPC flow logs instead. Which solution meets these requirements?

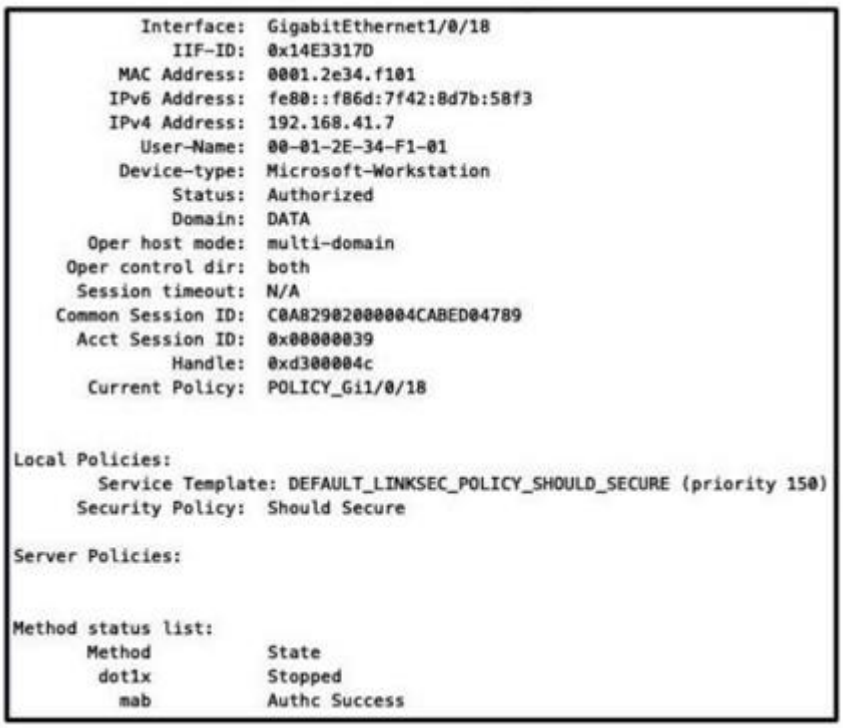
A. Cisco Cloudlock
B. Cisco Stealthwatch Cloud
C. NetFlow collectors
D. Cisco Umbrella

Q100.

What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group'?

A. external identity source
B. CoA
C. SNMP probe
D. posture assessment

Q101.



```
           Interface:  GigabitEthernet1/0/18
              IIF-ID:  0x14E3317D
         MAC Address:  0001.2e34.f101
        IPv6 Address:  fe80::f86d:7f42:8d7b:58f3
        IPv4 Address:  192.168.41.7
           User-Name:  00-01-2E-34-F1-01
         Device-type:  Microsoft-Workstation
              Status:  Authorized
              Domain:  DATA
     Oper host mode:  multi-domain
   Oper control dir:  both
    Session timeout:  N/A
  Common Session ID:  C0A82982000004CABED04789
    Acct Session ID:  0x00000039
             Handle:  0xd300004c
     Current Policy:  POLICY_Gi1/0/18


Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
    Security Policy:  Should Secure

Server Policies:


Method status list:
       Method           State
        dot1x           Stopped
          mab           Authc Success
```

Refer to the exhibit Which configuration item makes it possible to have the AAA session on the network?

A. aaa authentication login console ise
B. aaa authorization network default group ise
C. aaa authorization exec default ise
D. aaa authentication enable default enable

Q102.

Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two)

A. Cisco Duo Security
B. Cisco ISE
C. Cisco TrustSec
D. Cisco DNA Center
E. Cisco Umbrella