Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

NEW QUESTION 1
- (Exam Topic 2)
Which public cloud provider supports the Cisco Next Generation Firewall Virtual?

A. Google Cloud Platform
B. Red Hat Enterprise Visualization
C. VMware ESXi
D. Amazon Web Services

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/ white-paper-c11-740505.html

NEW QUESTION 2
- (Exam Topic 2)
After a recent breach, an organization determined that phishing was used to gain initial access to the network before regaining persistence. The information gained from the phishing attack was a result of users visiting known malicious websites. What must be done in order to prevent this from happening in the future?

A. Modify an access policy
B. Modify identification profiles
C. Modify outbound malware scanning policies
D. Modify web proxy settings

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Access

NEW QUESTION 3
- (Exam Topic 2)
An organization recently installed a Cisco WSA and would like to take advantage of the AVC engine to allow the organization to create a policy to control application specific activity. After enabling the AVC engine, what must be done to implement this?

A. Use security services to configure the traffic monitor, .
B. Use URL categorization to prevent the application traffic.
C. Use an access policy group to configure application control settings.
D. Use web security reporting to validate engine functionality

Answer: C

Explanation:
The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or allow applications individually or according to application type. You can also apply controls to particular application types.

NEW QUESTION 4
- (Exam Topic 2)
How does Cisco Advanced Phishing Protection protect users?

A. It validates the sender by using DKIM.
B. It determines which identities are perceived by the sender
C. It utilizes sensors that send messages securely.
D. It uses machine learning and real-time behavior analytics.

Answer: D

Explanation:
Reference: https://docs.ces.cisco.com/docs/advanced-phishing-protection

NEW QUESTION 5
- (Exam Topic 2)
Why is it important to have logical security controls on endpoints even though the users are trained to spot security threats and the network devices already help prevent them?

A. to prevent theft of the endpoints
B. because defense-in-depth stops at the network
C. to expose the endpoint to more threats
D. because human error or insider threats will still exist

Answer: D

NEW QUESTION 6

- (Exam Topic 2)
Refer to the exhibit.

An administrator is adding a new Cisco FTD device to their network and wants to manage it with Cisco FMC. The Cisco FTD is not behind a NAT device. Which command is needed to enable this on the Cisco FTD?

A. configure manager add DONTRESOLVE kregistration key>
B. configure manager add <FMC IP address> <registration key> 16
C. configure manager add DONTRESOLVE <registration key> FTD123
D. configure manager add <FMC IP address> <registration key>

Answer: D

Explanation:
Reference: https://cyruslab.net/2019/09/03/ciscocisco-firepower-lab-setup/

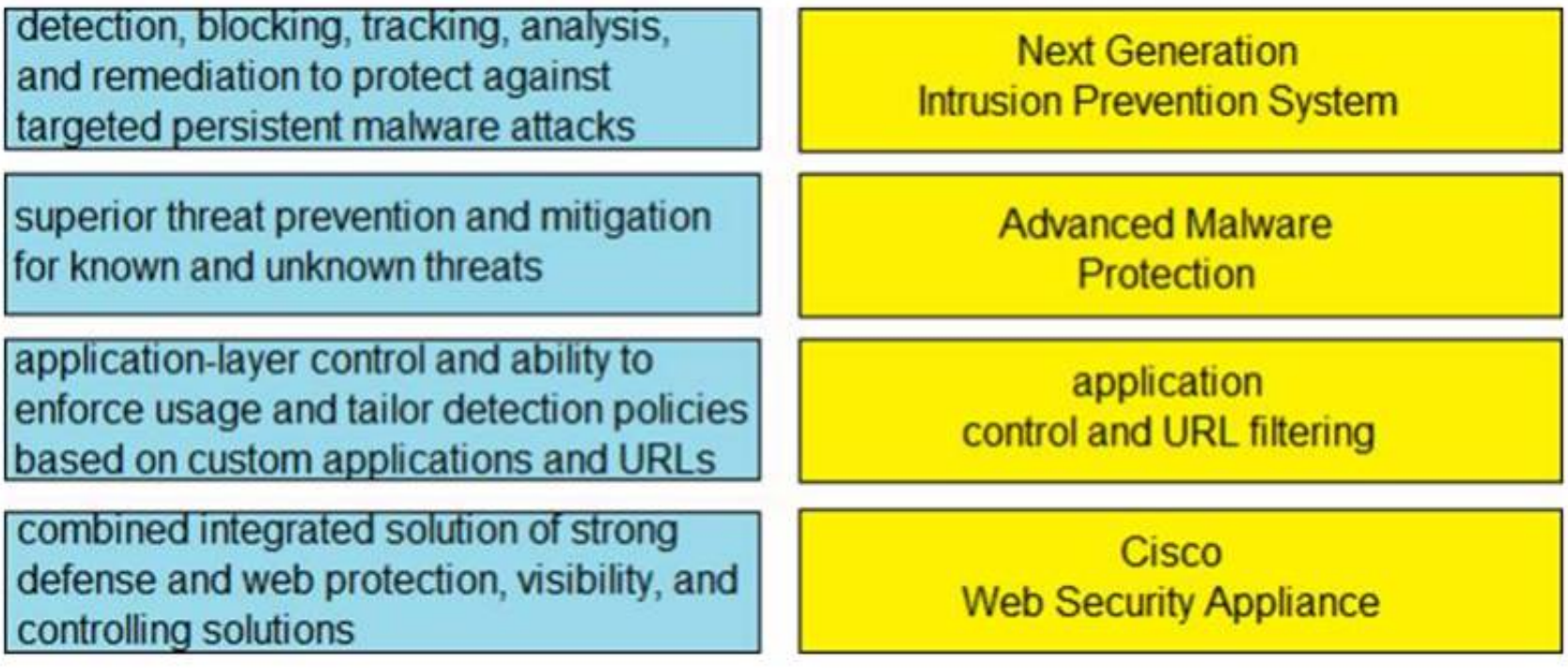
NEW QUESTION 7
- (Exam Topic 2)
An organization has a Cisco Stealthwatch Cloud deployment in their environment. Cloud logging is working as expected, but logs are not being received from the on-premise network, what action will resolve this issue?

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

Answer: D

Explanation:
Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide

NEW QUESTION 8
- (Exam Topic 2)
Drag and drop the capabilities from the left onto the correct technologies on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, chat or text message Description automatically generated

NEW QUESTION 9
- (Exam Topic 2)
An organization has two systems in their DMZ that have an unencrypted link between them for communication.
The organization does not have a defined password policy and uses several default accounts on the systems. The application used on those systems also have not gone through stringent code reviews. Which vulnerability would help an attacker brute force their way into the systems?

A. weak passwords
B. lack of input validation
C. missing encryption
D. lack of file permission

Answer: C

Explanation:
Reference: https://tools.ietf.org/html/rfc3954

NEW QUESTION 10
- (Exam Topic 1)
Refer to the exhibit.

```
Sysauthcontrol              Enabled
Dot1x Protocol Version          3

Dot1x Info for GigabitEthernet1/0/12
-----------------------------------
PAE                     = AUTHENTICATOR
PortControl             = FORCE_AUTHORIZED
ControlDirection        = Both
HostMode                = SINGLE_HOST
QuietPeriod             = 60
ServerTimeout           = 0
SuppTimeout             = 30
ReAuthMax               = 2
MaxReq                  = 2
TxPeriod                = 30
```

Which command was used to display this output?

A. show dot1x all
B. show dot1x
C. show dot1x all summary
D. show dot1x interface gi1/0/12

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
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

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/platfo the answer should be “Platform Settings Policy”, not “Platform Service Policy” but it is the bestanswer here so we have to choose it.

NEW QUESTION 14
- (Exam Topic 1)

For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two)

A. Windows service
B. computer identity
C. user identity
D. Windows firewall
E. default browser

Answer: AD

NEW QUESTION 15
- (Exam Topic 1)
Refer to the exhibit.

```
snmp-server group SNMP v3 auth access
15
```

What does the number 15 represent in this configuration?

A. privilege level for an authorized user to this router
B. access list that identifies the SNMP devices that can access the router
C. interval in seconds between SNMPv3 authentication attempts
D. number of possible failed attempts until the SNMPv3 user is locked out

Answer: B

Explanation:
The syntax of this command is shown below:snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]}] [read read-view] [write write-view] [notify notify-view] [access access-list]The command above restricts which IP source addresses are allowed to access SNMP functions on the router. You could restrict SNMP access by simply applying an interface ACL to block incoming SNMP packets that don't come from trusted servers. However, this would not be as effective as using the global SNMP commands shown in this recipe. Because you can apply this method once for the whole router, it is much simpler than applying ACLs to block SNMP on all interfaces separately. Also, using interface ACLs would block not only SNMP packets intended for this router, but also may stop SNMP packets that just happened to be passing through on their way to some other destination device.

NEW QUESTION 18
- (Exam Topic 1)
What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?

A. EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.
B. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.
C. EPP focuses on network security, and EDR focuses on device security.
D. EDR focuses on network security, and EPP focuses on device security.

Answer: A

NEW QUESTION 23
- (Exam Topic 1)
Refer to the exhibit.

```
*Jun 30 16:52:33.795: ISAKMP:(1002): retransmission skipped for phase 1 (time
since last transmission 504)
R1#
*Jun 30 16:52:40.183: ISAKMP:(1001):purging SA., sa=68CEE058, delme=68CEE058
R1#
*Jun 30 16:52:43.291: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:43.291: ISAKMP (1002): incrementing error counter on sa, attempt 5
of 5: retransmit phase 1
*Jun 30 16:52:43.295: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002): sending packet to 10.10.12.2 my_port 500
peer_port 500 (I) MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002):Sending an IKE IPv4 Packet.
R1#
*Jun 30 16:52:53.299: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:53.299: ISAKMP:(1002):peer does not do paranoid keepalives.

*Jun 30 16:52:53.299: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.303: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.307: ISAKMP: Unlocking peer struct 0x68287318 for
isadb_mark_sa_deleted(), count 0
*Jun 30 16:52:53.307: ISAKMP: Deleting peer node by peer_reap for 10.10.12.2:
68287318
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node 79875537 error FALSE reason "IKE
deleted"
R1#
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node -484575753 error FALSE reason
"IKE deleted"
*Jun 30 16:52:53.315: ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL
*Jun 30 16:52:53.319: ISAKMP:(1002):Old State = IKE_I_MM5 New State = IKE_DEST_SA
```

A network administrator configured a site-to-site VPN tunnel between two Cisco IOS routers, and hosts are unable to communicate between two sites of VPN. The network administrator runs the debug crypto isakmp sa command to track VPN status. What is the problem according to this command output?

A. hashing algorithm mismatch
B. encryption algorithm mismatch
C. authentication key mismatch
D. interesting traffic was not applied

Answer: C

NEW QUESTION 25
- (Exam Topic 1)
What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?

A. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously.
B. It discovers and controls cloud apps that are connected to a company's corporate environment.
C. It deletes any application that does not belong in the network.
D. It sends the application information to an administrator to act on.

Answer: B

NEW QUESTION 26
- (Exam Topic 1)
Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?

A. cloud web services
B. network AMP
C. private cloud
D. public cloud

Answer: C

NEW QUESTION 29
- (Exam Topic 1)
What are two reasons for implementing a multifactor authentication solution such as Duo Security provide to an organization? (Choose two)

A. flexibility of different methods of 2FA such as phone callbacks, SMS passcodes, and push notifications
B. single sign-on access to on-premises and cloud applications
C. integration with 802.1x security using native Microsoft Windows supplicant
D. secure access to on-premises and cloud applications
E. identification and correction of application vulnerabilities before allowing access to resources

Answer: AD

Explanation:
Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using asecond factor (like your phone or other mobile device) prevents anyone but you from logging in, even if theyknow your password.Note: Single sign-on (SSO) is a property of identity and access management that enables users to securelyauthenticate with multiple applications and websites by logging in only once with just one set of credentials(username and password). With SSO, the application or website that the user is trying to access relies on atrusted third party to verify that users are who they say they are.

NEW QUESTION 33
- (Exam Topic 1)
After deploying a Cisco ESA on your network, you notice that some messages fail to reach their destinations. Which task can you perform to determine where each message was lost?

A. Configure the trackingconfig command to enable message tracking.
B. Generate a system report.
C. Review the log files.
D. Perform a trace.

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_A

NEW QUESTION 37
- (Exam Topic 1)
A mall provides security services to customers with a shared appliance. The mall wants separation of management on the shared appliance. Which ASA deployment mode meets these needs?

A. routed mode
B. transparent mode
C. multiple context mode
D. multiple zone mode

Answer: C

NEW QUESTION 40
- (Exam Topic 1)
Which license is required for Cisco Security Intelligence to work on the Cisco Next Generation Intrusion Prevention System?

A. control
B. malware

C. URL filtering
D. protect

Answer: D

NEW QUESTION 42
- (Exam Topic 1)
Which deployment model is the most secure when considering risks to cloud adoption?

A. Public Cloud
B. Hybrid Cloud
C. Community Cloud
D. Private Cloud

Answer: D

NEW QUESTION 44
- (Exam Topic 1)
An MDM provides which two advantages to an organization with regards to device management? (Choose two)

A. asset inventory management
B. allowed application management
C. Active Directory group policy management
D. network device management
E. critical device management

Answer: AB

NEW QUESTION 45
- (Exam Topic 1)
Which exfiltration method does an attacker use to hide and encode data inside DNS requests and queries?

A. DNS tunneling
B. DNSCrypt
C. DNS security
D. DNSSEC

Answer: A

Explanation:
DNS Tunneling is a method of cyber attack that encodes the data of other programs or protocols in DNSqueries and responses. DNS tunneling often includes data payloads that can be added to an attacked DNSserver and used to control a remote server and applications.

NEW QUESTION 50
- (Exam Topic 1)
Which two fields are defined in the NetFlow flow? (Choose two)

A. type of service byte
B. class of service bits
C. Layer 4 protocol type
D. destination port
E. output logical interface

Answer: AD

Explanation:
Cisco standard NetFlow version 5 defines a flow as a unidirectional sequence of packets that all share seven values which define a unique key for the flow:+ Ingress interface (SNMP ifIndex)+ Source IP address+ Destination IP address+ IP protocol+ Source port for UDP or TCP, 0 for other protocols+ Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols+ IP Type of ServiceNote: A flow is a unidirectional series of packets between a given source and destination.

NEW QUESTION 53
- (Exam Topic 1)
What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services? (Choose two)

A. multiple factor auth
B. local web auth
C. single sign-on
D. central web auth
E. TACACS+

Answer: BD

NEW QUESTION 57
- (Exam Topic 1)
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)

A. Patch for cross-site scripting.
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.
D. Install a spam and virus email filter.
E. Protect systems with an up-to-date antimalware program

Answer: DE

Explanation:
Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputablesource. It is usually done through email. The goal is to steal sensitive data like credit card and login information,or to install malware on the victim's machine.

NEW QUESTION 62
- (Exam Topic 1)
What must be used to share data between multiple security products?

A. Cisco Rapid Threat Containment
B. Cisco Platform Exchange Grid
C. Cisco Advanced Malware Protection
D. Cisco Stealthwatch Cloud

Answer: B

NEW QUESTION 66
- (Exam Topic 1)
Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?

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

Answer: A

NEW QUESTION 67
- (Exam Topic 1)
Which two features of Cisco Email Security can protect your organization against email threats? (Choose two)

A. Time-based one-time passwords
B. Data loss prevention
C. Heuristic-based filtering
D. Geolocation-based filtering
E. NetFlow

Answer: BD

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA

NEW QUESTION 72
- (Exam Topic 1)
What is a characteristic of Firepower NGIPS inline deployment mode?

A. ASA with Firepower module cannot be deployed.
B. It cannot take actions such as blocking traffic.
C. It is out-of-band from traffic.
D. It must have inline interface pairs configured.

Answer: D

NEW QUESTION 77
- (Exam Topic 1)
Which benefit does endpoint security provide the overall security posture of an organization?

A. It streamlines the incident response process to automatically perform digital forensics on the endpoint.
B. It allows the organization to mitigate web-based attacks as long as the user is active in the domain.
C. It allows the organization to detect and respond to threats at the edge of the network.
D. It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.

Answer: D

NEW QUESTION 81
- (Exam Topic 1)
In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

A. Smurf
B. distributed denial of service
C. cross-site scripting
D. rootkit exploit

Answer: C

Explanation:
Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on.For example the code below is written in hex: <ahref=javascript:alert&#x28'XSS')>Click Hereis equivalent to:Click HereNote: In the format "&#xhhhh", hhhh is the code point in hexadecimal form.

NEW QUESTION 85
- (Exam Topic 1)
What is a characteristic of a bridge group in ASA Firewall transparent mode?

A. It includes multiple interfaces and access rules between interfaces are customizable
B. It is a Layer 3 segment and includes one port and customizable access rules
C. It allows ARP traffic with a single access rule
D. It has an IP address on its BVI interface and is used for management traffic

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-generalconfig/intro-fw.h BVI interface is not used for management purpose. But we can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA.

NEW QUESTION 87
- (Exam Topic 1)
Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

A. Nexus
B. Stealthwatch
C. Firepower
D. Tetration

Answer: D

NEW QUESTION 89
- (Exam Topic 1)
Which IPS engine detects ARP spoofing?

A. Atomic ARP Engine
B. Service Generic Engine
C. ARP Inspection Engine
D. AIC Engine

Answer: A

NEW QUESTION 90
- (Exam Topic 1)
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

Answer: D

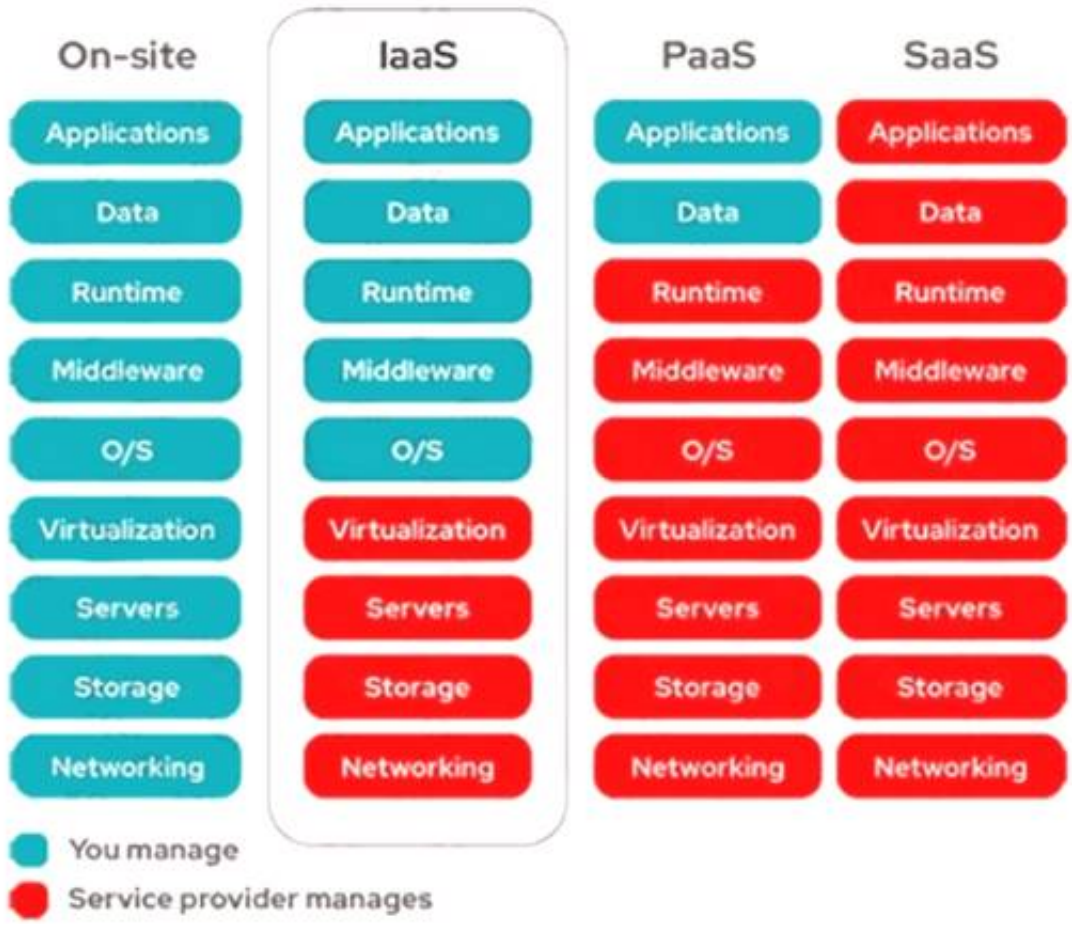
Explanation:
Reference: https://docs.umbrella.com/deployment-umbrella/docs/manage-logs

NEW QUESTION 91
- (Exam Topic 1)
In which cloud services model is the tenant responsible for virtual machine OS patching?

A. IaaS
B. UCaaS
C. PaaS
D. SaaS

Answer: A

Explanation:
Only in On-site (on-premises) and IaaS we (tenant) manage O/S (Operating System).



NEW QUESTION 94
- (Exam Topic 1)
Which command enables 802.1X globally on a Cisco switch?

A. dot1x system-auth-control
B. dot1x pae authenticator
C. authentication port-control aut
D. aaa new-model

Answer: A

NEW QUESTION 99
- (Exam Topic 1)
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

NEW QUESTION 104
- (Exam Topic 1)
Which two behavioral patterns characterize a ping of death attack? (Choose two)

A. The attack is fragmented into groups of 16 octets before transmission.
B. The attack is fragmented into groups of 8 octets before transmission.
C. Short synchronized bursts of traffic are used to disrupt TCP connections.
D. Malformed packets are used to crash systems.
E. Publicly accessible DNS servers are typically used to execute the attack.

Answer: BD

Explanation:
Ping of Death (PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash,destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.A correctly-formed ping packet is typically 56 bytes in size, or 64 bytes when the ICMP header is considered,and 84 including Internet Protocol version 4 header. However, any IPv4 packet (including pings) may be as large as 65,535 bytes. Some computer systems were never designed to properly handle a ping packet larger than the maximum packet size because it violates the Internet Protocol documentedLike other large but well-formed packets, a ping of death is fragmented into groups of 8 octets beforetransmission. However, when the target computer reassembles the malformed packet, a buffer overflow can occur, causing a system crash and potentially allowing the injection of malicious code.

NEW QUESTION 108
- (Exam Topic 1)
Refer to the exhibit.

```
HQ_Router(config)#username admin5 privilege 5
HQ_Router(config)#privilege interface level 5
shutdown
HQ_Router(config)#privilege interface level 5 ip
HQ_Router(config)#privilege interface level 5
description
```

A network administrator configures command authorization for the admin5 user. What is the admin5 user able to do on HQ_Router after this configuration?

A. set the IP address of an interface
B. complete no configurations
C. complete all configurations
D. add subinterfaces

Answer: B

Explanation:
The user “admin5” was configured with privilege level 5. In order to allow configuration (enter globalconfiguration mode), we must type this command:(config)#privilege exec level 5 configure terminalWithout this command, this user cannot do any configuration.Note: Cisco IOS supports privilege levels from 0 to 15, but the privilege levels which are used by default are privilege level 1 (user EXEC) and level privilege 15 (privilege EXEC)

NEW QUESTION 113
- (Exam Topic 1)
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. Same Site cookie attribute should not be used.

Answer: AB

NEW QUESTION 115
- (Exam Topic 1)
When wired 802.1X authentication is implemented, which two components are required? (Choose two)

A. authentication server: Cisco Identity Service Engine
B. supplicant: Cisco AnyConnect ISE Posture module
C. authenticator: Cisco Catalyst switch
D. authenticator: Cisco Identity Services Engine
E. authentication server: Cisco Prime Infrastructure

Answer: AC

NEW QUESTION 116
- (Exam Topic 1)
Which Cisco security solution protects remote users against phishing attacks when they are not connected to the VPN?

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

Answer: B

Explanation:
Cisco Umbrella protects users from accessing malicious domains by proactively analyzing and blocking unsafe destinations – before a connection is ever made. Thus it can protect from phishing attacks by blocking suspicious domains when users click on the given links that an attacker sent. Cisco Umbrella roaming protects your employees even when they are off the VPN.

NEW QUESTION 118
- (Exam Topic 1)
Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and
prioritize application traffic?

A. Cisco Security Intelligence
B. Cisco Application Visibility and Control
C. Cisco Model Driven Telemetry
D. Cisco DNA Center

Answer: B

Explanation:

Reference:
https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/guide/avc-user-guide/avc_tech_overview.html

NEW QUESTION 119
- (Exam Topic 1)
In a PaaS model, which layer is the tenant responsible for maintaining and patching?

A. hypervisor
B. virtual machine
C. network
D. application

Answer: D

NEW QUESTION 121
- (Exam Topic 1)
What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?

A. It tracks flow-create, flow-teardown, and flow-denied events.
B. It provides stateless IP flow tracking that exports all records of a specific flow.
C. It tracks the flow continuously and provides updates every 10 seconds.
D. Its events match all traffic classes in parallel.

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/ monitor-nsel.html

NEW QUESTION 122
- (Exam Topic 1)
What is the difference between deceptive phishing and spear phishing?

A. Deceptive phishing is an attacked aimed at a specific user in the organization who holds a C-level role.
B. A spear phishing campaign is aimed at a specific person versus a group of people.
C. Spear phishing is when the attack is aimed at the C-level executives of an organization.
D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Answer: B

Explanation:

In deceptive phishing, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.
Spear phishing is carefully designed to get a single recipient to respond. Criminals select an individual target within an organization, using social media and other public information – and craft a fake email tailored for that person.

NEW QUESTION 123
- (Exam Topic 1)
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

NEW QUESTION 127
- (Exam Topic 1)
What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two)

A. data exfiltration
B. command and control communication
C. intelligent proxy
D. snort
E. URL categorization

Answer: AB

Explanation:
Reference:
https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-aglance-c45-73655

NEW QUESTION 132
- (Exam Topic 1)

Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?

A. PaaS
B. XaaS
C. IaaS
D. SaaS

Answer: A

Explanation:
Reference: CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide

NEW QUESTION 137
- (Exam Topic 1)
Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two)

A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS
B. Cisco FTDv with one management interface and two traffic interfaces configured
C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises
D. Cisco FTDv with two management interfaces and one traffic interface configured
E. Cisco FTDv configured in routed mode and IPv6 configured

Answer: AC

NEW QUESTION 142
- (Exam Topic 3)
An engineer recently completed the system setup on a Cisco WSA Which URL information does the system send to SensorBase Network servers?

A. Summarized server-name information and MD5-hashed path information
B. complete URL,without obfuscating the path segments
C. URL information collected from clients that connect to the Cisco WSA using Cisco AnyConnect
D. none because SensorBase Network Participation is disabled by default

Answer: B

NEW QUESTION 144
- (Exam Topic 3)
Which algorithm is an NGE hash function?

A. HMAC
B. SHA-1
C. MD5
D. SISHA-2

Answer: D

NEW QUESTION 148
- (Exam Topic 3)
Which open source tool does Cisco use to create graphical visualizations of network telemetry on Cisco IOS XE devices?

A. InfluxDB
B. Splunk
C. SNMP
D. Grafana

Answer: D

NEW QUESTION 153
- (Exam Topic 3)
Why is it important for the organization to have an endpoint patching strategy?

A. so the organization can identify endpoint vulnerabilities
B. so the internal PSIRT organization is aware of the latest bugs
C. so the network administrator is notified when an existing bug is encountered
D. so the latest security fixes are installed on the endpoints

Answer: D

NEW QUESTION 154
- (Exam Topic 3)
An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users. Which action accomplishes this goal?

A. Restrict access to only websites with trusted third-party signed certificates.
B. Modify the user’s browser settings to suppress errors from Cisco Umbrella.
C. Upload the organization root CA to Cisco Umbrella.

D. Install the Cisco Umbrella root CA onto the user's device.

Answer: D

NEW QUESTION 156
- (Exam Topic 3)
A company has 5000 Windows users on its campus. Which two precautions should IT take to prevent WannaCry ransomware from spreading to all clients? (Choose two.)

A. Segment different departments to different IP blocks and enable Dynamic ARp inspection on all VLANs
B. Ensure that noncompliant endpoints are segmented off to contain any potential damage.
C. Ensure that a user cannot enter the network of another department.
D. Perform a posture check to allow only network access to (hose Windows devices that are already patched.
E. Put all company users in the trusted segment of NGFW and put all servers to the DMZ segment of the Cisco NGF
F. ni

Answer: BD

NEW QUESTION 159
- (Exam Topic 3)
An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1 1 11 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

NEW QUESTION 160
- (Exam Topic 3)
Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'
```

What does the API key do while working with https://api.amp.cisco.com/v1/computers?

A. displays client ID
B. HTTP authorization
C. Imports requests
D. HTTP authentication

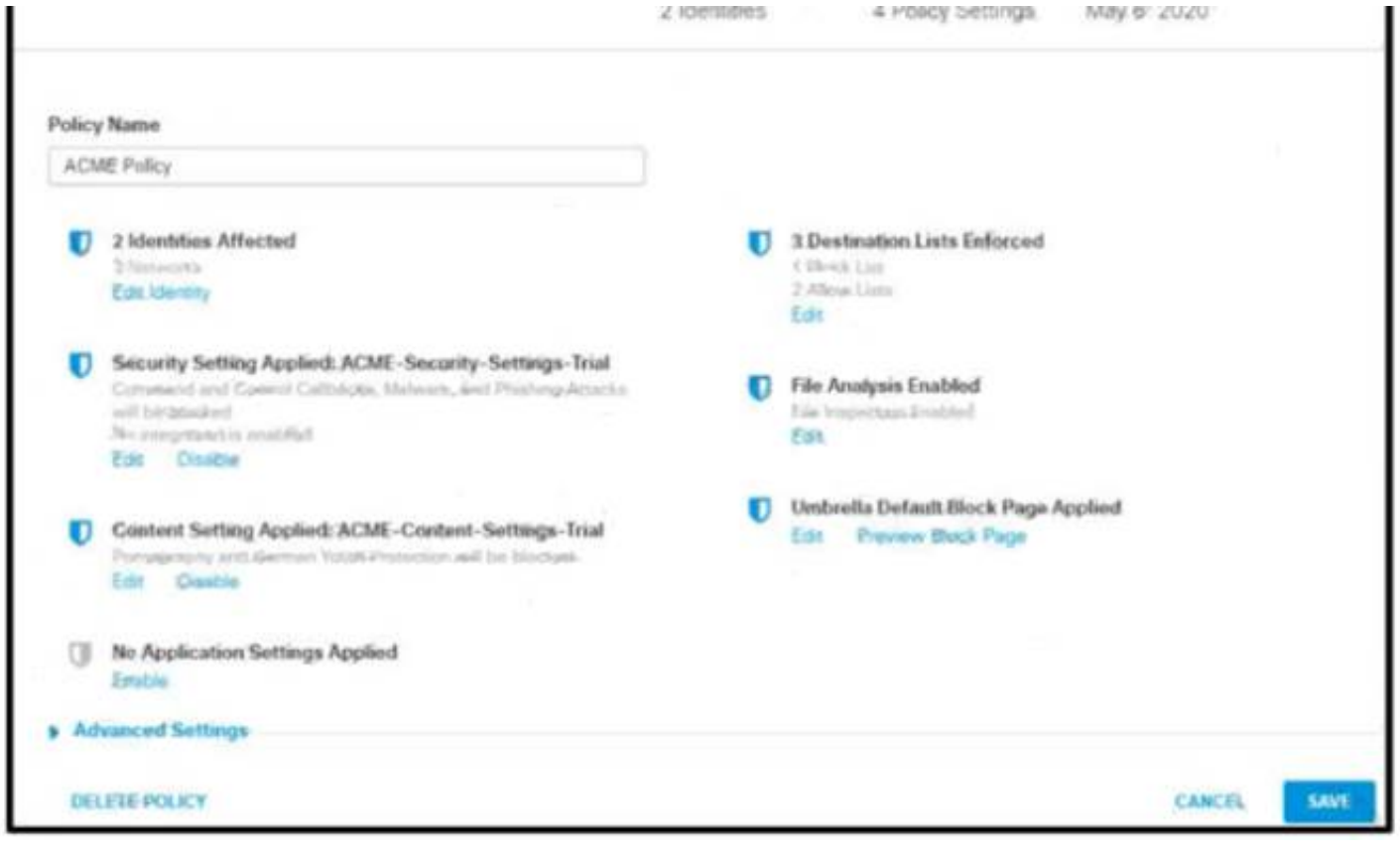
Answer: D

NEW QUESTION 164
- (Exam Topic 3)
When a transparent authentication fails on the Web Security Appliance, which type of access does the end user get?

A. guest
B. limited Internet
C. blocked
D. full Internet

Answer: C

NEW QUESTION 168
- (Exam Topic 3)
Refer to the exhibit.



How does Cisco Umbrella manage traffic that is directed toward risky domains?

A. Traffic is proximed through the intelligent proxy.
B. Traffic is managed by the security settings and blocked.
C. Traffic is managed by the application settings, unhandled and allowed.
D. Traffic is allowed but logged.

Answer: B

NEW QUESTION 172
- (Exam Topic 3)
Which technology provides a combination of endpoint protection endpoint detection, and response?

A. Cisco AMP
B. Cisco Talos
C. Cisco Threat Grid
D. Cisco Umbrella

Answer: A

NEW QUESTION 174
- (Exam Topic 3)
Refer to the exhibit.

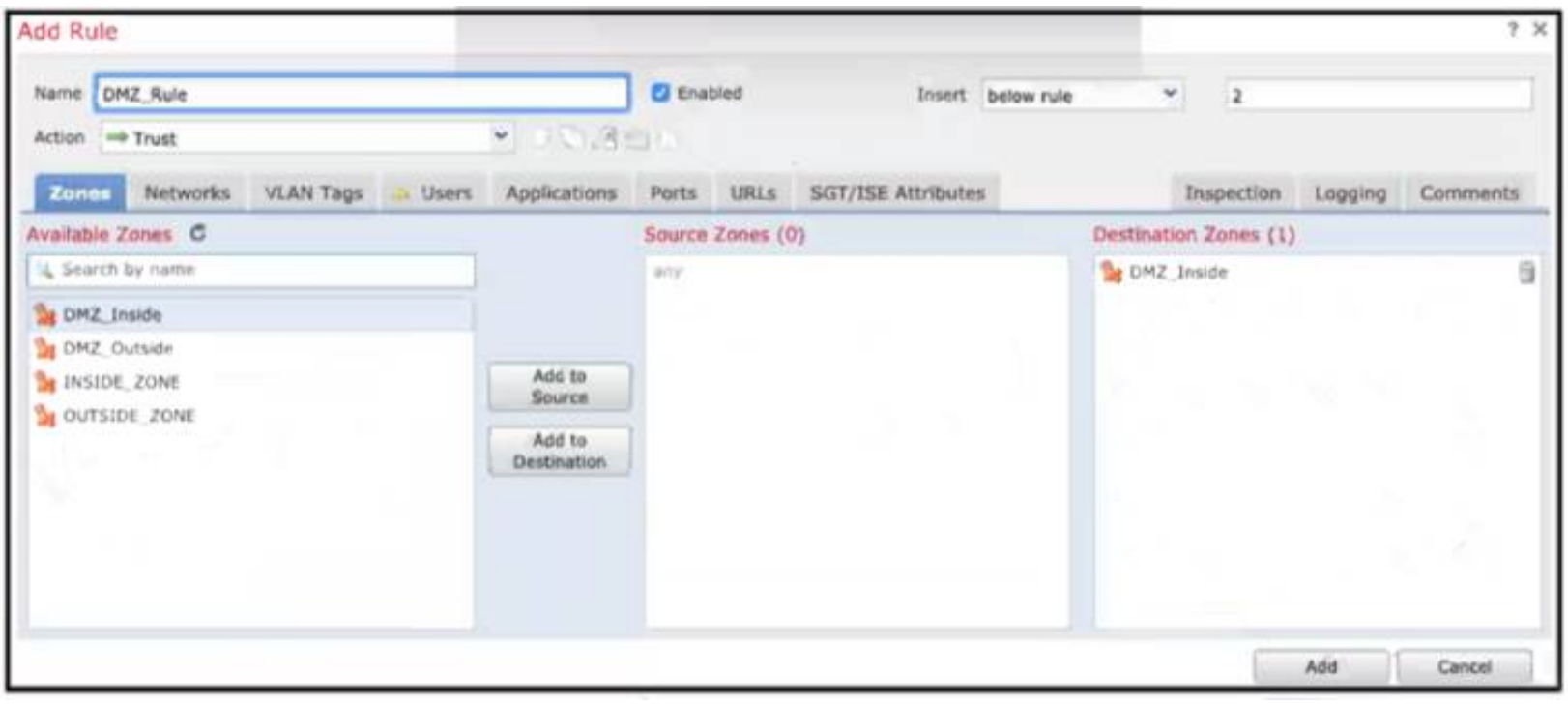
```
interface GigabitEthernet1/0/18
switchport access vlan 41
switchport mode access
switchport voice vlan 44
device-tracking attach-policy IPDT_MAX_10
authentication periodic
authentication timer reauthenticate server
access-session host-mode multi-domain
access-session port-control auto
dot1x pae authenticator
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 gaining access.
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: D

NEW QUESTION 175
- (Exam Topic 3)



Refer to the exhibit When configuring this access control rule in Cisco FMC, what happens with the traffic destined to the DMZjnside zone once the configuration is deployed?

A. All traffic from any zone to the DMZ_inside zone will be permitted with no further inspection
B. No traffic will be allowed through to the DMZ_inside zone regardless of if it's trusted or not
C. All traffic from any zone will be allowed to the DMZ_inside zone only after inspection
D. No traffic will be allowed through to the DMZ_inside zone unless it's already trusted

Answer: A

NEW QUESTION 179
- (Exam Topic 3)
Which solution should be leveraged for secure access of a CI/CD pipeline?

A. Duo Network Gateway
B. remote access client
C. SSL WebVPN
D. Cisco FTD network gateway

Answer: A

NEW QUESTION 183
- (Exam Topic 3)
Which Talos reputation center allows for tracking the reputation of IP addresses for email and web traffic?

A. IP and Domain Reputation Center
B. File Reputation Center
C. IP Slock List Center
D. AMP Reputation Center

Answer: A

NEW QUESTION 185
- (Exam Topic 3)
What does Cisco ISE use to collect endpoint attributes that are used in profiling?

A. probes
B. posture assessment
C. Cisco AnyConnect Secure Mobility Client
D. Cisco pxGrid

Answer: A

Explanation:
Reference:
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/2-6/admin_guide

NEW QUESTION 190
- (Exam Topic 3)
Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks? (Choose two.)

A. blocks malicious websites and adds them to a block list
B. does a real-time user web browsing behavior analysis
C. provides a defense for on-premises email deployments
D. uses a static algorithm to determine malicious
E. determines if the email messages are malicious

Answer: CE

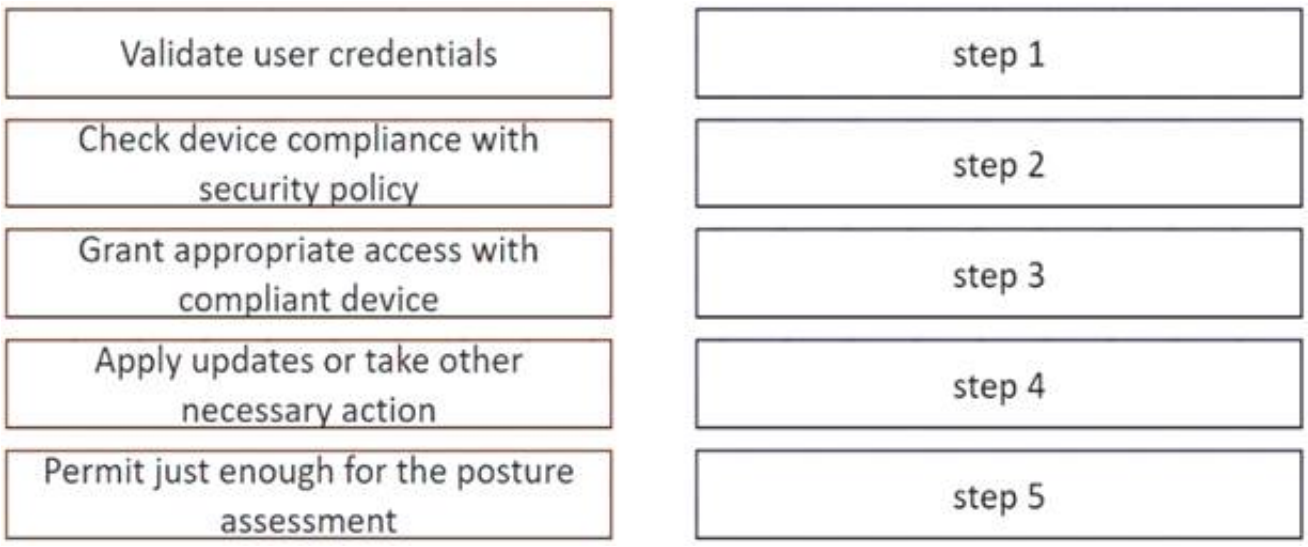
NEW QUESTION 194
- (Exam Topic 3)
Which type of DNS abuse exchanges data between two computers even when there is no direct connection?

A. Malware installation
B. Command-and-control communication
C. Network footprinting
D. Data exfiltration

Answer: D

Explanation:
Reference: https://www.netsurion.com/articles/5-types-of-dns-attacks-and-how-to-detect-them

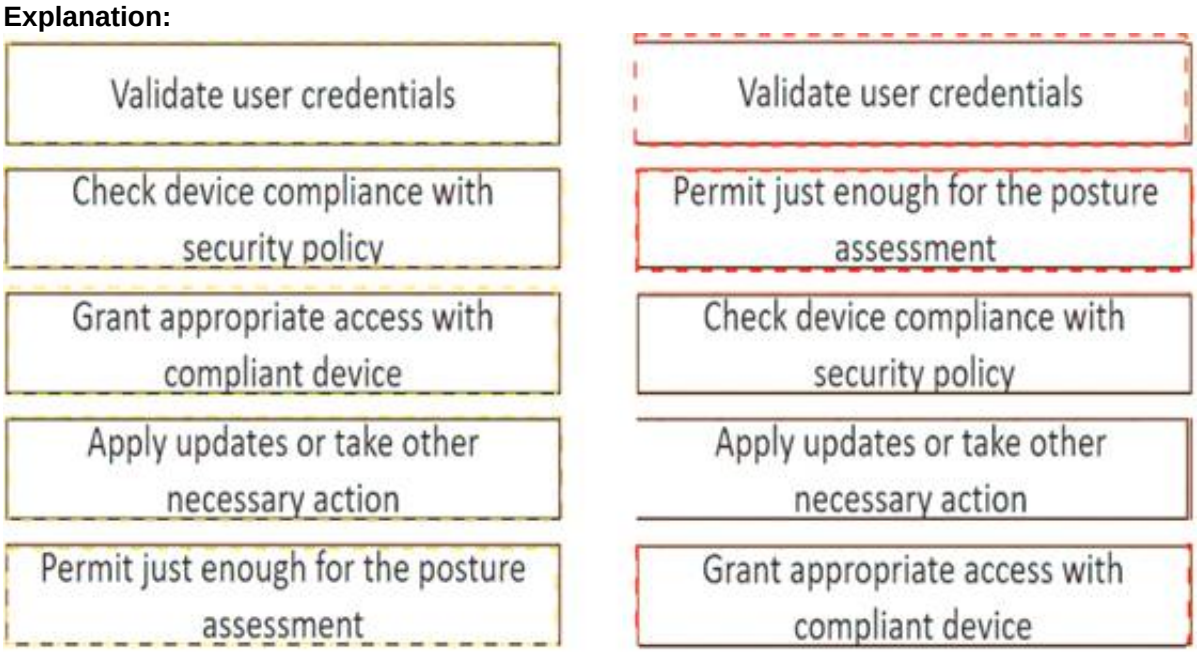
NEW QUESTION 197
- (Exam Topic 3)
Drag and drop the posture assessment flow actions from the left into a sequence on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 202
- (Exam Topic 3)
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 run Cisco AsyncOS 10.0 or greater.
B. The hosts must run different versions of Cisco AsyncOS.
C. The hosts must have access to the same defined network.
D. The hosts must use a different datastore than the virtual appliance.

Answer: C

NEW QUESTION 206
- (Exam Topic 3)
What are two ways that Cisco Container Platform provides value to customers who utilize cloud service providers? (Choose two.)

A. Allows developers to create code once and deploy to multiple clouds
B. helps maintain source code for cloud deployments

C. manages Docker containers
D. manages Kubernetes clusters
E. Creates complex tasks for managing code

Answer: AE

NEW QUESTION 209
- (Exam Topic 3)
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: D

NEW QUESTION 214
- (Exam Topic 3)
Which DevSecOps implementation process gives a weekly or daily update instead of monthly or quarterly in the applications?

A. Orchestration
B. CI/CD pipeline
C. Container
D. Security

Answer: B

Explanation:
Reference: https://devops.com/how-to-implement-an-effective-ci-cd-pipeline/

NEW QUESTION 218
- (Exam Topic 3)
An administrator is establishing a new site-to-site VPN connection on a Cisco IOS router. The organization needs to ensure that the ISAKMP key on the hub is used only for terminating traffic from the IP address of 172.19.20.24. Which command on the hub will allow the administrator to accomplish this?

A. crypto ca identity 172.19.20.24
B. crypto isakmp key Cisco0123456789 172.19.20.24
C. crypto enrollment peer address 172.19.20.24
D. crypto isakmp identity address 172.19.20.24

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp3880782430The command “crypto enrollment peer address” is not valid either.The command “crypto ca identity …” is only used to declare a trusted CA for the router and puts you in the caidentity configuration mode. Also it should be followed by a name, not an IP address. For example: “crypto caidentity CA-Server” -> Answer A is not correct.Only answer B is the best choice left.

NEW QUESTION 220
- (Exam Topic 3)
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. Transport mode
B. Forward file
C. PAC file
D. Bridge mode

Answer: C

Explanation:
A Proxy Auto-Configuration (PAC) file is a JavaScript function definition that determines whether web browserrequests (HTTP, HTTPS, and FTP) go direct to the destination or are forwarded to a web proxy server.PAC files are used to support explicit proxy deployments in which client browsers are explicitly configured tosend traffic to the web proxy. The big advantage of PAC files is that they are usually relatively easy to createand maintain.

NEW QUESTION 224
- (Exam Topic 3)
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 reputation scores of 1-3 will be blocked.
B. Only URLs for botnets with a reputation score of 3 will be blocked.
C. Only URLs for botnets with reputation scores of 3-5 will be blocked.
D. Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked.

Answer: A

NEW QUESTION 229
- (Exam Topic 3)
What are two things to consider when using PAC files with the Cisco WSA? (Choose two.)

A. If the WSA host port is changed, the default port redirects web traffic to the correct port automatically.
B. PAC files use if-else statements to determine whether to use a proxy or a direct connection for traffic between the PC and the host.
C. The WSA hosts PAC files on port 9001 by default.
D. The WSA hosts PAC files on port 6001 by default.
E. By default, they direct traffic through a proxy when the PC and the host are on the same subnet.

Answer: AD

NEW QUESTION 231
- (Exam Topic 3)
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: A

NEW QUESTION 232
- (Exam Topic 3)
Drag and drop the exploits from the left onto the type of security vulnerability on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 233
- (Exam Topic 3)
Drag and drop the features of Cisco ASA with Firepower from the left onto the benefits on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Full Context Awareness - policy enforcement NGIPS - threat prevention
AMP - real-time
Collective Sec Intel - Detection, blocking an remediation

NEW QUESTION 236
- (Exam Topic 3)
Which type of attack is MFA an effective deterrent for?

A. ping of death
B. phishing
C. teardrop
D. syn flood

Answer: B

NEW QUESTION 240
- (Exam Topic 3)
What is the purpose of the Cisco Endpoint IoC feature?

A. It provides stealth threat prevention.
B. lt is a signature-based engine.
C. lt is an incident response tool
D. It provides precompromise detection.

Answer: C

Explanation:
https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Secure_Mana

NEW QUESTION 241
- (Exam Topic 3)
What is a difference between a DoS attack and a DDoS attack?

A. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where multiple systems target a single system with a DoS attack
B. A DoS attack is where a computer is used to flood a server with TCP and UDP packets whereas a DDoS attack is where a computer is used to flood multiple servers that are distributed over a LAN
C. A DoS attack is where a computer is used to flood a server with UDP packets whereas a DDoS attack is where a computer is used to flood a server with TCP packets
D. A DoS attack is where a computer is used to flood a server with TCP packets whereas a DDoS attack is where a computer is used to flood a server with UDP packets

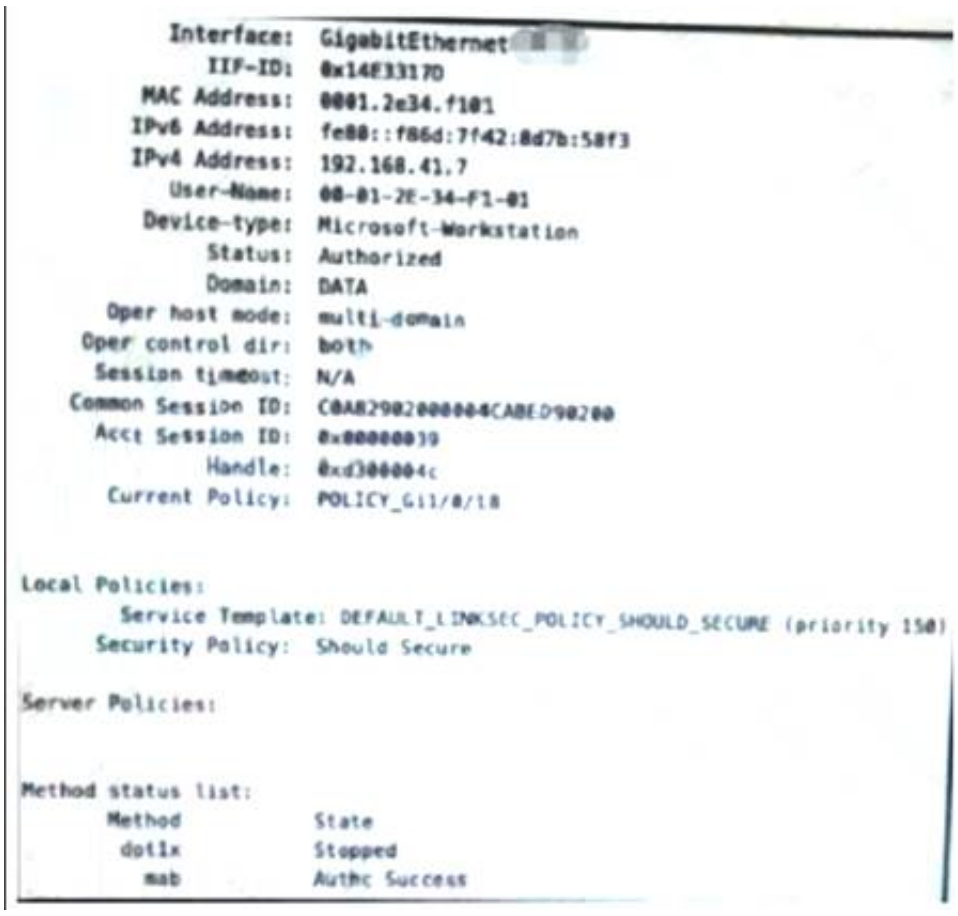
Answer: A

NEW QUESTION 244
- (Exam Topic 3)
An administrator configures a new destination list in Cisco Umbrella so that the organization can block specific domains for its devices. What should be done to ensure that all subdomains of domain.com are blocked?

A. Configure the *.com address in the block list.
B. Configure the *.domain.com address in the block list
C. Configure the *.domain.com address in the block list
D. Configure the domain.com address in the block list

Answer: C

NEW QUESTION 247
- (Exam Topic 3)
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 authentication enable default enable
C. aaa authorization network default group ise
D. aaa authorization exec default ise

Answer: C

NEW QUESTION 249
- (Exam Topic 3)
Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)

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

Answer: AE

NEW QUESTION 253
- (Exam Topic 3)
Which two authentication protocols are supported by the Cisco WSA? (Choose two.)

A. WCCP
B. NTLM
C. TLS
D. SSL
E. LDAP

Answer: BE

NEW QUESTION 254
- (Exam Topic 3)
Which API method and required attribute are used to add a device into Cisco DNA Center with the native API?

A. GET and serialNumber
B. userSudiSerlalNos and deviceInfo
C. POST and name
D. lastSyncTime and pid

Answer: A

NEW QUESTION 257
- (Exam Topic 3)
In which two ways does the Cisco Advanced Phishing Protection solution protect users? (Choose two.)

A. It prevents use of compromised accounts and social engineering.
B. It prevents all zero-day attacks coming from the Internet.
C. It automatically removes malicious emails from users' inbox.
D. It prevents trojan horse malware using sensors.
E. It secures all passwords that are shared in video conferences.

Answer: BC

NEW QUESTION 259
- (Exam Topic 3)
An engineer must modify a policy to block specific addresses using Cisco Umbrella. The policy is created already and is actively u: of the default policy elements. What else must be done to accomplish this task?

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

Answer: B

NEW QUESTION 261
- (Exam Topic 3)
What are two functions of TAXII in threat intelligence sharing? (Choose two.)

A. determines the "what" of threat intelligence
B. Supports STIX information
C. allows users to describe threat motivations and abilities
D. exchanges trusted anomaly intelligence information
E. determines how threat intelligence information is relayed

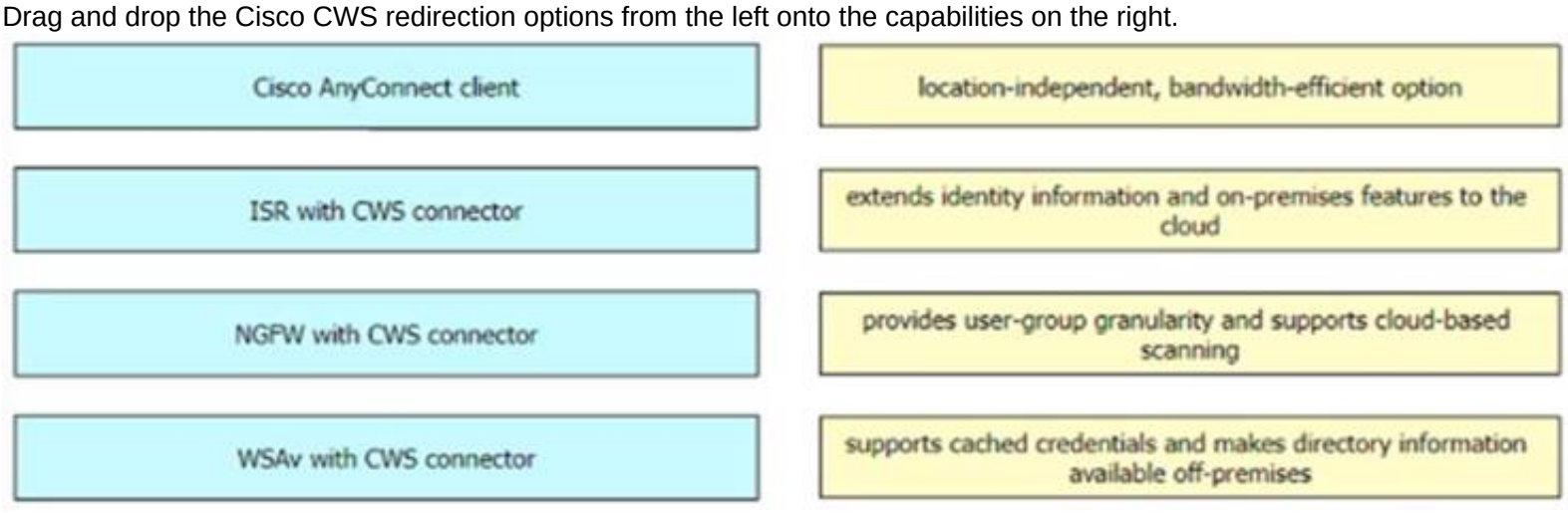
Answer: BE

NEW QUESTION 266
- (Exam Topic 3)
What is the result of the ACME-Router(config)#login block-for 100 attempts 4 within 60 command on a Cisco IOS router?

A. lf four log in attempts fail in 100 seconds, wait for 60 seconds to next log in prompt.
B. After four unsuccessful log in attempts, the line is blocked for 100 seconds and only permit IP addresses are permitted in ACL
C. After four unsuccessful log in attempts, the line is blocked for 60 seconds and only permit IP addresses are permitted in ACL1
D. If four failures occur in 60 seconds, the router goes to quiet mode for 100 seconds.

Answer: D

NEW QUESTION 267
- (Exam Topic 3)
Drag and drop the Cisco CWS redirection options from the left onto the capabilities on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://www.westconcomstor.com/medias/CWS-data-sheet-c78-729637-1-.pdf?context=bWFzdGVyfHJvb3R8M

NEW QUESTION 272
- (Exam Topic 3)

A university policy must allow open access to resources on the Internet for research, but internal workstations are exposed to malware. Which Cisco AMP feature allows the engineering team to determine whether a file is installed on a selected few workstations?

A. file prevalence
B. file discovery
C. file conviction
D. file manager

Answer: A

NEW QUESTION 277
- (Exam Topic 3)
Which two protocols must be configured to authenticate end users to the Cisco WSA? (Choose two.)

A. TACACS+
B. CHAP
C. NTLMSSP
D. RADIUS
E. Kerberos

Answer: AD

NEW QUESTION 282
- (Exam Topic 3)
An engineer is trying to decide whether to use Cisco Umbrella, Cisco CloudLock, Cisco Stealthwatch, or Cisco AppDynamics Cloud Monitoring for visibility into data transfers as well as protection against data exfiltration Which solution best meets these requirements?

A. Cisco CloudLock
B. Cisco AppDynamics Cloud Monitoring
C. Cisco Umbrella
D. Cisco Stealthwatch

Answer: D

NEW QUESTION 283
- (Exam Topic 3)
Which type of encryption uses a public key and private key?

A. Asymmetric
B. Symmetric
C. Linear
D. Nonlinear

Answer: A

NEW QUESTION 287
- (Exam Topic 3)
An administrator is configuring N I P on Cisco ASA via ASDM and needs to ensure that rogue NTP servers cannot insert themselves as the authoritative time source Which two steps must be taken to accomplish this task? (Choose two)

A. Specify the NTP version
B. Configure the NTP stratum
C. Set the authentication key
D. Choose the interface for syncing to the NTP server
E. Set the NTP DNS hostname

Answer: CD

NEW QUESTION 289
- (Exam Topic 3)
Which Cisco Firewall solution requires zone definition?

A. CBAC
B. Cisco AMP
C. ZBFW
D. Cisco ASA

Answer: C

NEW QUESTION 292
- (Exam Topic 3)
Which encryption algorithm provides highly secure VPN communications?

A. 3DES
B. AES 256
C. AES 128
D. DES

Answer: B

NEW QUESTION 297
- (Exam Topic 3)
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: A

NEW QUESTION 301
- (Exam Topic 3)
How does Cisco Workload Optimization portion of the network do EPP solutions solely performance issues?

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

Answer: B

NEW QUESTION 305
- (Exam Topic 3)
Which Cisco security solution secures public, private, hybrid, and community clouds?

A. Cisco ISE
B. Cisco ASAv
C. Cisco Cloudlock
D. Cisco pxGrid

Answer: C

NEW QUESTION 310
- (Exam Topic 3)
An organization is implementing AAA for their users. They need to ensure that authorization is verified for every command that is being entered by the network administrator. Which protocol must be configured in order to provide this capability?

A. EAPOL
B. SSH
C. RADIUS
D. TACACS+

Answer: D

NEW QUESTION 315
- (Exam Topic 3)
What are two workload security models? (Choose two.)

A. SaaS
B. PaaS
C. off-premises
D. on-premises
E. IaaS

Answer: CD

NEW QUESTION 320
- (Exam Topic 3)
An engineer needs to configure an access control policy rule to always send traffic for inspection without using the default action. Which action should be configured for this rule?

A. monitor
B. allow
C. block
D. trust

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/acce the first three access control rules in the policy—Monitor, Trust, and Block—cannot inspect matching
traffic. Monitor rules track and log but do not inspect network traffic, so the system continues to match traffic

against additional rules to determine whether to permit or deny it
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/acce

NEW QUESTION 324
- (Exam Topic 3)
An administrator configures a Cisco WSA to receive redirected traffic over ports 80 and 443. The organization requires that a network device with specific WSA integration capabilities be configured to send the traffic to the WSA to proxy the requests and increase visibility, while making this invisible to the users. What must be done on the Cisco WSA to support these requirements?

A. Configure transparent traffic redirection using WCCP in the Cisco WSA and on the network device
B. Configure active traffic redirection using WPAD in the Cisco WSA and on the network device
C. Use the Layer 4 setting in the Cisco WSA to receive explicit forward requests from the network device
D. Use PAC keys to allow only the required network devices to send the traffic to the Cisco WSA

Answer: A

NEW QUESTION 326
- (Exam Topic 3)
Which feature within Cisco ISE verifies the compliance of an endpoint before providing access to the network?

A. Posture
B. Profiling
C. pxGrid
D. MAB

Answer: A

NEW QUESTION 329
- (Exam Topic 3)
What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.) The eDirectory client must be installed on each client workstation.

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

Answer: AB

Explanation:
Transparently identify users with authentication realms – This option is available when one or more authentication realms are configured to support transparent identification using one of the following authentication servers:
Active Directory – Create an NTLM or Kerberos authentication realm and enable transparent user identification. In addition, you must deploy a separate Active Directory agent such as Cisco's Context Directory Agent. For more information, see Transparent User Identification with Active Directory.
LDAP – Create an LDAP authentication realm configured as an eDirectory, andenable transparent user identification. For more information, see Transparent User Identification with LDAP.
Details:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGui

NEW QUESTION 334
- (Exam Topic 3)
Which two capabilities of Integration APIs are utilized with Cisco DNA center? (Choose two)

A. Upgrade software on switches and routers
B. Third party reporting
C. Connect to ITSM platforms
D. Create new SSIDs on a wireless LAN controller
E. Automatically deploy new virtual routers

Answer: BC

Explanation:
Reference:
https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/integration-api-westbound

NEW QUESTION 335
- (Exam Topic 3)
Refer to the exhibit.

```
"remarks" [],
"destinationService" {
"kind" serviceKind,
"value" destinationServic
},
"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()
```

Enter your search term

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

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

Answer: A

NEW QUESTION 336
- (Exam Topic 3)
What is a function of Cisco AMP for Endpoints?

A. It detects DNS attacks
B. It protects against web-based attacks
C. It blocks email-based attacks
D. It automates threat responses of an infected host

Answer: D

NEW QUESTION 340
- (Exam Topic 3)
What is an advantage of network telemetry over SNMP pulls?

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

Answer: D

NEW QUESTION 342
- (Exam Topic 3)
An engineer is configuring Dropbox integration with Cisco Cloudlock. Which action must be taken before granting API access in the Dropbox admin console?

A. Authorize Dropbox within the Platform settings in the Cisco Cloudlock portal.
B. Add Dropbox to the Cisco Cloudlock Authentication and API section in the Cisco Cloudlock portal.
C. Send an API request to Cisco Cloudlock from Dropbox admin portal.
D. Add Cisco Cloudlock to the Dropbox admin portal.

Answer: A

NEW QUESTION 345
- (Exam Topic 3)
What limits communication between applications or containers on the same node?

A. microsegmentation
B. container orchestration
C. microservicing
D. Software-Defined Access

Answer: D

NEW QUESTION 350
- (Exam Topic 3)
A network engineer is trying to figure out whether FlexVPN or DMVPN would fit better in their environment. They have a requirement for more stringent security multiple security associations for the connections, more efficient VPN establishment as well consuming less bandwidth. Which solution would be best for this and why?

A. DMVPN because it supports IKEv2 and FlexVPN does not
B. FlexVPN because it supports IKEv2 and DMVPN does not
C. FlexVPN because it uses multiple SAs and DMVPN does not
D. DMVPN because it uses multiple SAs and FlexVPN does not

Answer: C

Explanation:
FlexVPN supports IKEv2 -> Answer A is not correct.DMVPN supports both IKEv1 & IKEv2 -> Answer B is not correct.FlexVPN support multiple SAs -> Answer D is not correct.

NEW QUESTION 355
- (Exam Topic 3)
How does Cisco AMP for Endpoints provide next-generation protection?

A. It encrypts data on user endpoints to protect against ransomware.
B. It leverages an endpoint protection platform and endpoint detection and response.
C. It utilizes Cisco pxGrid, which allows Cisco AMP to pull threat feeds from threat intelligence centers.
D. It integrates with Cisco FTD devices.

Answer: B

NEW QUESTION 356
- (Exam Topic 3)
What is a description of microsegmentation?

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

Answer: B

NEW QUESTION 357
- (Exam Topic 3)
Which kind of API that is used with Cisco DNA Center provisions SSIDs, QoS policies, and update software versions on switches?

A. Integration
B. Intent
C. Event
D. Multivendor

Answer: B

NEW QUESTION 361
- (Exam Topic 3)
What provides total management for mobile and PC including managing inventory and device tracking, remote view, and live troubleshooting using the included native remote desktop support?

A. mobile device management
B. mobile content management
C. mobile application management
D. mobile access management

Answer: A

NEW QUESTION 365
- (Exam Topic 3)
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. SQL injection

D. cross-site scripting

Answer: D

NEW QUESTION 370
- (Exam Topic 3)
When NetFlow is applied to an interface, which component creates the flow monitor cache that is used to collect traffic based on the key and nonkey fields in the configured record?

A. records
B. flow exporter
C. flow sampler
D. flow monitor

Answer: D

NEW QUESTION 371
- (Exam Topic 3)
Which category includes DoS Attacks?

A. Virus attacks
B. Trojan attacks
C. Flood attacks
D. Phishing attacks

Answer: C

NEW QUESTION 374
- (Exam Topic 3)
Refer to the exhibit.

Consider that any feature of DNS requests, such as the length off the domain name and the number of subdomains, can be used to construct models of expected behavior to which observed values can be compared. Which type of malicious attack are these values associated with?

A. Spectre Worm
B. Eternal Blue Windows
C. Heartbleed SSL Bug
D. W32/AutoRun worm

Answer: D

NEW QUESTION 376
- (Exam Topic 3)
What is a feature of NetFlow Secure Event Logging?

A. It exports only records that indicate significant events in a flow.
B. It filters NSEL events based on the traffic and event type through RSVP.
C. It delivers data records to NSEL collectors through NetFlow over TCP only.
D. It supports v5 and v8 templates.

Answer: A

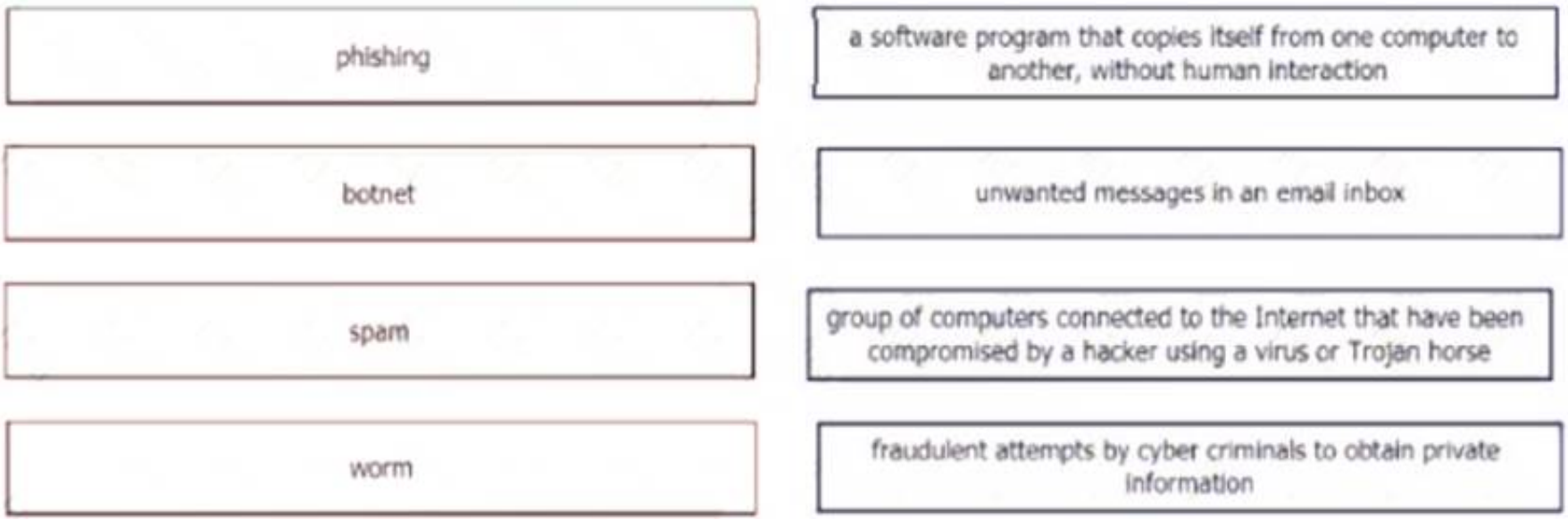
NEW QUESTION 381
- (Exam Topic 3)
Which DoS attack uses fragmented packets in an attempt to crash a target machine?

A. teardrop
B. smurf
C. LAND
D. SYN flood

Answer: A

Explanation:
Reference: https://www.radware.com/security/ddos-knowledge-center/ddospedia/teardrop-attack/

NEW QUESTION 384
- (Exam Topic 2)
Drag and drop the common security threats from the left onto the definitions on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
A picture containing application Description automatically generated

NEW QUESTION 387
- (Exam Topic 2)
What features does Cisco FTDv provide over ASAv?

A. Cisco FTDv runs on VMWare while ASAv does not
B. Cisco FTDv provides 1GB of firewall throughput while Cisco ASAv does not
C. Cisco FTDv runs on AWS while ASAv does not
D. Cisco FTDv supports URL filtering while ASAv does not

Answer: D

NEW QUESTION 390
- (Exam Topic 2)
Which type of API is being used when a security application notifies a controller within a software-defined network architecture about a specific security threat?

A. westbound AP
B. southbound API
C. northbound API
D. eastbound API

Answer: C

NEW QUESTION 394
- (Exam Topic 2)
Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated

NEW QUESTION 395
- (Exam Topic 2)
An organization wants to secure users, data, and applications in the cloud. The solution must be API-based and operate as a cloud-native CASB. Which solution must be used for this implementation?

A. Cisco Cloudlock
B. Cisco Cloud Email Security
C. Cisco Firepower Next-Generation Firewall
D. Cisco Umbrella

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45-738565.pdf

NEW QUESTION 398
- (Exam Topic 2)
An engineer is implementing NTP authentication within their network and has configured both the client and
server devices with the command ntp authentication-key 1 md5 Cisc392368270. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however it is unable to do so. Which command is required to enable the client to accept the server's authentication key?

A. ntp peer 1.1.1.1 key 1
B. ntp server 1.1.1.1 key 1
C. ntp server 1.1.1.2 key 1
D. ntp peer 1.1.1.2 key 1

Answer: B

Explanation:
To configure an NTP enabled router to require authentication when other devices connect to it, use thefollowing commands:NTP_Server(config)#ntp authentication-key 2 md5 securitytutNTP_Server(config)#ntp authenticateNTP_Server(config)#ntp trusted-key 2Then you must configure the same authentication-key on the client router:NTP_Client(config)#ntp authentication-key 2 md5 securitytutNTP_Client(config)#ntp authenticateNTP_Client(config)#ntp trusted-key 2NTP_Client(config)#ntp server 10.10.10.1 key 2Note: To configure a Cisco device as a NTP client, use the command ntp server <IP address>. For example:Router(config)#ntp server 10.10.10.1. This command will instruct the router to query 10.10.10.1 for the time.

NEW QUESTION 402
- (Exam Topic 2)
What is a benefit of performing device compliance?

A. Verification of the latest OS patches
B. Device classification and authorization
C. Providing multi-factor authentication
D. Providing attribute-driven policies

Answer: A

NEW QUESTION 405
- (Exam Topic 2)
Which type of protection encrypts RSA keys when they are exported and imported?

A. file
B. passphrase
C. NGE
D. nonexportable

Answer: B

NEW QUESTION 406
- (Exam Topic 2)
What is the benefit of installing Cisco AMP for Endpoints on a network?

A. It provides operating system patches on the endpoints for security.
B. It provides flow-based visibility for the endpoints network connections.
C. It enables behavioral analysis to be used for the endpoints.
D. It protects endpoint systems through application control and real-time scanning

Answer: D

NEW QUESTION 407
- (Exam Topic 2)
Which risk is created when using an Internet browser to access cloud-based service?

A. misconfiguration of infrastructure, which allows unauthorized access
B. intermittent connection to the cloud connectors
C. vulnerabilities within protocol
D. insecure implementation of API

Answer: D

NEW QUESTION 409
- (Exam Topic 2)
Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?

A. Encrypted Traffic Analytics
B. Threat Intelligence Director
C. Cognitive Threat Analytics
D. Cisco Talos Intelligence

Answer: B

NEW QUESTION 411
- (Exam Topic 2)
Refer to the exhibit.

```
ip dhcp snooping
ip dhcp snooping vlan 41,44
!
interface GigabitEthernet1/0/1
 description Uplink_To_Distro_Switch_g1/0/11
 switchport trunk native vlan 999
 switchport trunk allowed vlan 40,41,44
 switchport mode trunk
```

An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained. Which command should be configured on the switch interface in order to provide the user with network connectivity?

A. ip dhcp snooping verify mac-address
B. ip dhcp snooping limit 41
C. ip dhcp snooping vlan 41
D. ip dhcp snooping trust

Answer: D

Explanation:
To understand DHCP snooping we need to learn about DHCP spoofing attack first.
DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a “man-in-the-middle”.The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is “closer” than the DHCP Server then he doesn’t need to do anything. Or he can DoS the DHCP Server so that it can’t send the DHCP Response.DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature thatdetermines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.
Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.
The port connected to a DHCP server should be configured as trusted port with the “ip dhcp snooping trust” command. Other ports connecting to hosts are untrusted ports by default.
In this question, we need to configure the uplink to “trust” (under interface Gi1/0/1) as shown below.

NEW QUESTION 413
- (Exam Topic 2)
What is the difference between Cross-site Scripting and SQL Injection, attacks?

A. Cross-site Scripting is an attack where code is injected into a database, whereas SQL Injection is an attack where code is injected into a browser.
B. Cross-site Scripting is a brute force attack targeting remote sites, whereas SQL Injection is a social engineering attack.
C. Cross-site Scripting is when executives in a corporation are attacked, whereas SQL Injection is when a database is manipulated.
D. Cross-site Scripting is an attack where code is executed from the server side, whereas SQL Injection is an attack where code is executed from the client side.

Answer: A

Explanation:
Answer B is not correct because Cross-site Scripting (XSS) is not a brute force attack.Answer C is not correct because the statement “Cross-site Scripting is when executives in a corporation are attacked” is not true. XSS is a client-side vulnerability that targets other application users.Answer D is not correct because the statement “Cross-site Scripting is an attack where code is executed from the server side”. In fact, XSS is a method that exploits website vulnerability by injecting scripts that will run at client’s side.Therefore only answer A is left. In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites whereattackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POSTparameters.Note: The main difference between a SQL and XSS injection attack is that 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.

NEW QUESTION 418
- (Exam Topic 2)
What is provided by the Secure Hash Algorithm in a VPN?

A. integrity
B. key exchange
C. encryption

D. authentication

Answer: A

Explanation:
Reference: https://www.ciscopress.com/articles/article.asp?p=24833&seqNum=4

NEW QUESTION 422
- (Exam Topic 2)
A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an undetermined verdict. What is causing this issue?

A. The policy was created to send a message to quarantine instead of drop
B. The file has a reputation score that is above the threshold
C. The file has a reputation score that is below the threshold
D. The policy was created to disable file analysis

Answer: D

Explanation:
Maybe the “newly installed service” in this Qmentions about Advanced Malware Protection (AMP) which can be used along with ESA. AMP allows superior protection across the attack continuum.+ File Reputation – captures a fingerprint of each file as it traverses the ESA and sends it to AMP’s cloudbased intelligence network for a reputation verdict. Given these results, you can automatically block malicious files and apply administrator-defined policy.+ File Analysis – provides the ability to analyze unknown files that are traversing the ESA. A highly secure sandbox environment enables AMP to glean precise details about the file’s behavior and to combine that data with detailed human and machine analysis to determine the file’s threat level. This disposition is then fed into AMP cloud-based intelligence network and used to dynamically update and expand the AMP cloud data set for enhanced protection

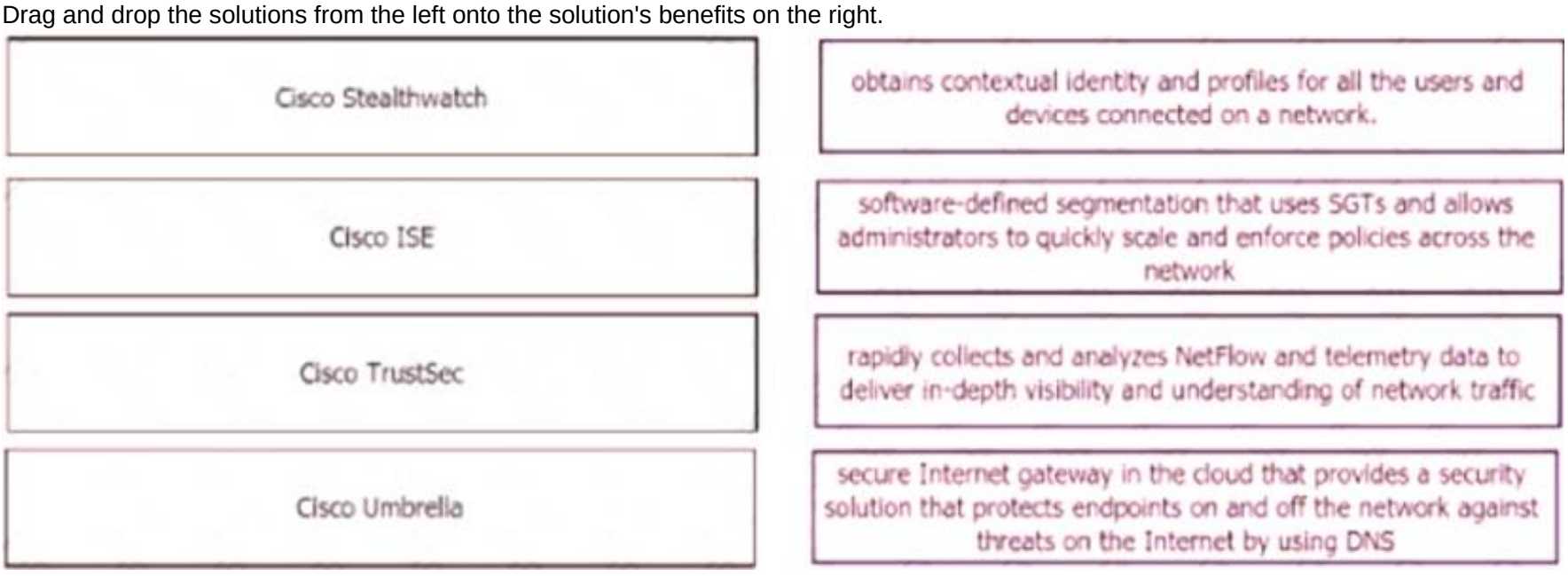
NEW QUESTION 423
- (Exam Topic 2)
An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?

A. Cisco Umbrella
B. Cisco Cloud Email Security
C. Cisco NGFW
D. Cisco Cloudlock

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45- 738565.pdf

NEW QUESTION 426
- (Exam Topic 2)
Drag and drop the solutions from the left onto the solution's benefits on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Cisco Stealthwatch - rapidly collects and analyzes netflow and telementy data to deliver in-depth visibility and understanding of network traffic
Cisco ISE – obtains contextual identity and profiles for all users and device
Cisco TrustSec – software defined segmentation that uses SGTs
Cisco Umbrella – secure internet gateway ion the cloud that provides a security solution

NEW QUESTION 429
- (Exam Topic 2)

When configuring ISAKMP for IKEv1 Phase1 on a Cisco IOS router, an administrator needs to input the command crypto isakmp key cisco address 0.0.0.0. The administrator is not sure what the IP addressing in this command issued for. What would be the effect of changing the IP address from 0.0.0.0 to 1.2.3.4?

A. The key server that is managing the keys for the connection will be at 1.2.3.4
B. The remote connection will only be allowed from 1.2.3.4
C. The address that will be used as the crypto validation authority
D. All IP addresses other than 1.2.3.4 will be allowed

Answer: B

Explanation:
The command crypto isakmp key cisco address 1.2.3.4 authenticates the IP address of the 1.2.3.4 peer by using the key cisco. The address of “0.0.0.0” will authenticate any address with this key

NEW QUESTION 431
- (Exam Topic 2)
In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?

A. LDAP injection
B. man-in-the-middle
C. cross-site scripting
D. insecure API

Answer: B

NEW QUESTION 433
- (Exam Topic 2)
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.

privilege escalation	Tetration platform learns the normal behavior of users.
user login suspicious behavior	Tetration platform is armed to look at sensitive files.
interesting file access	Tetration platform watches user access failures and methods
file access from a different user	Tetration platform watches for movement in the process lineage tree.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/whitepaper-c11-7403

NEW QUESTION 434
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

350-701 Practice Exam Features:

* 350-701 Questions and Answers Updated Frequently

* 350-701 Practice Questions Verified by Expert Senior Certified Staff

* 350-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 350-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year