QUESTION 338
Refer to the exhibit. A Cisco ISE administrator adds a new switch to an 802.1X deployment and has difficulty with some endpoints gaining access.


```
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
```

Most PCs and IP phones can connect and authenticate using their machine certificate credentials. However printer and video cameras cannot base d on the interface configuration provided, what must be to get these devices on to 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. Configure authentication event fail retry 2 action authorize vlan 41 on the interface
D. Add mab to the interface configuration.

Answer: A

QUESTION 339
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. The RADIUS authentication key is transmitted only from the defined RADIUS source interface
C. RADIUS requests are generated only by a router if a RADIUS source interface is defined.

D. Encrypted RADIUS authentication requires the RADIUS source interface be defined

Answer: B

QUESTION 340
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. Forward file
C. PAC file
D. Bridge mode

Answer: C

QUESTION 341
Refer to the exhibit. What does this Python script accomplish?

```
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")))
```

A. It allows authentication with TLSv1 SSL protocol
B. It authenticates to a Cisco ISE with an SSH connection.
C. It authenticates to a Cisco ISE server using the username of ersad

Answer: C

QUESTION 342

350-701 Exam Dumps 350-701 Exam Questions 350-701 PDF Dumps 350-701 VCE Dumps

https://www.braindump2go.com/350-701.html

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

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

Answer: B

QUESTION 343
Which feature is leveraged by advanced antimalware capabilities to be an effective endpomt protection platform?

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

Answer: C

QUESTION 344
An organization wants to implement a cloud-delivered and SaaS-based solution to provide visibility 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 Stealthwatch Cloud
B. Cisco Umbrella
C. NetFlow collectors
D. Cisco Cloudlock

Answer: A

QUESTION 345
What is the difference between a vulnerability and an exploit?

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

Answer: B

QUESTION 346
Cisco SensorBase gaihers threat information from a variety of Cisco products and services and performs analytics to find patterns on threats.
Which term describes this process?

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

Answer: A

QUESTION 347

An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1.1.1.1 using the flow record Stea!thwatch406397954 command.
Which additional command is required to complete the flow record?

A. transport udp 2055
B. match ipv4 ttl
C. cache timeout active 60
D. destination 1.1.1.1

Answer: B

QUESTION 348
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 Tetration
B. Cisco ISE?
C. Cisco AMP for Network
D. Cisco AnyConnect

Answer: C

QUESTION 349
How is data sent out to the attacker during a DNS tunneling attack?

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

Answer: B

QUESTION 350
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. Configure Cisco DUO with the external Active Directory connector and tie it to the policy set within Cisco ISE.
B. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE
C. Create an identity policy within Cisco ISE to send all authentication requests to Cisco DUO.
D. Modify the current policy with the condition MFASourceSequence DUO=true in the authorization conditions within Cisco ISE

Answer: C

QUESTION 351
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 administrator must upload the file instead of the hash for Cisco AMP to use.
B. The MD5 hash uploaded to the simple detection policy is in the incorrect format
C. The APK must be uploaded for the application that the detection is intended
D. Detections for MD5 signatures must be configured in the advanced custom detection policies

Answer: D

QUESTION 352
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. Platform as a Service because the customer manages the operating system
B. Infrastructure as a Service because the customer manages the operating system
C. Platform as a Service because the service provider manages the operating system
D. Infrastructure as a Service because the service provider manages the operating system

Answer: B

QUESTION 353
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. Open port 8905 on the firewall between the Cisco ISE nodes
D. Add the DNS entry for the new Cisco ISE node into the DNS server

Answer: B

QUESTION 354
Refer to the exhibit. What will occur when this device tries to connect to the port?

```
interface GigabitEthernet1/0/18
 description ISE dot1x Port
 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
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 spanning-tree portfast
 service-policy type control subscriber POLICY_Gi1/0/18
```

A. 802.1X will not work, but MAB will start and allow the device on the network.
B. 802.1X will not work and the device will not be allowed network access
C. 802 1X will work and the device will be allowed on the network
D. 802 1X and MAB will both be used and ISE can use policy to determine the access level

Answer: D

QUESTION 355
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 RADIUS server and then join the cluster by using the Cisco ESA CLI.
B. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA GUI
C. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA GUI.
D. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA CLI

Answer: D

QUESTION 356
Which portion of the network do EPP solutions solely focus on and EDR solutions do not?

A. server farm
B. perimeter
C. core
D. East-West gateways

Answer: B

QUESTION 357
Refer to the exhibit. An engineer is implementing a certificate based VPN.
What is the result of the existing configuration?

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

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

Answer: A

QUESTION 358
What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?

A. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not
B. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA.
C. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA
D. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA

Answer: D