Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

NEW QUESTION 1
- (Exam Topic 2)
Which type of algorithm provides the highest level of protection against brute-force attacks?

A. PFS
B. HMAC
C. MD5
D. SHA

Answer: D

NEW QUESTION 2
- (Exam Topic 2)
What is a function of 3DES in reference to cryptography?

A. It hashes files.
B. It creates one-time use passwords.
C. It encrypts traffic.
D. It generates private keys.

Answer: C

NEW QUESTION 3
- (Exam Topic 2)
In which two ways does Easy Connect help control network access when used with Cisco TrustSec? (Choose two)

A. It allows multiple security products to share information and work together to enhance security posture in the network.
B. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.
C. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.
D. It integrates with third-party products to provide better visibility throughout the network.
E. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).

Answer: CE

Explanation:
Reference:
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-witheasy-connect-c

NEW QUESTION 4
- (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 5
- (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 6
- (Exam Topic 2)
An organization has a Cisco ESA set up with 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 send copies to other recipients
B. quarantine and send a DLP violation notification
C. quarantine and alter the subject header with a DLP violation
D. deliver and add disclaimer text

Answer: D

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 7
- (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 8
- (Exam Topic 2)
In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint Protection Platform?

A. when there is a need for traditional anti-malware detection
B. when there is no need to have the solution centrally managed
C. when there is no firewall on the network
D. when there is a need to have more advanced detection capabilities

Answer: D

Explanation:
Endpoint protection platforms (EPP) prevent endpoint security threats like known and unknown malware.Endpoint detection and response (EDR) solutions can detect and respond to threats that your EPP and other security tools did not catch.EDR and EPP have similar goals but are designed to fulfill different purposes. EPP is designed to providedevice-level protection by identifying malicious files, detecting potentially malicious activity, and providing tools for incident investigation and response.The preventative nature of EPP complements proactive EDR. EPP acts as the first line of defense, filtering out attacks that can be detected by the organization’s deployed security solutions. EDR acts as a second layer of protection, enabling security analysts to perform threat hunting and identify more subtle threats to the endpoint.Effective endpoint defense requires a solution that integrates the capabilities of both EDR and EPP to provide protection against cyber threats without overwhelming an organization’s security team.

NEW QUESTION 9
- (Exam Topic 2)
A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?

A. Use MAB with profiling
B. Use MAB with posture assessment.
C. Use 802.1X with posture assessment.
D. Use 802.1X with profiling.

Answer: A

Explanation:
Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456

NEW QUESTION 10
- (Exam Topic 2)
Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?

A. file access from a different user
B. interesting file access
C. user login suspicious behavior
D. privilege escalation

Answer: C

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

NEW QUESTION 10
- (Exam Topic 2)
A Cisco Firepower administrator needs to configure a rule to allow a new application that has never been seen on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose

two)

A. permit
B. trust
C. reset
D. allow
E. monitor

Answer: BE

Explanation:
Each rule also has an action, which determines whether you monitor, trust, block, or allow matching traffic.Note: With action “trust”, Firepower does not do any more inspection on the traffic. There will be no intrusion protection and also no file-policy on this traffic.

NEW QUESTION 12
- (Exam Topic 1)
What is a commonality between DMVPN and FlexVPN technologies?

A. FlexVPN and DMVPN use IS-IS routing protocol to communicate with spokes
B. FlexVPN and DMVPN use the new key management protocol
C. FlexVPN and DMVPN use the same hashing algorithms
D. IOS routers run the same NHRP code for DMVPN and FlexVPN

Answer: D

Explanation:
Reference: https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/

NEW QUESTION 15
- (Exam Topic 1)
An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the endpoint to apply a new or updated policy from ISE. Which CoA type achieves this goal?

A. Port Bounce
B. CoA Terminate
C. CoA Reauth
D. CoA Session Query

Answer: C

NEW QUESTION 20
- (Exam Topic 1)
What is the primary role of the Cisco Email Security Appliance?

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

Answer: B

Explanation:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/February2013/Cisco_SBA_BN_EmailSecurityUsing

NEW QUESTION 22
- (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 27
- (Exam Topic 1)
Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two)

A. accounting
B. assurance
C. automation
D. authentication
E. encryption

Answer: BC

Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06- cisco-dna-center-aag-cte-en.html

NEW QUESTION 30
- (Exam Topic 1)
Which feature is supported when deploying Cisco ASAv within AWS public cloud?

A. multiple context mode
B. user deployment of Layer 3 networks
C. IPv6
D. clustering

Answer: B

Explanation:
The ASAv on AWS supports the following features:+ Support for Amazon EC2 C5 instances, the next generation of the Amazon EC2 Compute Optimized instancefamily.+ Deployment in the Virtual Private Cloud (VPC)+ Enhanced networking (SR-IOV) where available+ Deployment from Amazon Marketplace+ Maximum of four vCPUs per instance+ User deployment of L3 networks+ Routed mode (default)Note: The Cisco Adaptive Security Virtual Appliance (ASAv) runs the same software as physical Cisco ASAs to deliver proven security functionality in a virtual form factor. The ASAv can be deployed in the public AWS cloud.It can then be configured to protect virtual and physical data center workloads that expand, contract, or shift their location over time. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96 qsg/asavaws.html

NEW QUESTION 34
- (Exam Topic 1)
Why would a user choose an on-premises ESA versus the CES solution?

A. Sensitive data must remain onsite.
B. Demand is unpredictable.
C. The server team wants to outsource this service.
D. ESA is deployed inline.

Answer: A

NEW QUESTION 39

- (Exam Topic 1)
What is the primary benefit of deploying an ESA in hybrid mode?

A. You can fine-tune its settings to provide the optimum balance between security and performance for your environment
B. It provides the lowest total cost of ownership by reducing the need for physical appliances
C. It provides maximum protection and control of outbound messages
D. It provides email security while supporting the transition to the cloud

Answer: D

Explanation:
Cisco Hybrid Email Security is a unique service offering that facilitates the deployment of your email securityinfrastructure both on premises and in the cloud. You can change the number of on-premises versus cloudusers at any time throughout the term of your contract, assuming the total number of users does not change.This allows for deployment flexibility as your organization's needs change.

NEW QUESTION 40
- (Exam Topic 1)
Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?

A. aaa server radius dynamic-author
B. aaa new-model
C. auth-type all
D. ip device-tracking

Answer: D

NEW QUESTION 42
- (Exam Topic 1)
What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?

A. Enable IP Layer enforcement.
B. Activate the Advanced Malware Protection license
C. Activate SSL decryption.
D. Enable Intelligent Proxy.

Answer: D

NEW QUESTION 43
- (Exam Topic 1)
Which two key and block sizes are valid for AES? (Choose two)

A. 64-bit block size, 112-bit key length
B. 64-bit block size, 168-bit key length
C. 128-bit block size, 192-bit key length
D. 128-bit block size, 256-bit key length
E. 192-bit block size, 256-bit key length

Answer: CD

Explanation:
The AES encryption algorithm encrypts and decrypts data in blocks of 128 bits (block size). It can do this using 128-bit, 192-bit, or 256-bit keys

NEW QUESTION 45
- (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 50
- (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 51
- (Exam Topic 1)
Refer to the exhibit.

```
aaa new-model
radius-server host 10.0.0.12 key
secret12
```

Which statement about the authentication protocol used in the configuration is true?

A. The authentication request contains only a password
B. The authentication request contains only a username
C. The authentication and authorization requests are grouped in a single packet
D. There are separate authentication and authorization request packets

Answer: C

Explanation:
This command uses RADIUS which combines authentication and authorization in one function (packet).

NEW QUESTION 55
- (Exam Topic 1)
Refer to the exhibit.

```
Gateway of last resort is 1.1.1.1 to network 0.0.0.0

S*   0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C        1.1.1.0 255.255.255.0 is directly connect, outside
S        172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C        192.168.100.0 255.255.255.0 is directly connected, inside
C        172.16.10.0 255.255.255.0 is directly connected, dmz
S          10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz

-------------------------------------------------------------------

access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
 match access-list redirect-acl

policy-map inside-policy
 class redirect-class
 sfr fail-open

service-policy inside-policy global
```

What is a result of the configuration?

A. Traffic from the DMZ network is redirected
B. Traffic from the inside network is redirected
C. All TCP traffic is redirected
D. Traffic from the inside and DMZ networks is redirected

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configurefirepower-00.htm

NEW QUESTION 56
- (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 61
- (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 64
- (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 66
- (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 67
- (Exam Topic 1)
A network administrator configures Dynamic ARP Inspection on a switch. After Dynamic ARP Inspection is applied, all users on that switch are unable to communicate with any destination. The network administrator checks the interface status of all interfaces, and there is no err-disabled interface. What is causing this problem?

A. DHCP snooping has not been enabled on all VLANs.
B. The ip arp inspection limit command is applied on all interfaces and is blocking the traffic of all users.
C. Dynamic ARP Inspection has not been enabled on all VLANs
D. The no ip arp inspection trust command is applied on all user host interfaces

Answer: D

Explanation:
Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. After enabling DAI, all ports become untrusted ports.

NEW QUESTION 72
- (Exam Topic 1)
Which RADIUS attribute can you use to filter MAB requests in an 802.1 x deployment?

A. 1
B. 2
C. 6
D. 31

Answer: C

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networkingservices/config_

NEW QUESTION 73
- (Exam Topic 1)
Which technology must be used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

A. DMVPN
B. FlexVPN
C. IPsec DVTI
D. GET VPN

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/dam/en/us/products/collateral/security/group-encrypted-transport-vpn/GETVPN_DIG_

NEW QUESTION 75
- (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 79
- (Exam Topic 1)
Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?

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

Answer: D

NEW QUESTION 84
- (Exam Topic 1)
What provides visibility and awareness into what is currently occurring on the network?

A. CMX
B. WMI
C. Prime Infrastructure
D. Telemetry

Answer: D

Explanation:
Reference: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/activethreat-analytics

NEW QUESTION 85
- (Exam Topic 1)
Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?

A. quality of service
B. time synchronization
C. network address translations
D. intrusion policy

Answer: B

NEW QUESTION 90
- (Exam Topic 1)
Which two characteristics of messenger protocols make data exfiltration difficult to detect and prevent? (Choose two)

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

Answer: CE

NEW QUESTION 92
- (Exam Topic 1)
Which two kinds of attacks are prevented by multifactor authentication? (Choose two)

A. phishing
B. brute force
C. man-in-the-middle
D. DDOS
E. teardrop

Answer: BC

NEW QUESTION 95
- (Exam Topic 1)
Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

A. user input validation in a web page or web application
B. Linux and Windows operating systems
C. database
D. web page images

Answer: A

Explanation:
SQL injection usually occurs when you ask a user for input, like their username/userid, but the user gives(“injects”) you an SQL statement that you will unknowingly run on your database. For example:Look at the following example, which creates a SELECT statement by adding a variable (txtUserId) to a selectstring. The variable is fetched from user input (getRequestString):txtUserId = getRequestString(“UserId”);txtSQL = “SELECT * FROM Users WHERE UserId = ” + txtUserId;If user enter something like this: “100 OR 1=1” then the SzQL statement will look like this:SELECT * FROM Users WHERE UserId = 100 OR 1=1;The SQL above is valid and will return ALL rows from the “Users” table, since OR 1=1 is always TRUE. Ahacker might get access to all the user names and passwords in this database.

NEW QUESTION 97
- (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 99
- (Exam Topic 1)
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. ip flow monitor input
C. ip flow-export destination 1.1.1.1 2055
D. flow exporter

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_nsel.h

NEW QUESTION 102
- (Exam Topic 1)
Which statement about the configuration of Cisco ASA NetFlow v9 Secure Event Logging is true?

A. To view bandwidth usage for NetFlow records, the QoS feature must be enabled.
B. A sysopt command can be used to enable NSEL on a specific interface.
C. NSEL can be used without a collector configured.
D. A flow-export event type must be defined under a policy

Answer: D

NEW QUESTION 107
- (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 112
- (Exam Topic 1)
Which function is the primary function of Cisco AMP threat Grid?

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

Answer: C

NEW QUESTION 114
- (Exam Topic 1)
When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?

A. Spero analysis
B. dynamic analysis
C. sandbox analysis
D. malware analysis

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Refere Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload
thewhole file. Dynamic analysis sends files to AMP ThreatGrid.Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco ThreatGrid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file ismalicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threatscore, you can view a dynamic analysis summary report with the reasons for the assigned threat score. Youcan also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well asscrubbed reports with limited data for files that your organization did not submit.Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, andother types of files for the most common types of malware, using a detection rule set provided by the CiscoTalos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud,and does not run the file, local malware analysis saves time and system resources. -> Malware analysis doesnot upload files to anywhere, it only checks the files locally.There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in avirtual machine.

NEW QUESTION 117
- (Exam Topic 1)
A network engineer has entered the snmp-server user andy myv3 auth sha cisco priv aes 256 cisc0380739941 command and needs to send SNMP information to a host at 10.255.254.1. Which command achieves this goal?

A. snmp-server host inside 10.255.254.1 version 3 andy
B. snmp-server host inside 10.255.254.1 version 3 myv3
C. snmp-server host inside 10.255.254.1 snmpv3 andy
D. snmp-server host inside 10.255.254.1 snmpv3 myv3

Answer: A

Explanation:
The command "snmp-server user user-name group-name [remote ip-address [udp-port port]]

{v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]" adds a new user (in this case "andy") to an SNMPv3 group (in this case group name "myv3") and configures a password for the user.In the "snmp-server host" command, we need to:+ Specify the SNMP version with key word "version {1 | 2 | 3}"+ Specify the username ("andy"), not group name ("myv3").Note: In "snmp-server host inside …" command, "inside" is the interface name of the ASA interface through which the NMS (located at 10.255.254.1) can be reached.

NEW QUESTION 121
- (Exam Topic 1)
Which two tasks allow NetFlow on a Cisco ASA 5500 Series firewall? (Choose two)

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

Answer: CE

NEW QUESTION 124
- (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 125
- (Exam Topic 1)
Which SNMPv3 configuration must be used to support the strongest security possible?

A. asa-host(config)#snmp-server group myv3 v3 privasa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
B. asa-host(config)#snmp-server group myv3 v3 noauthasa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
C. asa-host(config)#snmpserver group myv3 v3 noauthasa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
D. asa-host(config)#snmp-server group myv3 v3 privasa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

Answer: D

NEW QUESTION 127
- (Exam Topic 1)
An engineer needs a solution for TACACS+ authentication and authorization for device administration. The engineer also wants to enhance wired and wireless network security by requiring users and endpoints to use 802.1X, MAB, or WebAuth. Which product meets all of these requirements?

A. Cisco Prime Infrastructure
B. Cisco Identity Services Engine
C. Cisco Stealthwatch
D. Cisco AMP for Endpoints

Answer: B

NEW QUESTION 128
- (Exam Topic 1)
Which feature of Cisco ASA allows VPN users to be postured against Cisco ISE without requiring an inline posture node?

A. RADIUS Change of Authorization
B. device tracking
C. DHCP snooping
D. VLAN hopping

Answer: A

NEW QUESTION 132
- (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 134
- (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 138
- (Exam Topic 1)
Refer to the exhibit.

```
SwitchA(config)#interface gigabitethernet1/0/1
SwitchA(config-if)#dot1x host-mode multi-host
SwitchA(config-if)#dot1x timeout quiet-period 3
SwitchA(config-if)#dot1x timeout tx-period 15
SwitchA(config-if)#authentication port-control
auto
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 12
```

An engineer configured wired 802.1x on the network and is unable to get a laptop to authenticate. Which port configuration is missing?

A. authentication open
B. dotlx reauthentication
C. cisp enable
D. dot1x pae authenticator

Answer: D

NEW QUESTION 142
- (Exam Topic 1)
Under which two circumstances is a CoA issued? (Choose two)

A. A new authentication rule was added to the policy on the Policy Service node.
B. An endpoint is deleted on the Identity Service Engine server.
C. A new Identity Source Sequence is created and referenced in the authentication policy.
D. An endpoint is profiled for the first time.
E. A new Identity Service Engine server is added to the deployment with the Administration persona

Answer: BD

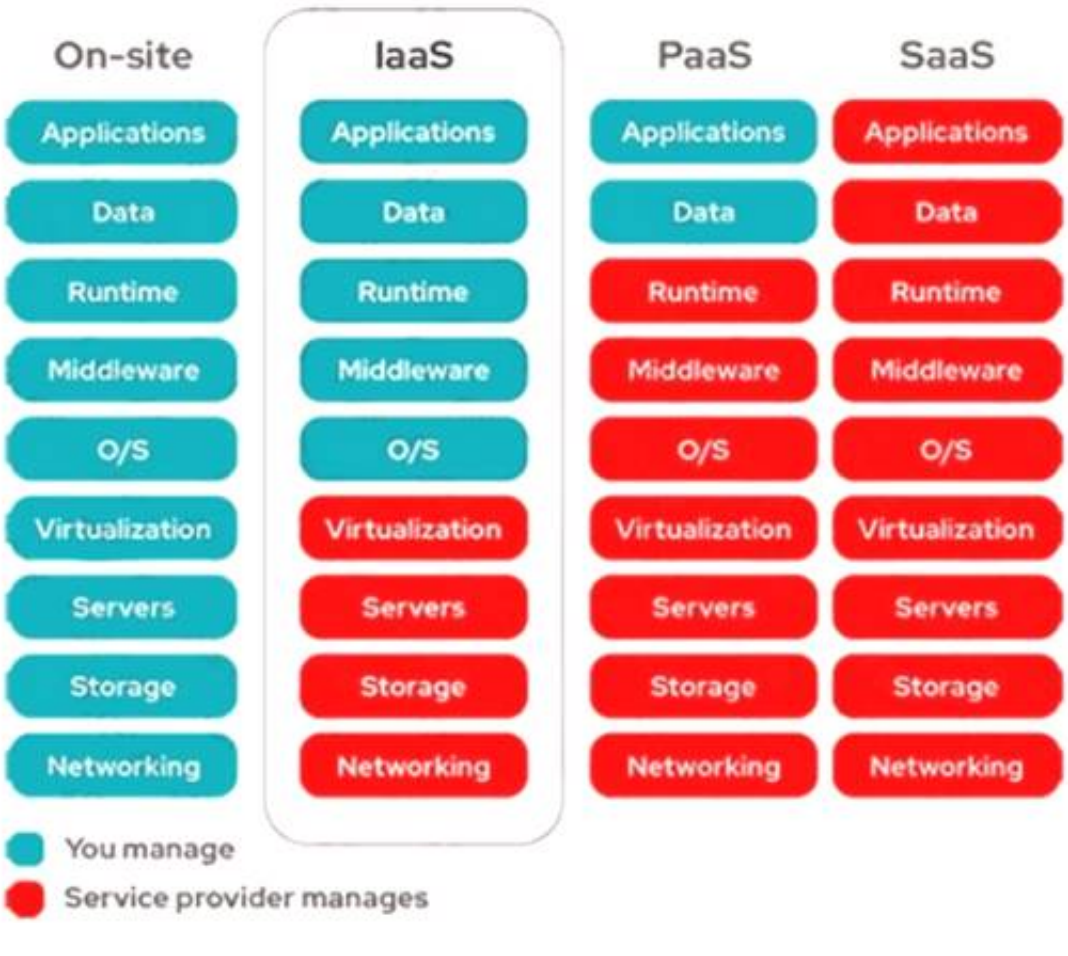
Explanation:
The profiling service issues the change of authorization in the following cases:– Endpoint deleted—When an endpoint is deleted from the Endpoints page and the endpoint is disconnectedor removed from the network.An exception action is configured—If you have an exception action configured per profile that leads to anunusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to thecorresponding static profile by issuing a CoA.– An endpoint is profiled for the first time—When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.+ An endpoint identity group has changed—When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide

NEW QUESTION 147
- (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 149
- (Exam Topic 1)
What provides the ability to program and monitor networks from somewhere other than the DNAC GUI?

A. NetFlow
B. desktop client
C. ASDM
D. API

Answer: D

NEW QUESTION 151
- (Exam Topic 1)
Which threat involves software being used to gain unauthorized access to a computer system?

A. virus
B. NTP amplification
C. ping of death
D. HTTP flood

Answer: A

NEW QUESTION 153
- (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 156
- (Exam Topic 1)
Which statement about IOS zone-based firewalls is true?

A. An unassigned interface can communicate with assigned interfaces
B. Only one interface can be assigned to a zone.
C. An interface can be assigned to multiple zones.
D. An interface can be assigned only to one zone.

Answer: D

NEW QUESTION 157
- (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 158
- (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 161
- (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 162
- (Exam Topic 1)
Which algorithm provides encryption and authentication for data plane communication?

A. AES-GCM
B. SHA-96
C. AES-256
D. SHA-384

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/ security-overview.html

NEW QUESTION 164
- (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 167
- (Exam Topic 1)
Which type of attack is social engineering?

A. trojan
B. phishing
C. malware
D. MITM

Answer: B

Explanation:
Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to
solicit personal,often financial, information. Attackers may send email seemingly from a reputable credit card company orfinancial institution that requests account information, often suggesting that there is a problem.

NEW QUESTION 171
- (Exam Topic 1)
What is the function of Cisco Cloudlock for data security?

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

Answer: A

NEW QUESTION 174
- (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 178
- (Exam Topic 1)
How many interfaces per bridge group does an ASA bridge group deployment support?

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

Answer: B

Explanation:
Each of the ASAs interfaces need to be grouped into one or more bridge groups. Each of these groups acts as an independent transparent firewall. It is not possible for one bridge group to communicate with another bridge group without assistance from an external router.As of 8.4(1) upto 8 bridge groups are supported with 2-4 interface in each group. Prior to this only one bridge group was supported and only 2 interfaces.Up to 4 interfaces are permitted per bridge–group (inside, outside, DMZ1, DMZ2)

NEW QUESTION 179
- (Exam Topic 1)
Which two conditions are prerequisites for stateful failover for IPsec? (Choose two)

A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device;the IPsec configuration is copied automatically
B. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.
C. The IPsec configuration that is set up on the active device must be duplicated on the standby device
D. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically.
E. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device

Answer: CE

Explanation:
Stateful failover for IP Security (IPsec) enables a router to continue processing and forwarding IPsec packetsafter a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automaticallytakes over the tasks of the active (primary) router if the active router loses connectivity for any reason. Thisfailover process is transparent to users and does not require adjustment or reconfiguration of any remote peer.Stateful failover for IPsec requires that your network contains two identical routers that are available to be eitherthe primary or secondary device. Both routers should be the same type of device, have the same CPU andmemory, and have either no encryption accelerator or identical encryption accelerators.Prerequisites for Stateful Failover for IPsec
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpnavailability-15- the prerequisites only stated that “Both routers should be the same type of device” but in the“Restrictions for Stateful Failover for IPsec” section of the link above, it requires “Both the active and standby devices must run the identical version of the Cisco IOS software” so answer E is better than answer B.

NEW QUESTION 182
- (Exam Topic 1)
The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

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

Answer: D

NEW QUESTION 185

- (Exam Topic 1)
Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?

A. TLSv1.2
B. TLSv1.1
C. BJTLSv1
D. DTLSv1

Answer: D

Explanation:
DTLS is used for delay sensitive applications (voice and video) as its UDP based while TLS is TCP based.Therefore DTLS offers strongest throughput performance. The throughput of DTLS at the time of AnyConnect connection can be expected to have processing performance close to VPN throughput.

NEW QUESTION 186
- (Exam Topic 1)
An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?

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

Answer: D

NEW QUESTION 191
- (Exam Topic 1)
Which form of attack is launched using botnets?

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

Answer: C

Explanation:
A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them.Cyber criminals use botnets to instigate botnet attacks, which include malicious activities such as credentialsleaks, unauthorized access, data theft and DDoS attacks.

NEW QUESTION 196
- (Exam Topic 3)
Which command is used to log all events to a destination colector 209.165.201.107?

A. CiscoASA(config-pmap-c)#flow-export event-type flow-update destination 209.165.201.10
B. CiscoASA(config-cmap)# flow-export event-type all destination 209.165.201.
C. CiscoASA(config-pmap-c)#flow-export event-type all destination 209.165.201.10
D. CiscoASA(config-cmap)#flow-export event-type flow-update destination 209.165.201.10

Answer: C

NEW QUESTION 200
- (Exam Topic 3)
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 the ip dhcp snooping trust command on the DHCP interfaces to get the information 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 a service template within the switch to standardize the port configurations so that the correct information is sent to Cisco ISE
D. Configure the device sensor feature within the switch to send the appropriate protocol information

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-ConfigureDevice-Sensor

NEW QUESTION 204
- (Exam Topic 3)
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. Southbound APIs utilize CLI, SNMP, and RESTCONF.
E. Northbound interfaces utilize OpenFlow and OpFlex to integrate with network devices.

Answer: CD

NEW QUESTION 205
- (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 207
- (Exam Topic 3)
Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)

A. It must include the current date.
B. It must reside in the trusted store of the WSA.
C. It must reside in the trusted store of the endpoint.
D. It must have been signed by an internal CA.
E. it must contain a SAN.

Answer: AB

NEW QUESTION 209
- (Exam Topic 3)
Which characteristic is unique to a Cisco WSAv as compared to a physical appliance?

A. supports VMware vMotion on VMware ESXi
B. requires an additional license
C. performs transparent redirection
D. supports SSL decryption

Answer: A

NEW QUESTION 214
- (Exam Topic 3)
Why is it important to patch endpoints consistently?

A. Patching reduces the attack surface of the infrastructure.
B. Patching helps to mitigate vulnerabilities.
C. Patching is required per the vendor contract.
D. Patching allows for creating a honeypot.

Answer: B

NEW QUESTION 217
- (Exam Topic 3)
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

NEW QUESTION 219
- (Exam Topic 3)
Which algorithm is an NGE hash function?

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

Answer: D

NEW QUESTION 223
- (Exam Topic 3)
Which solution stops unauthorized access to the system if a user's password is compromised?

A. VPN
B. MFA

C. AMP
D. SSL

Answer: B

NEW QUESTION 227
- (Exam Topic 3)
Which solution for remote workers enables protection, detection, and response on the endpoint against known and unknown threats?

A. Cisco AMP for Endpoints
B. Cisco AnyConnect
C. Cisco Umbrella
D. Cisco Duo

Answer: A

NEW QUESTION 231
- (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 234
- (Exam Topic 3)
Refer to the exhibit,

```
*Jul  1 15:33:50.027: ISAKMP: (0):Enqueued KEY_MGR_SESSION_CLOSED for Tunnel0 deletion
*Jul  1 15:33:50.027: ISAKMP: (0):Deleting peer node by peer_reap for 2.2.2.2: D1250B0
*Jul  1 15:33:50.029: ISAKMP: (1001):peer does not do paranoid keepalives.
*Jul  1 15:33:54.781: ISAKMP-PAK: (0):received packet from 2.2.2.2 dport 500 sport 500 Global (N) NEW SA
*Jul  1 15:33:54.781: ISAKMP: (0):Created a peer struct for 2.2.2.2, peer port 500
*Jul  1 15:33:54.781: ISAKMP: (0):New peer created peer = 0x11026528 peer_handle = 0x80000004
*Jul  1 15:33:54.781: ISAKMP: (0):Locking peer struct 0x11026528, refcount 1 for crypto_isakmp_process_block
*Jul  1 15:33:54.782: ISAKMP: (0):local port 500, remote port 500
*Jul  1 15:33:54.782: ISAKMP: (0):Find a dup sa in the avl tree during calling isadb_insert sa = 104E3C68
*Jul  1 15:33:54.782: ISAKMP: (0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jul  1 15:33:54.782: ISAKMP: (0):Old State = IKE_READY  New State = IKE_R_MM1
```

which command results in these messages when attempting to troubleshoot an iPsec VPN connection?

A. debug crypto isakmp
B. debug crypto ipsec endpoint
C. debug crypto Ipsec
D. debug crypto isakmp connection

Answer: A

NEW QUESTION 236
- (Exam Topic 3)
What are two functionalities of SDN Northbound APIs? (Choose two.)

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

Answer: AB

NEW QUESTION 240
- (Exam Topic 3)
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. Use the track movement option within the authorization profile for the authorization policy line that the unauthenticated devices hit.
C. 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.

D. Add the DACL name for the Airespace ACL configured on the WLC in the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.

Answer: D

NEW QUESTION 245
- (Exam Topic 3)
Which two Cisco ISE components must be configured for BYOD? (Choose two.)

A. local WebAuth
B. central WebAuth
C. null WebAuth
D. guest
E. dual

Answer: BD

NEW QUESTION 248
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 251
- (Exam Topic 3)
An engineer is deploying Cisco Advanced Malware Protection (AMP) for Endpoints and wants to create a policy that prevents users from executing file named abc424952615.exe without quarantining that file What type of Outbreak Control list must the SHA.-256 hash value for the file be added to in order to accomplish this?

A. Advanced Custom Detection
B. Blocked Application
C. Isolation
D. Simple Custom Detection

Answer: B

NEW QUESTION 255
- (Exam Topic 3)
Which Cisco DNA Center Intent API action is used to retrieve the number of devices known to a DNA Center?

A. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/network-device/count
B. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/network-device
C. GEThttps://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/networkdevice?parameter1=value&parameter2=v
D. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v 1/networkdevice/startIndex/recordsToReturn

Answer: A

NEW QUESTION 260
- (Exam Topic 3)
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. Configure intrusion rules for the DNP3 preprocessor
D. Modify the access control policy to trust the industrial traffic

Answer: C

Explanation:
"configure INTRUSION RULES for DNP3" -> Documentation states, that enabling INTRUSION RULES is mandatory for CIP to work + required preprocessors (in Network Access Policy - NAP) will be enabled automatically:
"If you want the CIP preprocessor rules listed in the following table to generate events, you MUST enable them. See Setting Intrusion Rule States for information on enabling rules."
"If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings, although the preprocessor remains disabled in the web interface for the corresponding network analysis policy."
[1]
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada

NEW QUESTION 263

- (Exam Topic 3)
An engineer is configuring cloud logging using a company-managed Amazon S3 bucket for Cisco Umbrella logs. What benefit does this configuration provide for accessing log data?

A. It is included m the license cost for the multi-org console of Cisco Umbrella
B. It can grant third-party SIEM integrations write access to the S3 bucket
C. No other applications except Cisco Umbrella can write to the S3 bucket
D. Data can be stored offline for 30 days.

Answer: D

NEW QUESTION 268
- (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.

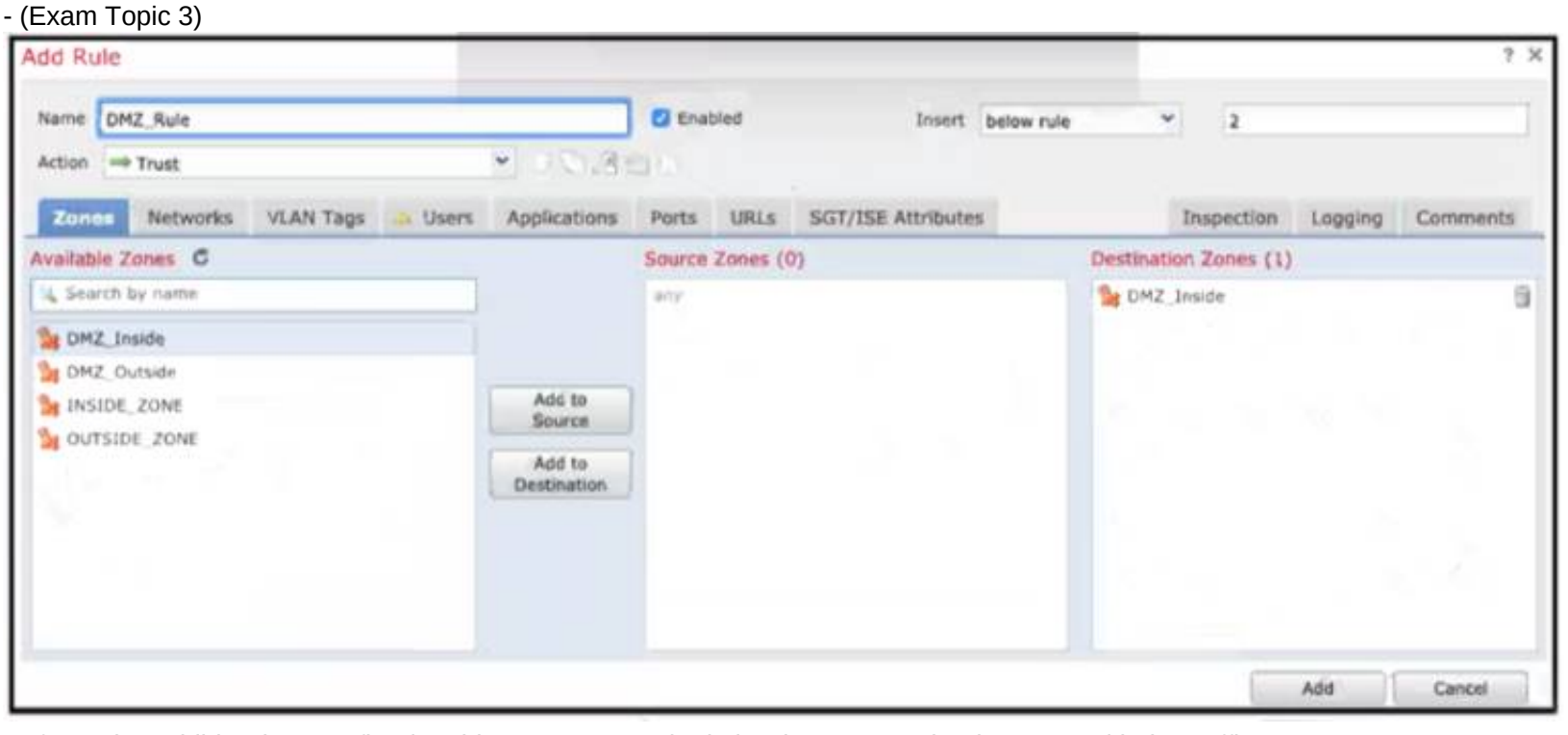
Answer: D

NEW QUESTION 271
- (Exam Topic 3)
A company discovered an attack propagating through their network via a file. A custom file 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 created is functioning as it should?

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

Answer: C

NEW QUESTION 273
- (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 278
- (Exam Topic 3)
Which solution is more secure than the traditional use of a username and password and encompasses at least two of the methods of authentication?

A. single-sign on
B. RADIUS/LDAP authentication
C. Kerberos security solution
D. multifactor authentication

Answer: D

NEW QUESTION 282
- (Exam Topic 3)
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. Manually change the management port on Cisco FMC and all managed Cisco FTD devices
B. Set the tunnel to go through the Cisco FTD
C. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices
D. Set the tunnel port to 8305

Answer: A

Explanation:
The FMC and managed devices communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305.Cisco strongly recommends that you keep the default settings for the remote management port, but if themanagement port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate with each other.
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmtnw.html

NEW QUESTION 285
- (Exam Topic 3)
Which two components do southbound APIs use to communicate with downstream devices? (Choose two.)

A. services running over the network
B. OpenFlow
C. external application APIs
D. applications running over the network
E. OpFlex

Answer: BE

NEW QUESTION 286
- (Exam Topic 3)
A network engineer is tasked with configuring a Cisco ISE server to implement external authentication against Active Directory. What must be considered about the authentication requirements? (Choose two.)

A. RADIUS communication must be permitted between the ISE server and the domain controller.
B. The ISE account must be a domain administrator in Active Directory to perform JOIN operations.
C. Active Directory only supports user authentication by using MSCHAPv2.
D. LDAP communication must be permitted between the ISE server and the domain controller.
E. Active Directory supports user and machine authentication by using MSCHAPv2.

Answer: BC

NEW QUESTION 290
- (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 294
- (Exam Topic 3)
Which Cisco cloud security software centrally manages policies on multiple platforms such as Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS?

A. Cisco Defense Orchestrator
B. Cisco Configuration Professional
C. Cisco Secureworks
D. Cisco DNAC

Answer: A

NEW QUESTION 298
- (Exam Topic 3)
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

NEW QUESTION 303
- (Exam Topic 3)
An engineer is configuring device-hardening on a router in order to prevent credentials from being seen if the router configuration was compromised. Which command should be used?

A. service password-encryption
B. username <username> privilege 15 password <password>
C. service password-recovery
D. username < username> password <password>

Answer: A

NEW QUESTION 304
- (Exam Topic 3)
Which Cisco platform provides an agentless solution to provide visibility across the network including encrypted traffic analytics to detect malware in encrypted traffic without the need for decryption?

A. Cisco Advanced Malware Protection
B. Cisco Stealthwatch
C. Cisco Identity Services Engine
D. Cisco AnyConnect

Answer: B

NEW QUESTION 305
- (Exam Topic 3)
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

NEW QUESTION 309
- (Exam Topic 3)
Which two protocols must be configured to authenticate end users to the Web Security Appliance? (Choose two.)

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

Answer: AB

NEW QUESTION 312
- (Exam Topic 3)
Which two parameters are used to prevent a data breach in the cloud? (Choose two.)

A. DLP solutions
B. strong user authentication
C. encryption

D. complex cloud-based web proxies
E. antispoofing programs

Answer: AB

NEW QUESTION 316
- (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 319
- (Exam Topic 3)
What is the process In DevSecOps where all changes In the central code repository are merged and synchronized?

A. CD
B. EP
C. CI
D. QA

Answer: C

NEW QUESTION 321
- (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 325
- (Exam Topic 3)
DoS attacks are categorized as what?

A. phishing attacks
B. flood attacks
C. virus attacks
D. trojan attacks

Answer: B

NEW QUESTION 327
- (Exam Topic 3)
Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or Microsoft vSwitch?

A. inter-EPG isolation
B. inter-VLAN security
C. intra-EPG isolation
D. placement in separate EPGs

Answer: C

Explanation:
Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or microsegmented (uSeg) EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another.

NEW QUESTION 331
- (Exam Topic 3)
Which type of data exfiltration technique encodes data in outbound DNS requests to specific servers and can be stopped by Cisco Umbrella?

A. DNS tunneling
B. DNS flood attack
C. cache poisoning
D. DNS hijacking

Answer:

A

NEW QUESTION 333
- (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 336
- (Exam Topic 3)
An organization wants to provide visibility and to identify active threats in its network using a VM. The organization wants to extract metadata from network packet flow while ensuring that payloads are not retained or transferred outside the network. Which solution meets these requirements?

A. Cisco Umbrella Cloud
B. Cisco Stealthwatch Cloud PNM
C. Cisco Stealthwatch Cloud PCM
D. Cisco Umbrella On-Premises

Answer: B

Explanation:
Reference:
https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf

NEW QUESTION 341
- (Exam Topic 3)
An organization must add new firewalls to its infrastructure and wants to use Cisco ASA or Cisco FTD.
The chosen firewalls must provide methods of blocking traffic that include offering the user the option to bypass the block for certain sites after displaying a warning page and to reset the connection. Which solution should the organization choose?

A. Cisco FTD because it supports system rate level traffic blocking, whereas Cisco ASA does not
B. Cisco ASA because it allows for interactive blocking and blocking with reset to be configured via the GUI, whereas Cisco FTD does not.
C. Cisco FTD because it enables interactive blocking and blocking with reset natively, whereas Cisco ASAdoes not
D. Cisco ASA because it has an additional module that can be installed to provide multiple blocking capabilities, whereas Cisco FTD does not.

Answer: C

NEW QUESTION 345
- (Exam Topic 3)
What is a difference between GETVPN and IPsec?

A. GETVPN reduces latency and provides encryption over MPLS without the use of a central hub
B. GETVPN provides key management and security association management
C. GETVPN is based on IKEv2 and does not support IKEv1
D. GETVPN is used to build a VPN network with multiple sites without having to statically configure all devices

Answer: C

NEW QUESTION 347
- (Exam Topic 3)
What do tools like Jenkins, Octopus Deploy, and Azure DevOps provide in terms of application and infrastructure automation?

A. continuous integration and continuous deployment
B. cloud application security broker
C. compile-time instrumentation
D. container orchestration

Answer: A

NEW QUESTION 348
- (Exam Topic 3)
An engineer is configuring IPsec VPN and needs an authentication protocol that is reliable and supports ACK and sequence. Which protocol accomplishes this goal?

A. AES-192
B. IKEv1
C. AES-256
D. ESP

Answer: D

NEW QUESTION 351
- (Exam Topic 3)
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: C

NEW QUESTION 352
- (Exam Topic 3)
Refer to the exhibit.

```
ASA# show service-policy sfr

Global policy:
  Service-policy: global_policy
    Class-map: SFR
      SFR: card status Up, mode fail-open monitor-only
        Packet input 0, packet output [illegible] drop 0, reset-drop 0
```

What are two indications of the Cisco Firepower Services Module configuration? (Choose two.)

A. The module is operating in IDS mode.
B. Traffic is blocked if the module fails.
C. The module fails to receive redirected traffic.
D. The module is operating in IPS mode.
E. Traffic continues to flow if the module fails.

Answer: AE

Explanation:
sfr {fail-open | fail-close [monitor-only]} <- There's a couple different options here. The first one is fail-open which means that if the Firepower software module is unavailable, the ASA will continue to forward traffic. fail-close means that if the Firepower module fails, the traffic will stop flowing. While this doesn't seem ideal, there might be a use case for it when securing highly regulated environments. The monitor-only switch can be used with both and basically puts the Firepower services into IDS-mode only. This might be useful for initial testing or setup.

NEW QUESTION 355
- (Exam Topic 3)
What does endpoint isolation in Cisco AMP for Endpoints security protect from?

A. an infection spreading across the network E
B. a malware spreading across the user device
C. an infection spreading across the LDAP or Active Directory domain from a user account
D. a malware spreading across the LDAP or Active Directory domain from a user account

Answer: C

Explanation:
https://community.cisco.com/t5/endpoint-security/amp-endpoint-isolation/td-p/4086674#:~:text=Isolating%20an

NEW QUESTION 358
- (Exam Topic 3)
When network telemetry is implemented, what is important to be enabled across all network infrastructure devices to correlate different sources?

A. CDP
B. NTP
C. syslog
D. DNS

Answer: B

NEW QUESTION 363
- (Exam Topic 3)
When MAB is configured for use within the 802.1X environment, an administrator must create a policy that allows the devices onto the network. Which information is used for the username and password?

A. The MAB uses the IP address as username and password.
B. The MAB uses the call-station-ID as username and password.

C. Each device must be set manually by the administrator.
D. The MAB uses the MAC address as username and password.

Answer: D

NEW QUESTION 367
- (Exam Topic 3)
An engineer needs to detect and quarantine a file named abc424400664 zip based on the MD5 signature of the file using the Outbreak Control list feature within Cisco Advanced Malware Protection (AMP) for Endpoints The configured detection method must work on files of unknown disposition Which Outbreak Control list must be configured to provide this?

A. Blocked Application
B. Simple Custom Detection
C. Advanced Custom Detection
D. Android Custom Detection

Answer: C

NEW QUESTION 371
- (Exam Topic 3)
An engineer is configuring Cisco WSA and needs to deploy it in transparent mode. Which configuration component must be used to accomplish this goal?

A. MDA on the router
B. PBR on Cisco WSA
C. WCCP on switch
D. DNS resolution on Cisco WSA

Answer: C

NEW QUESTION 372
- (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 374
- (Exam Topic 3)
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 ASA because it enables URL filtering and blocks malicious URLs by default, whereas Cisco FTD 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 includes URL filtering in the access control policy capabilities, whereas Cisco ASA does not
D. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not

Answer: C

NEW QUESTION 379
- (Exam Topic 3)
Which role is a default guest type in Cisco ISE?

A. Monthly
B. Yearly
C. Contractor
D. Full-Time

Answer: C

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-4-1/admin_guide/b_ise_admin_guide_141/b_ise_admin_g

NEW QUESTION 384
- (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 389
- (Exam Topic 3)
Which benefit does DMVPN provide over GETVPN?

A. DMVPN supports QoS, multicast, and routing, and GETVPN supports only QoS.
B. DMVPN is a tunnel-less VPN, and GETVPN is tunnel-based.
C. DMVPN supports non-IP protocols, and GETVPN supports only IP protocols.
D. DMVPN can be used over the public Internet, and GETVPN requires a private network.

Answer: D

NEW QUESTION 394
- (Exam Topic 3)
Which function is included when Cisco AMP is added to web security?

A. multifactor, authentication-based user identity
B. detailed analytics of the unknown file's behavior
C. phishing detection on emails
D. threat prevention on an infected endpoint

Answer: B

NEW QUESTION 397
- (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 400
- (Exam Topic 3)
Which security solution is used for posture assessment of the endpoints in a BYOD solution?

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

Answer: D

NEW QUESTION 403
- (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 406
- (Exam Topic 3)
Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

A. OpenC2
B. OpenlOC
C. CybOX
D. STIX

Answer: D

NEW QUESTION 410
- (Exam Topic 3)
What are two workloaded security models? (Choose two)

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

Answer: CD

NEW QUESTION 414
- (Exam Topic 3)
Which feature is used in a push model to allow for session identification, host reauthentication, and session termination?

A. AAA attributes
B. CoA request
C. AV pair
D. carrier-grade NAT

Answer: C

NEW QUESTION 417
- (Exam Topic 3)
Using Cisco Cognitive Threat Analytics, which platform automatically blocks risky sites, and test unknown sites for hidden advanced threats before allowing users to click them?

A. Cisco Identity Services Engine (ISE)
B. Cisco Enterprise Security Appliance (ESA)
C. Cisco Web Security Appliance (WSA)
D. Cisco Advanced Stealthwatch Appliance (ASA)

Answer: C

NEW QUESTION 422
- (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 427
- (Exam Topic 3)
Refer to the exhibit.

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

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. NTP authentication is not enabled.
C. The hashing algorithm that was used was MD5. which is unsupported.

D. The router was not rebooted after the NTP configuration updated.

Answer: B

NEW QUESTION 431
- (Exam Topic 3)

```
def dnac_login(host, username, password):
    url = "https://{}/api/system/v1/auth/token".format(host)
    response = requests.request("POST", url,
auth=HTTPBasicAuth(username, password),
                                headers=headers, verify=False)
    return response.json() ["Token"]
```

Refer to the exhibit. What is the result of the Python script?

A. It uses the POST HTTP method to obtain a username and password to be used for authentication.
B. It uses the POST HTTP method to obtain a token to be used for authentication.
C. It uses the GET HTTP method to obtain a token to be used for authentication.
D. It uses the GET HTTP method to obtain a username and password to be used for authentication

Answer: B

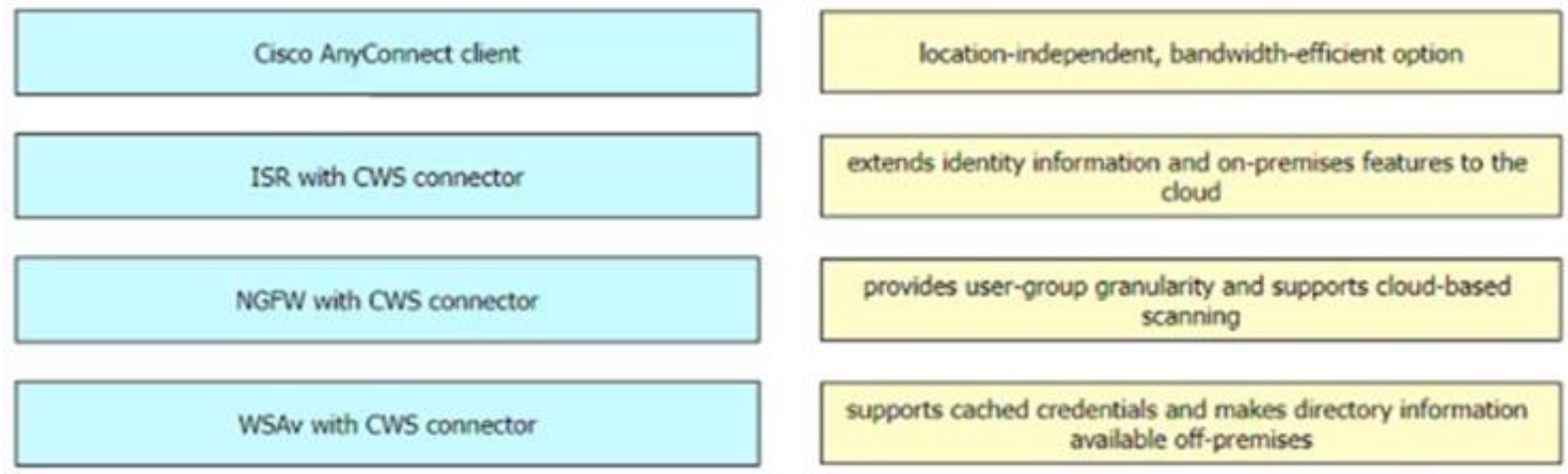
NEW QUESTION 433
- (Exam Topic 3)
Which posture assessment requirement provides options to the client for remediation and requires the remediation within a certain timeframe?

A. Audit
B. Mandatory
C. Optional
D. Visibility

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_client_posture_ Mandatory Requirements During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings

NEW QUESTION 438
- (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 440
- (Exam Topic 3)
Which parameter is required when configuring a Netflow exporter on a Cisco Router?

A. DSCP value
B. Source interface
C. Exporter name
D. Exporter description

Answer: C

Explanation:
An example of configuring a NetFlow exporter is shown below:flow exporter Exporterdestination 192.168.100.22transport udp 2055

NEW QUESTION 442
- (Exam Topic 3)
What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?

A. trusted automated exchange
B. Indicators of Compromise
C. The Exploit Database
D. threat intelligence

Answer: D

NEW QUESTION 445
- (Exam Topic 3)
A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to
ensure that bandwidth is available for VPN users needing access to corporate resources on the10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the
network?

A. Use split tunneling to tunnel traffic for the 10.0.0.0/24 network only.
B. Configure VPN load balancing to distribute traffic for the 10.0.0.0/24 network,
C. Configure VPN load balancing to send non-corporate traffic straight to the internet.
D. Use split tunneling to tunnel all traffic except for the 10.0.0.0/24 network.

Answer: A

NEW QUESTION 449
- (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

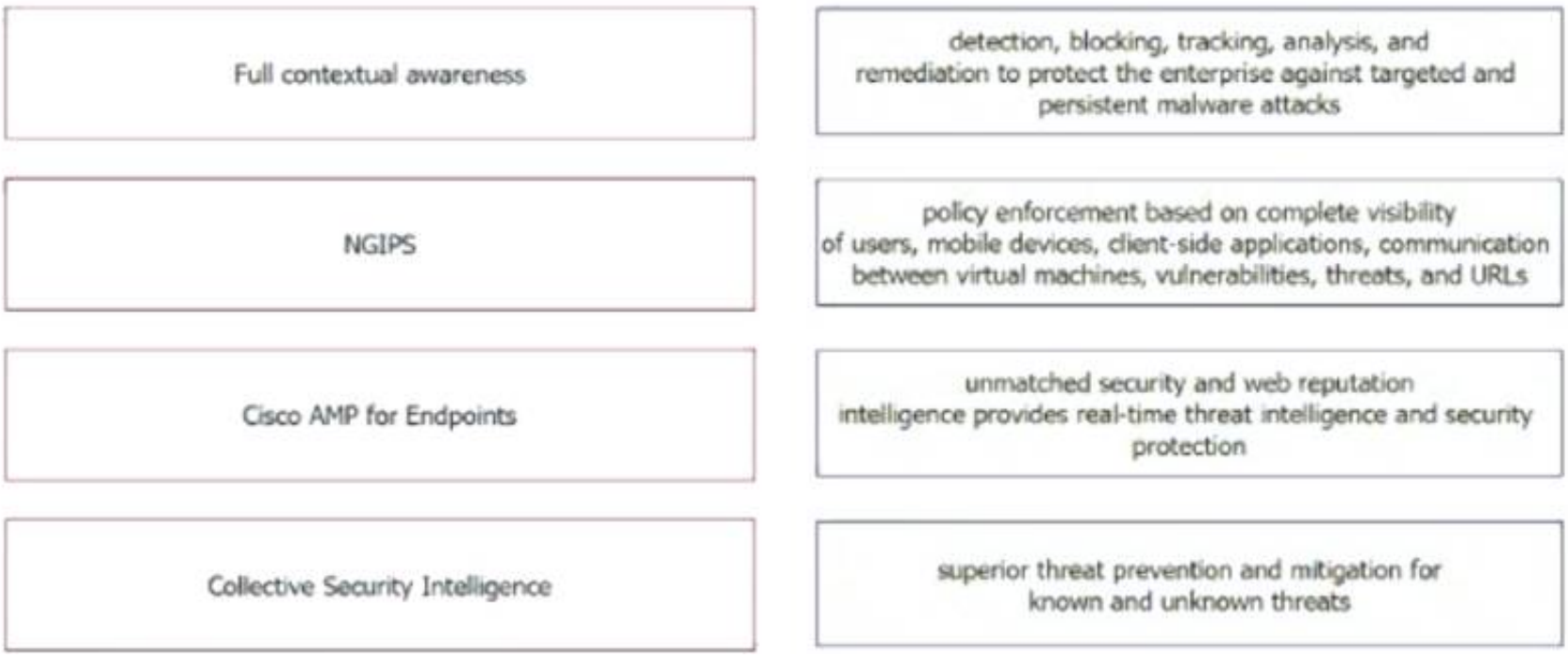
NEW QUESTION 450
- (Exam Topic 3)
What is the purpose of the Cisco Endpoint IoC feature?

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

Answer: A

Explanation:
Reference: https://docs.amp.cisco.com/Cisco%20Endpoint%20IOC%20Attributes.pdf
The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

NEW QUESTION 455
- (Exam Topic 3)
Drag and drop the security solutions from the left onto the benefits they provide on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 458
- (Exam Topic 3)
Which technology provides the benefit of Layer 3 through Layer 7 innovative deep packet inspection, enabling the platform to identify and output various applications within the network traffic flows?

A. Cisco NBAR2
B. Cisco ASAV
C. Account on Resolution
D. Cisco Prime Infrastructure

Answer: A

NEW QUESTION 463
- (Exam Topic 3)
What is the benefit of integrating Cisco ISE with a MDM solution?

A. It provides compliance checks for access to the network
B. It provides the ability to update other applications on the mobile device
C. It provides the ability to add applications to the mobile device through Cisco ISE
D. It provides network device administration access

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperab

NEW QUESTION 467
- (Exam Topic 3)
An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation. What must be un solution?

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

Answer: D

NEW QUESTION 469
- (Exam Topic 3)
What is the purpose of CA in a PKI?

A. To issue and revoke digital certificates
B. To validate the authenticity of a digital certificate
C. To create the private key for a digital certificate
D. To certify the ownership of a public key by the named subject

Answer: A

Explanation:
Reference: https://cheapsslsecurity.com/blog/understanding-the-role-of-certificate-authorities-in-pki/

NEW QUESTION 473
- (Exam Topic 3)
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. Configure a Cisco FMC to send syslogs to Cisco Stealthwatch Cloud
B. Deploy the Cisco Stealthwatch Cloud PNM sensor that sends data to Cisco Stealthwatch Cloud
C. Deploy a Cisco FTD sensor to send network events to Cisco Stealthwatch Cloud
D. Configure a Cisco FMC to send NetFlow to Cisco Stealthwatch Cloud

Answer: B

Explanation:
Reference:
https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/LTRSEC-2240-LG2.pdf

NEW QUESTION 474
- (Exam Topic 3)
An engineer is implementing Cisco CES in an existing Microsoft Office 365 environment and must route inbound email to Cisco CE.. record must be modified to accomplish this task?

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

Answer: B

NEW QUESTION 478
- (Exam Topic 3)
Which feature enables a Cisco ISR to use the default bypass list automatically for web filtering?

A. filters
B. group key
C. company key
D. connector

Answer: D

NEW QUESTION 483
- (Exam Topic 3)
Which Cisco network security device supports contextual awareness?

A. Firepower
B. CISCO ASA
C. Cisco IOS
D. ISE

Answer: D

NEW QUESTION 487
- (Exam Topic 3)
What are two recommended approaches to stop DNS tunneling for data exfiltration and command and control call backs? (Choose two.)

A. Use intrusion prevention system.
B. Block all TXT DNS records.
C. Enforce security over port 53.
D. Use next generation firewalls.
E. Use Cisco Umbrella.

Answer: CE

NEW QUESTION 492
- (Exam Topic 3)
Which Cisco Umbrella package supports selective proxy for Inspection of traffic from risky domains?

A. SIG Advantage
B. DNS Security Essentials
C. SIG Essentials
D. DNS Security Advantage

Answer: C

NEW QUESTION 497
- (Exam Topic 3)
Which Cisco Firewall solution requires zone definition?

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

Answer: C

NEW QUESTION 499
- (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 501
- (Exam Topic 3)
Which attribute has the ability to change during the RADIUS CoA?

A. NTP
B. Authorization
C. Accessibility
D. Membership

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec

NEW QUESTION 505
- (Exam Topic 3)
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? (Choose two.)

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

Answer: BE

NEW QUESTION 510
- (Exam Topic 3)
What are two functions of IKEv1 but not IKEv2? (Choose two)

A. NAT-T is supported in IKEv1 but rot in IKEv2.
B. With IKEv1, when using aggressive mode, the initiator and responder identities are passed cleartext
C. With IKEv1, mode negotiates faster than main mode
D. IKEv1 uses EAP authentication
E. IKEv1 conversations are initiated by the IKE_SA_INIT message

Answer: CE

NEW QUESTION 513
- (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 517

- (Exam Topic 3)
Why is it important to have a patching strategy for endpoints?

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

Answer: C

NEW QUESTION 521
- (Exam Topic 3)
Email security has become a high priority task for a security engineer at a large multi-national organization due to ongoing phishing campaigns. To help control this, the engineer has deployed an Incoming Content Filter with a URL reputation of (-10 00 to -6 00) on the Cisco ESA Which action will the system perform to disable any links in messages that match the filter?

A. Defang
B. Quarantine
C. FilterAction
D. ScreenAction

Answer: B

Explanation:
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/esa-content-filters.pdf

NEW QUESTION 522
- (Exam Topic 3)
What is the recommendation in a zero-trust model before granting access to corporate applications and resources?

A. to use multifactor authentication
B. to use strong passwords
C. to use a wired network, not wireless
D. to disconnect from the network when inactive

Answer: A

NEW QUESTION 527
- (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 529
- (Exam Topic 3)
What must be enabled to secure SaaS-based applications?

A. modular policy framework
B. two-factor authentication
C. application security gateway
D. end-to-end encryption

Answer: C

NEW QUESTION 530
- (Exam Topic 3)
When a next-generation endpoint security solution is selected for a company, what are two key deliverables that help justify the implementation? (Choose two.)

A. signature-based endpoint protection on company endpoints
B. macro-based protection to keep connected endpoints safe
C. continuous monitoring of all files that are located on connected endpoints
D. email integration to protect endpoints from malicious content that is located in email
E. real-time feeds from global threat intelligence centers

Answer: CE

NEW QUESTION 533
- (Exam Topic 3)
Which CLI command is used to enable URL filtering support for shortened URLs on the Cisco ESA?

A. webadvancedconfig

B. websecurity advancedconfig
C. outbreakconfig
D. websecurity config

Answer: B

NEW QUESTION 535
- (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 539
- (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 543
- (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 544
- (Exam Topic 3)
Which two parameters are used for device compliance checks? (Choose two.)

A. endpoint protection software version
B. Windows registry values
C. DHCP snooping checks
D. DNS integrity checks
E. device operating system version

Answer: CE

NEW QUESTION 548
- (Exam Topic 3)
Which service allows a user export application usage and performance statistics with Cisco Application Visibility and control?

A. SNORT
B. NetFlow
C. SNMP
D. 802.1X

Answer: B

Explanation:
Application Visibility and control (AVC) supports NetFlow to export application usage and performancestatistics. This data can be used for analytics, billing, and security policies.

NEW QUESTION 552
- (Exam Topic 3)
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

NEW QUESTION 554
- (Exam Topic 3)
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. PowerOn Auto Provisioning
D. Seed IP
E. CDP AutoDiscovery

Answer: CD

NEW QUESTION 555
- (Exam Topic 3)
Refer to the exhibit.

```
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
```

What will occur when this device tries to connect to the port?

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: B

NEW QUESTION 558
- (Exam Topic 3)
What is a benefit of using a multifactor authentication strategy?

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

Answer: D

NEW QUESTION 562
- (Exam Topic 3)
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. Set the sftunnel to go through the Cisco FTD
B. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices
C. Set the sftunnel port to 8305.
D. Manually change the management port on Cisco FMC and all managed Cisco FTD devices

Answer: D

NEW QUESTION 567
- (Exam Topic 3)
Which category includes DoS Attacks?

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

Answer: C

NEW QUESTION 572

- (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 576
- (Exam Topic 3)
What is the purpose of a NetFlow version 9 template record?

A. It specifies the data format of NetFlow processes.
B. It provides a standardized set of information about an IP flow.
C. lt defines the format of data records.
D. It serves as a unique identification number to distinguish individual data records

Answer: C

NEW QUESTION 580
- (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 581
- (Exam Topic 3)
A network engineer has configured a NTP server on a Cisco ASA. The Cisco ASA has IP reachability to the NTP server and is not filtering any traffic. The show ntp association detail command indicates that the configured NTP server is unsynchronized and has a stratum of 16. What is the cause of this issue?

A. Resynchronization of NTP is not forced
B. NTP is not configured to use a working server.
C. An access list entry for UDP port 123 on the inside interface is missing.
D. An access list entry for UDP port 123 on the outside interface is missing.

Answer: B

NEW QUESTION 584
- (Exam Topic 3)
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

NEW QUESTION 586

- (Exam Topic 3)
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. Create a Cisco pxGrid connection to NIST to import this information into the security products for policy use
B. 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.
C. Download the threat intelligence feed from the IETF and import it into the Cisco FTD and Cisco WSA databases
D. Configure the integrations with Talos Intelligence to take advantage of the threat intelligence that it provides.

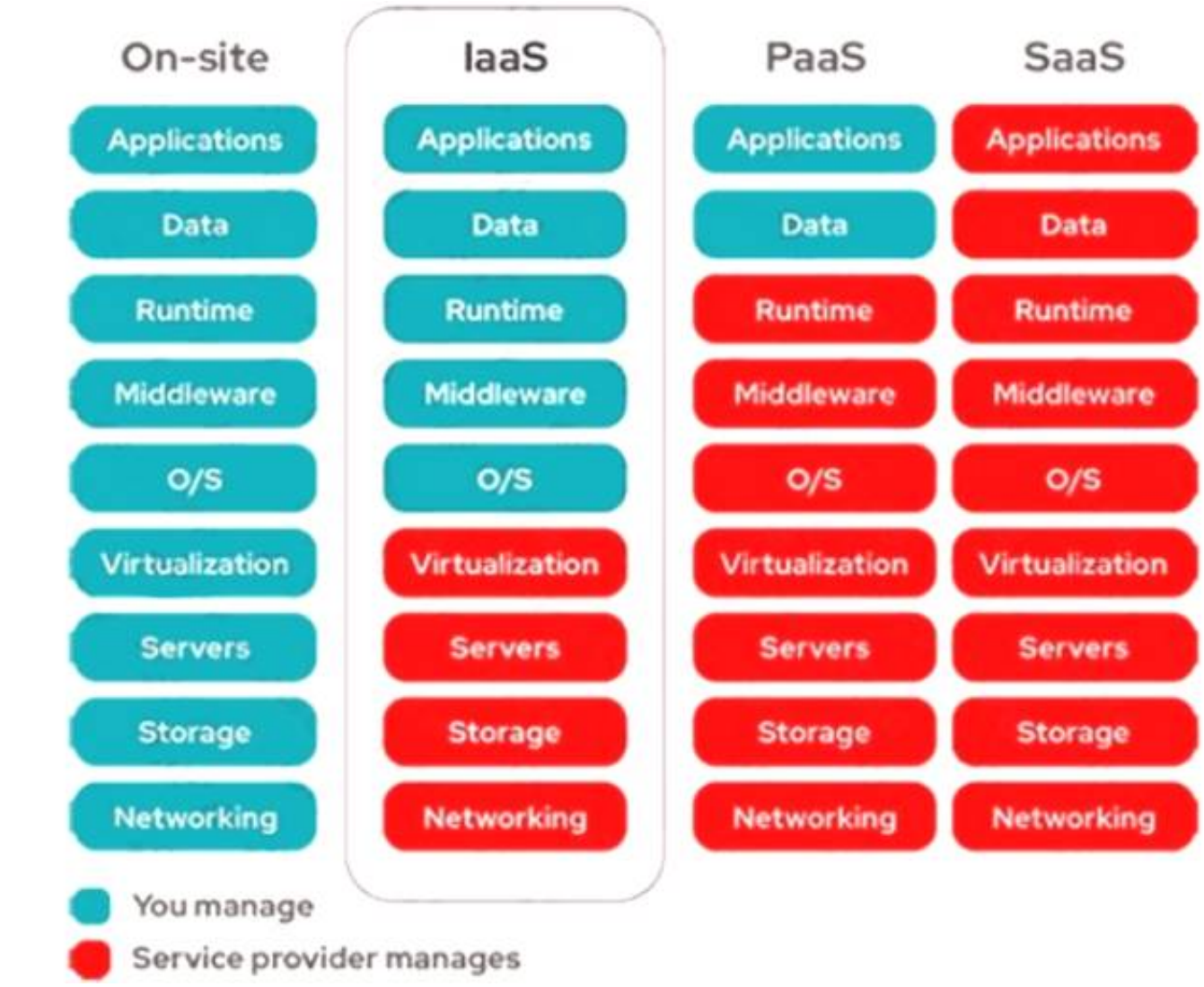
Answer: D

NEW QUESTION 587
- (Exam Topic 2)
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two)

A. virtualization
B. middleware
C. operating systems
D. applications
E. data

Answer: DE

Explanation:
Customers must manage applications and data in PaaS.



NEW QUESTION 588
- (Exam Topic 2)
What are two differences between a Cisco WSA that is running in transparent mode and one running in explicit mode? (Choose two)

A. The Cisco WSA responds with its own IP address only if it is running in explicit mode.
B. The Cisco WSA is configured in a web browser only if it is running in transparent mode.
C. The Cisco WSA responds with its own IP address only if it is running in transparent mode.
D. The Cisco WSA uses a Layer 3 device to redirect traffic only if it is running in transparent mode.
E. When the Cisco WSA is running in transparent mode, it uses the WSA's own IP address as the HTTP request destination.

Answer: AD

Explanation:
In explicit proxy mode, users are configured to use a web proxy and the web traffic is sent directly to the Cisco WSA. In contrast, in transparent proxy mode the Cisco WSA intercepts user's web traffic redirected from other network devices, such as switches, routers, or firewalls.

NEW QUESTION 591
- (Exam Topic 2)
With which components does a southbound API within a software-defined network architecture communicate?

A. controllers within the network
B. applications
C. appliances
D. devices such as routers and switches

Answer: D

Explanation:

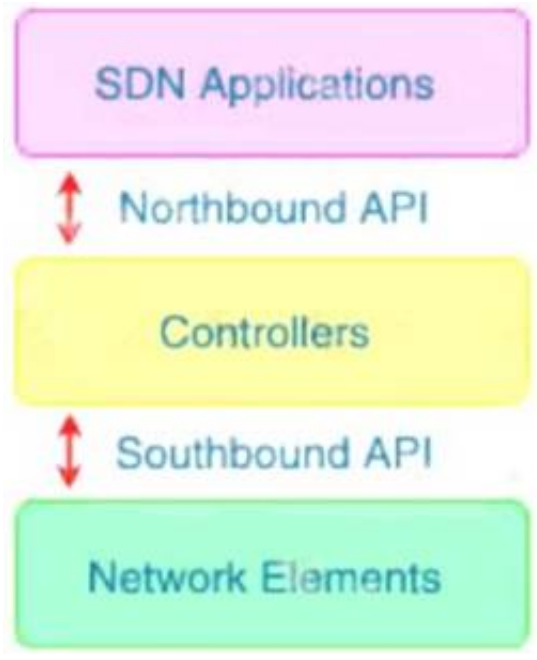
The Southbound API is used to communicate between Controllers and network devices.

NEW QUESTION 595
- (Exam Topic 2)
Which type of API is being used when a controller within a software-defined network architecture dynamically makes configuration changes on switches within the network?

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

Answer: B

Explanation:
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands andscalability needs.



NEW QUESTION 597
- (Exam Topic 2)
Which cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group?

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

Answer: B

Explanation:
Community Cloud allows system and services to be accessible by group of organizations. It
shares theinfrastructure between several organizations from a specific community. It may be managed internally byorganizations or by the third-party.

NEW QUESTION 602

- (Exam Topic 2)
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 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
D. The Cisco ASA can be configured for high availability whereas the Cisco IOS router with Zone-Based Policy Firewall cannot

Answer: A

NEW QUESTION 607
- (Exam Topic 2)
Which attack type attempts to shut down a machine or network so that users are not able to access it?

A. smurf
B. bluesnarfing
C. MAC spoofing
D. IP spoofing

Answer: A

Explanation:
Denial-of-service (DDoS) aims at shutting down a network or service, causing it to be inaccessible to itsintended users.The Smurf attack is a DDoS attack in which large numbers of Internet Control Message Protocol (ICMP)packets with the intended victim's spoofed source IP are broadcast to a computer network using an IPbroadcast address.

NEW QUESTION 609
- (Exam Topic 2)
What is the role of Cisco Umbrella Roaming when it is installed on an endpoint?

A. To protect the endpoint against malicious file transfers
B. To ensure that assets are secure from malicious links on and off the corporate network
C. To establish secure VPN connectivity to the corporate network
D. To enforce posture compliance and mandatory software

Answer: B

Explanation:
Umbrella Roaming is a cloud-delivered security service for Cisco's next-generation firewall. It protects your employees even when they are off the VPN.

NEW QUESTION 610
- (Exam Topic 2)
What are two characteristics of Cisco DNA Center APIs? (Choose two)

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

Answer: DE

NEW QUESTION 615
- (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 618
- (Exam Topic 2)
What is a difference between DMVPN and sVTI?

A. DMVPN supports tunnel encryption, whereas sVTI does not.
B. DMVPN supports dynamic tunnel establishment, whereas sVTI does not.
C. DMVPN supports static tunnel establishment, whereas sVTI does not.
D. DMVPN provides interoperability with other vendors, whereas sVTI does not.

Answer: B

NEW QUESTION 621
- (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 626
- (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 629
- (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: A

NEW QUESTION 634
- (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 636
- (Exam Topic 2)
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. Set content settings to High
B. Configure the intelligent proxy.
C. Use destination block lists.
D. Configure application block lists.

Answer: B

Explanation:
Reference: https://docs.umbrella.com/deployment-umbrella/docs/what-is-the-intelligent-proxy

NEW QUESTION 639
- (Exam Topic 2)
Which Dos attack uses fragmented packets to crash a target machine?

A. smurf
B. MITM
C. teardrop
D. LAND

Answer: C

Explanation:
A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a targetmachine. Since the machine receiving such packets cannot reassemble them due
to a bug in TCP/IPfragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

NEW QUESTION 642
- (Exam Topic 2)
What are two benefits of Flexible NetFlow records? (Choose two)

A. They allow the user to configure flow information to perform customized traffic identification
B. They provide attack prevention by dropping the traffic
C. They provide accounting and billing enhancements
D. They converge multiple accounting technologies into one accounting mechanism
E. They provide monitoring of a wider range of IP packet information from Layer 2 to 4

Answer: AD

Explanation:
Reference: https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon_external_docbase_0 d9.html#wp1057997Note: Traditional NetFlow allows us to monitor from Layer 2 to 4 but Flexible NetFlow goes beyond theselayers.

NEW QUESTION 646
- (Exam Topic 2)
An organization is receiving SPAM emails from a known malicious domain. What must be configured in order to prevent the session during the initial TCP communication?

A. Configure the Cisco ESA to drop the malicious emails
B. Configure policies to quarantine malicious emails
C. Configure policies to stop and reject communication
D. Configure the Cisco ESA to reset the TCP connection

Answer: D

NEW QUESTION 650
- (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 653
- (Exam Topic 2)
Refer to the exhibit.

```
import requests
client_id = '<Client id>'
api_key = '<API Key>'
url = 'https://api.amp.cisco.com/v1/computers'
response = requests.get(url, auth=(client_id, api_key))
response_json = response.json()
for computer in response_json['data']
    hostname = computer['hostname']
    print(hostname)
```

What will happen when the Python script is executed?

A. The hostname will be translated to an IP address and printed.
B. The hostname will be printed for the client in the client ID field.
C. The script will pull all computer hostnames and print them.
D. The script will translate the IP address to FODN and print it

Answer: C

NEW QUESTION 658
- (Exam Topic 2)
Refer to the exhibit.

```
Info: New SMTP ICID 30 interface Management (192.168.0.100)
   address 10.128.128.200 reverse dns host unknown verified no
Info: ICID 30 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS None
Info: ICID 30 TLS success protocol TLSv1 cipher
   DHE-RSA-AES256-SHA
Info: SMTP Auth: (ICID 30) succeeded for user: cisco using
   AUTH mechanism: LOGIN with profile: ldap_smtp
Info: MID 80 matched all recipients for per-recipient policy
   DEFAULT in the outbound table
```

Which type of authentication is in use?

A. LDAP authentication for Microsoft Outlook
B. POP3 authentication
C. SMTP relay server authentication
D. external user and relay mail authentication

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118844-technoteesa-00.htmlThe exhibit in this Qshows a successful TLS connection from the remote host (reception) in the mail log.

NEW QUESTION 661
- (Exam Topic 2)
A network administrator needs to find out what assets currently exist on the network. Third-party systems need to be able to feed host data into Cisco Firepower. What must be configured to accomplish this?

A. a Network Discovery policy to receive data from the host
B. a Threat Intelligence policy to download the data from the host
C. a File Analysis policy to send file data into Cisco Firepower
D. a Network Analysis policy to receive NetFlow data from the host

Answer: A

Explanation:
You can configure discovery rules to tailor the discovery of host and application data to your needs.The Firepower System can use data from NetFlow exporters to generate connection and discovery events, and to add host and application data to the network map.A network analysis policy governs how traffic is decoded and preprocessed so it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt -> Answer D is not correct.

NEW QUESTION 662
- (Exam Topic 2)
Which term describes when the Cisco Firepower downloads threat intelligence updates from Cisco Talos?

A. consumption

B. sharing
C. analysis
D. authoring

Answer: A

Explanation:
we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's FirepowerManagement Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector

NEW QUESTION 665
- (Exam Topic 2)
Which two cryptographic algorithms are used with IPsec? (Choose two)

A. AES-BAC
B. AES-ABC
C. HMAC-SHA1/SHA2
D. Triple AMC-CBC
E. AES-CBC

Answer: CE

Explanation:
Cryptographic algorithms defined for use with IPsec include:+ HMAC-SHA1/SHA2 for integrity protection and authenticity.+ TripleDES-CBC for confidentiality+ AES-CBC and AES-CTR for confidentiality.+ AES-GCM and ChaCha20-Poly1305 providing confidentiality and authentication together efficiently.

NEW QUESTION 670
- (Exam Topic 2)
Refer to the exhibit.

```
import requests
url = https://api.amp.cisco.com/v1/computers
headers = {
    'accept' : application/json
    'content-type' : application/json
    'authorization' : Basic API Credentials
    'cache-control' : "no cache"
}
response = requests.request ("GET", url, headers = headers)
print (response.txt)
```

What will happen when this Python script is run?

A. The compromised computers and malware trajectories will be received from Cisco AMP
B. The list of computers and their current vulnerabilities will be received from Cisco AMP
C. The compromised computers and what compromised them will be received from Cisco AMP
D. The list of computers, policies, and connector statuses will be received from Cisco AMP

Answer: D

Explanation:
Reference:
https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.apjc.

NEW QUESTION 671
- (Exam Topic 2)
What is a key difference between Cisco Firepower and Cisco ASA?

A. Cisco ASA provides access control while Cisco Firepower does not.
B. Cisco Firepower provides identity-based access control while Cisco ASA does not.
C. Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not.
D. Cisco ASA provides SSL inspection while Cisco Firepower does not.

Answer: C

NEW QUESTION 676
- (Exam Topic 2)
Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps.
Which two actions must be taken to ensure that interfaces are put back into service? (Choose two)

A. Have Cisco Prime Infrastructure issue an SNMP set command to re-enable the ports after the pre configured interval.
B. Use EEM to have the ports return to service automatically in less than 300 seconds.
C. Enter the shutdown and no shutdown commands on the interfaces.
D. Enable the snmp-server enable traps command and wait 300 seconds
E. Ensure that interfaces are configured with the error-disable detection and recovery feature

Answer: CE

Explanation:
You can also bring up the port by using these commands:+ The “shutdown” interface configuration command followed by the “no shutdown” interface configurationcommand restarts the disabled port.+ The “errdisable recovery cause …” global configuration command enables the timer to automatically recover error-disabled state, and the “errdisable recovery interval interval” global configuration command specifies the time to recover error-disabled state.

NEW QUESTION 678
.....

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