Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

NEW QUESTION 1
- (Exam Topic 2)
Which attack is preventable by Cisco ESA but not by the Cisco WSA?

A. buffer overflow
B. DoS
C. SQL injection
D. phishing

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advance

NEW QUESTION 2
- (Exam Topic 2)
What does Cisco AMP for Endpoints use to help an organization detect different families of malware?

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

Answer: A

Explanation:
Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdfETHOS = Fuzzy Fingerprinting using static/passive heuristics
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/BRKSEC-2139.pdf

NEW QUESTION 3
- (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 4
- (Exam Topic 2)
What is a benefit of conducting device compliance checks?

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

Answer: B

NEW QUESTION 5
- (Exam Topic 2)
An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco Firepower. Which feature should be used to accomplish this?

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

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper

NEW QUESTION 6
- (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 7
- (Exam Topic 2)
Which public cloud provider supports the Cisco Next Generation Firewall Virtual?

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

Answer: D

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

NEW QUESTION 8
- (Exam Topic 2)
Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.

PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A picture containing table Description automatically generated

NEW QUESTION 9
- (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 10
- (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 10
- (Exam Topic 2)
How does Cisco Advanced Phishing Protection protect users?

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

Answer: D

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

NEW QUESTION 11
- (Exam Topic 2)
What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group?

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

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide

NEW QUESTION 13
- (Exam Topic 2)
An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?

A. SIEM
B. CASB
C. Adaptive MFA
D. Cisco Cloudlock

Answer: D

Explanation:
Reference: https://docs.umbrella.com/cloudlock-documentation/docs/endpointsNote:+ Security information and event management (SIEM) platforms collect log and event data from securitysystems, networks and computers, and turn it into actionable security insights.+ An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when acondition of an alerting policy has been met.

NEW QUESTION 18
- (Exam Topic 2)
What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

A. Multiple NetFlow collectors are supported
B. Advanced NetFlow v9 templates and legacy v5 formatting are supported
C. Secure NetFlow connections are optimized for Cisco Prime Infrastructure
D. Flow-create events are delayed

Answer: B

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

NEW QUESTION 20
- (Exam Topic 2)
What are two DDoS attack categories? (Choose two)

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

Answer: BD

Explanation:
There are three basic categories of attack:+ volume-based attacks, which use high traffic to inundate the network bandwidth+ protocol attacks, which focus on exploiting server resources+ application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks
Reference: https://www.esecurityplanet.com/networks/types-of-ddos-attacks/

NEW QUESTION 24
- (Exam Topic 2)
Refer to the exhibit.

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

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

Answer: D

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

NEW QUESTION 28
- (Exam Topic 2)
What is a benefit of using Cisco FMC over Cisco ASDM?

A. Cisco FMC uses Java while Cisco ASDM uses HTML5.
B. Cisco FMC provides centralized management while Cisco ASDM does not.
C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.
D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheetc78-736775.ht

NEW QUESTION 29
- (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 34
- (Exam Topic 2)
Drag and drop the capabilities from the left onto the correct technologies on the right.

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, chat or text message Description automatically generated

NEW QUESTION 37
- (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 40
- (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 42
- (Exam Topic 1)

What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?

A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX

Answer: C

Explanation:
Configure a Crypto ISAKMP Key
In order to configure a preshared
configuration mode:
authentication key, enter thcerypto isakmp key
command in global
crypto isakmp key cisco123 address 172.16.1.1
https://community.cisco.com/t5/vpn/isakmp-with-0-0-0-0-dmvpn/td-p/4312380
It is a bad practice but it is valid. 172.16.0.0/16 the full range will be accepted as possible PEER
https://www.examtopics.com/discussions/cisco/view/46191-exam-350-701-topic-1-question-71-discussion/#:~:t Testing without a netmask shows that command interpretation has a preference for /16 and /24.
CSR-1(config)#crypto isakmp key cisco123 address 172.16.0.0
CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.0.0 [255.255.0.0] cisco123
CSR-1(config)#no crypto isakmp key cisco123 address 172.16.0.0 CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.0 CSR-1(config)#do show crypto isakmp key | i cisco
default 172.16.1.0 [255.255.255.0] cisco123
CSR-1(config)#no crypto isakmp key cisco123 address 172.16.1.0 CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.128
CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.1.128 cisco123 CSR-1(config)#

NEW QUESTION 46
- (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 51
- (Exam Topic 1)
An organization is trying to improve their Defense in Depth by blocking malicious destinations prior to a connection being established. The solution must be able to block certain applications from being used within the network. Which product should be used to accomplish this goal?

A. Cisco Firepower
B. Cisco Umbrella
C. ISE
D. AMP

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.

NEW QUESTION 55
- (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 59
- (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 61

- (Exam Topic 1)
Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

A. AMP
B. AnyConnect
C. DynDNS
D. Talos

Answer: D

Explanation:
When Umbrella receives a DNS request, it uses intelligence to determine if the request is safe, malicious or risky — meaning the domain contains both malicious and legitimate content. Safe and malicious requests are routed as usual or blocked, respectively. Risky requests are routed to our cloud-based proxy for deeper inspection. The Umbrella proxy uses Cisco Talos web reputation and other third-party feeds to determine if a URL is malicious.

NEW QUESTION 65
- (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 66
- (Exam Topic 1)
A mall provides security services to customers with a shared appliance. The mall wants separation of management on the shared appliance. Which ASA deployment mode meets these needs?

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

Answer: C

NEW QUESTION 68
- (Exam Topic 1)
An engineer configured a new network identity in Cisco Umbrella but must verify that traffic is being routed through the Cisco Umbrella network. Which action tests the routing?

A. Ensure that the client computers are pointing to the on-premises DNS servers.
B. Enable the Intelligent Proxy to validate that traffic is being routed correctly.
C. Add the public IP address that the client computers are behind to a Core Identity.
D. Browse to http://welcome.umbrella.com/ to validate that the new identity is working.

Answer: B

NEW QUESTION 71
- (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 76
- (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 78
- (Exam Topic 1)
A network engineer is configuring DMVPN and entered the crypto isakmp key cisc0380739941 address 1.1.1.1 command on hostA. The tunnel is not being established to hostB. What action is needed to authenticate the VPN?

A. Change isakmp to ikev2 in the command on hostA.
B. Enter the command with a different password on hostB.
C. Enter the same command on hostB.
D. Change the password on hostA to the default password.

Answer: C

NEW QUESTION 79
- (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 84
- (Exam Topic 1)
Which information is required when adding a device to Firepower Management Center?

A. username and password
B. encryption method
C. device serial number
D. registration key

Answer: D

NEW QUESTION 89
- (Exam Topic 1)
Which two risks is a company vulnerable to if it does not have a well-established patching solution for endpoints? (Choose two)

A. exploits
B. ARP spoofing
C. denial-of-service attacks
D. malware
E. eavesdropping

Answer: AD

Explanation:
Malware means “malicious software”, is any software intentionally designed to cause damage to a computer, server, client, or computer network. The most popular types of malware includes viruses, ransomware and spyware. Virus Possibly the most common type of malware, viruses attach their malicious code to clean code and wait to be run.
Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again.Spyware is spying software that can secretly record everything you enter, upload, download, and store on your computers or mobile devices. Spyware always tries to keep itself hidden.An exploit is a code that takes advantage of a software vulnerability or security flaw.Exploits and malware are two risks for endpoints that are not up to date. ARP spoofing and eavesdropping are attacks against the network while denial-of-service attack is based on the flooding of IP packets.

NEW QUESTION 92
- (Exam Topic 1)
What is a feature of the open platform capabilities of Cisco DNA Center?

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

Answer: A

NEW QUESTION 95

- (Exam Topic 1)
Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two)

A. packet decoder
B. SIP
C. modbus
D. inline normalization
E. SSL

Answer: BE

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Applic uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

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 100
- (Exam Topic 1)
Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?

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

Answer: A

NEW QUESTION 105
- (Exam Topic 1)
Which two mechanisms are used to control phishing attacks? (Choose two)

A. Enable browser alerts for fraudulent websites.
B. Define security group memberships.
C. Revoke expired CRL of the websites.
D. Use antispyware software.
E. Implement email filtering techniques.

Answer: AE

NEW QUESTION 108
- (Exam Topic 1)
An engineer wants to automatically assign endpoints that have a specific OUI into a new endpoint group.
Which probe must be enabled for this type of profiling to work?

A. NetFlow
B. NMAP
C. SNMP
D. DHCP

Answer: B

Explanation:
Reference:
http://www.network-node.com/blog/2016/1/2/ise-20-profiling

NEW QUESTION 112
- (Exam Topic 1)
In which two ways does a system administrator send web traffic transparently to the Web Security Appliance? (Choose two)

A. configure Active Directory Group Policies to push proxy settings
B. configure policy-based routing on the network infrastructure
C. reference a Proxy Auto Config file

D. configure the proxy IP address in the web-browser settings
E. use Web Cache Communication Protocol

Answer: BE

NEW QUESTION 115
- (Exam Topic 1)
What are two list types within AMP for Endpoints Outbreak Control? (Choose two)

A. blocked ports
B. simple custom detections
C. command and control
D. allowed applications
E. URL

Answer: BD

Explanation:
Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists.A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect andquarantine.Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company Reference: https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf

NEW QUESTION 120
- (Exam Topic 1)
Which two features of Cisco Email Security can protect your organization against email threats? (Choose two)

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

Answer: BD

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

NEW QUESTION 122
- (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 125
- (Exam Topic 1)
The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the ASA be added on the Cisco UC Manager platform?

A. Certificate Trust List
B. Endpoint Trust List
C. Enterprise Proxy Service
D. Secured Collaboration Proxy

Answer: A

NEW QUESTION 126
- (Exam Topic 1)
Which two deployment modes does the Cisco ASA FirePower module support? (Choose two)

A. transparent mode
B. routed mode
C. inline mode
D. active mode
E. passive monitor-only mode

Answer: CD

Explanation:
Reference:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/firewall/asa-firewall-asdm/modules-sfr.html

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 IPS engine detects ARP spoofing?

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

Answer: A

NEW QUESTION 132
- (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 136
- (Exam Topic 1)
Which attack is commonly associated with C and C++ programming languages?

A. cross-site scripting
B. water holing
C. DDoS
D. buffer overflow

Answer: D

Explanation:

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.
Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's alloted memory space. This happens quite frequently in the case of arrays.

NEW QUESTION 140
- (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 142
- (Exam Topic 1)
What is a difference between FlexVPN and DMVPN?

A. DMVPN uses IKEv1 or IKEv2, FlexVPN only uses IKEv1
B. DMVPN uses only IKEv1 FlexVPN uses only IKEv2
C. FlexVPN uses IKEv2, DMVPN uses IKEv1 or IKEv2
D. FlexVPN uses IKEv1 or IKEv2, DMVPN uses only IKEv2

Answer: C

NEW QUESTION 145
- (Exam Topic 1)
Which action controls the amount of URI text that is stored in Cisco WSA logs files?

A. Configure the datasecurityconfig command
B. Configure the advancedproxyconfig command with the HTTPS subcommand
C. Configure a small log-entry size.
D. Configure a maximum packet size.

Answer: B

NEW QUESTION 148
- (Exam Topic 1)
Which two activities can be done using Cisco DNA Center? (Choose two)

A. DHCP
B. Design
C. Accounting
D. DNS
E. Provision

Answer: BE

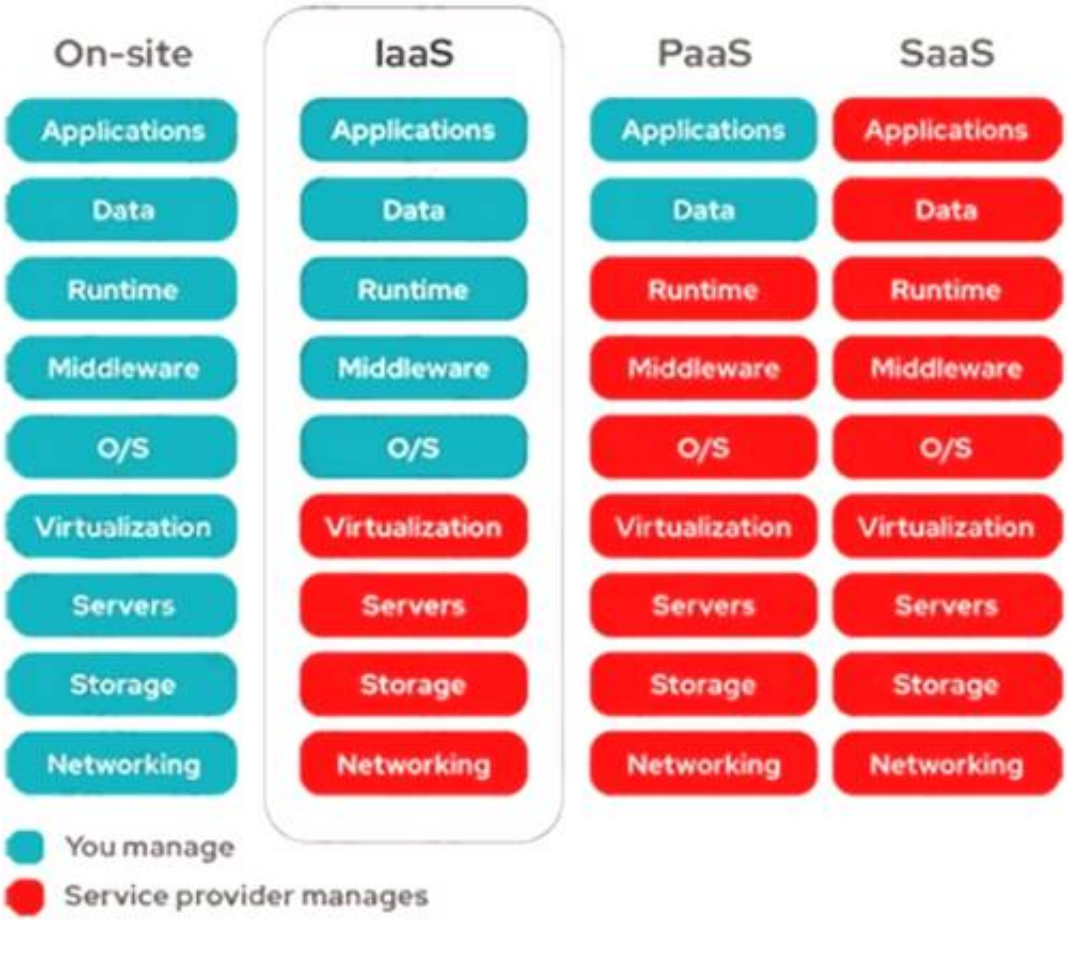
Explanation:
Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-so-cte-en.html

NEW QUESTION 149
- (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 150
- (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 151
- (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 154
- (Exam Topic 1)
Which two behavioral patterns characterize a ping of death attack? (Choose two)

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

Answer: BD

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

NEW QUESTION 158
- (Exam Topic 1)
Elliptic curve cryptography is a stronger more efficient cryptography method meant to replace which current encryption technology?

A. 3DES
B. RSA
C. DES
D. AES

Answer: B

Explanation:

Compared to RSA, the prevalent public-key cryptography of the Internet today, Elliptic Curve Cryptography (ECC) offers smaller key sizes, faster computation,as well as memory, energy and bandwidth savings and is thus better suited forsmall devices.

NEW QUESTION 163
- (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 168
- (Exam Topic 1)
An administrator wants to ensure that all endpoints are compliant before users are allowed access on the corporate network. The endpoints must have the corporate antivirus application installed and be running the latest build of Windows 10.
What must the administrator implement to ensure that all devices are compliant before they are allowed on the network?

A. Cisco Identity Services Engine and AnyConnect Posture module
B. Cisco Stealthwatch and Cisco Identity Services Engine integration
C. Cisco ASA firewall with Dynamic Access Policies configured
D. Cisco Identity Services Engine with PxGrid services enabled

Answer: A

NEW QUESTION 173
- (Exam Topic 1)
What is the difference between deceptive phishing and spear phishing?

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

Answer: B

Explanation:

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

NEW QUESTION 178
- (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 179
- (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 183
- (Exam Topic 1)
Which two capabilities does TAXII support? (Choose two)

A. Exchange
B. Pull messaging
C. Binding
D. Correlation
E. Mitigating

Answer: AB

Explanation:
The Trusted Automated eXchangeof Indicator Information (TAXII) specifies mechanisms for exchangingstructured cyber threat information between parties over the network.TAXII exists to provide specific capabilities to those interested in sharing structured cyber threat information.TAXII Capabilities are the highest level at which TAXII actions can be described. There are three capabilitiesthat this version of TAXII supports: push messaging, pull messaging, and discovery.Although there is no “binding” capability in the list but it is the best answer here.

NEW QUESTION 187
- (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 189
- (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 191
- (Exam Topic 1)
Which feature requires a network discovery policy on the Cisco Firepower Next Generation Intrusion Prevention System?

A. Security Intelligence
B. Impact Flags
C. Health Monitoring
D. URL Filtering

Answer: B

NEW QUESTION 192
- (Exam Topic 1)
Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two)

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

Answer: AC

NEW QUESTION 196
- (Exam Topic 1)
Where are individual sites specified to be blacklisted in Cisco Umbrella?

A. application settings
B. content categories

C. security settings
D. destination lists

Answer: D

Explanation:
Reference: https://docs.umbrella.com/deployment-umbrella/docs/working-with-destination-lists

NEW QUESTION 197
- (Exam Topic 1)
Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two)

A. DDoS
B. antispam
C. antivirus
D. encryption
E. DLP

Answer: DE

Explanation:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security

NEW QUESTION 201
- (Exam Topic 3)
What is a functional difference between Cisco AMP for Endpoints and Cisco Umbrella Roaming Client?

A. The Umbrella Roaming client stops and tracks malicious activity on hosts, and AMP for Endpoints tracks only URL-based threats.
B. The Umbrella Roaming Client authenticates users and provides segmentation, and AMP for Endpoints allows only for VPN connectivity
C. AMP for Endpoints authenticates users and provides segmentation, and the Umbrella Roaming Client allows only for VPN connectivity.
D. AMP for Endpoints stops and tracks malicious activity on hosts, and the Umbrella Roaming Client tracks only URL-based threats.

Answer: D

NEW QUESTION 205
- (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 208
- (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 210
- (Exam Topic 3)
How does Cisco Workload Optimization Manager help mitigate application performance issues?

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

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/one-enterprisesuite/solution-o

NEW QUESTION 212
- (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 214
- (Exam Topic 3)
An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1 1 11 using the flow record Stea!thwatch406397954 command Which additional command is required to complete the flow record?

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

Answer: B

NEW QUESTION 215
- (Exam Topic 3)
A customer has various external HTTP resources available including Intranet. Extranet, and Internet, with a proxy configuration running in explicit mode Which method allows the client desktop browsers to be configured to select when to connect direct or when to use the proxy?

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

Answer: C

NEW QUESTION 216
- (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 221
- (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

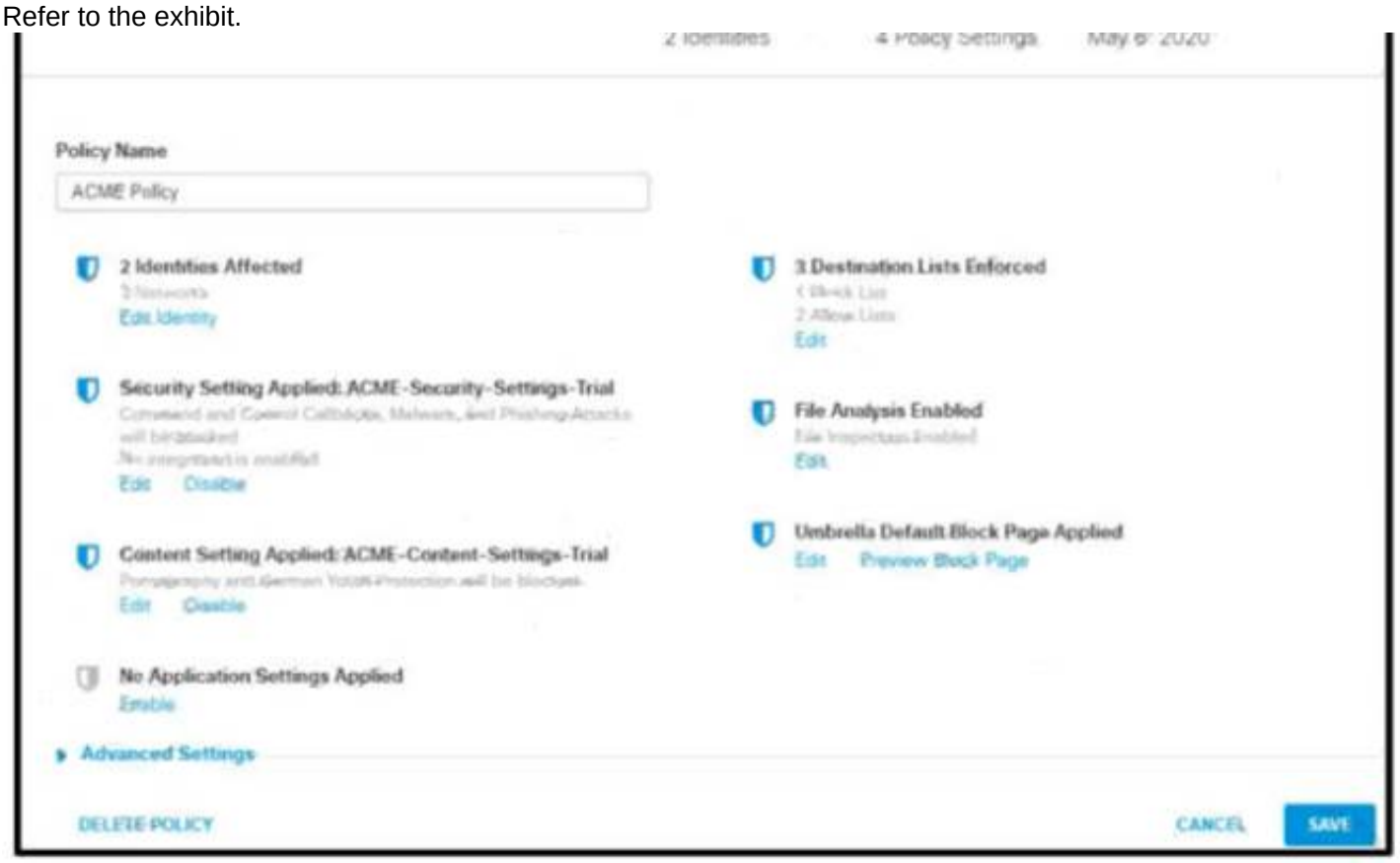
NEW QUESTION 224
- (Exam Topic 3)
An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users.

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

D. Import the Umbrella root CA into the trusted root store on the user's device.

Answer: A

NEW QUESTION 229
- (Exam Topic 3)
Refer to the exhibit.



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

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

Answer: B

NEW QUESTION 230
- (Exam Topic 3)
Which technology provides a combination of endpoint protection endpoint detection, and response?

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

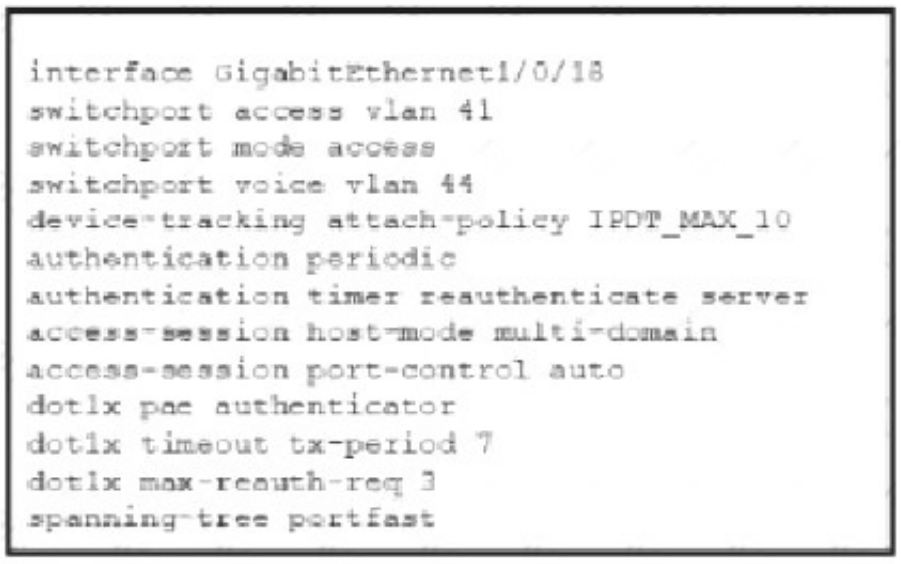
Answer: A

NEW QUESTION 235
- (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 240
- (Exam Topic 3)
Refer to the exhibit.



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.

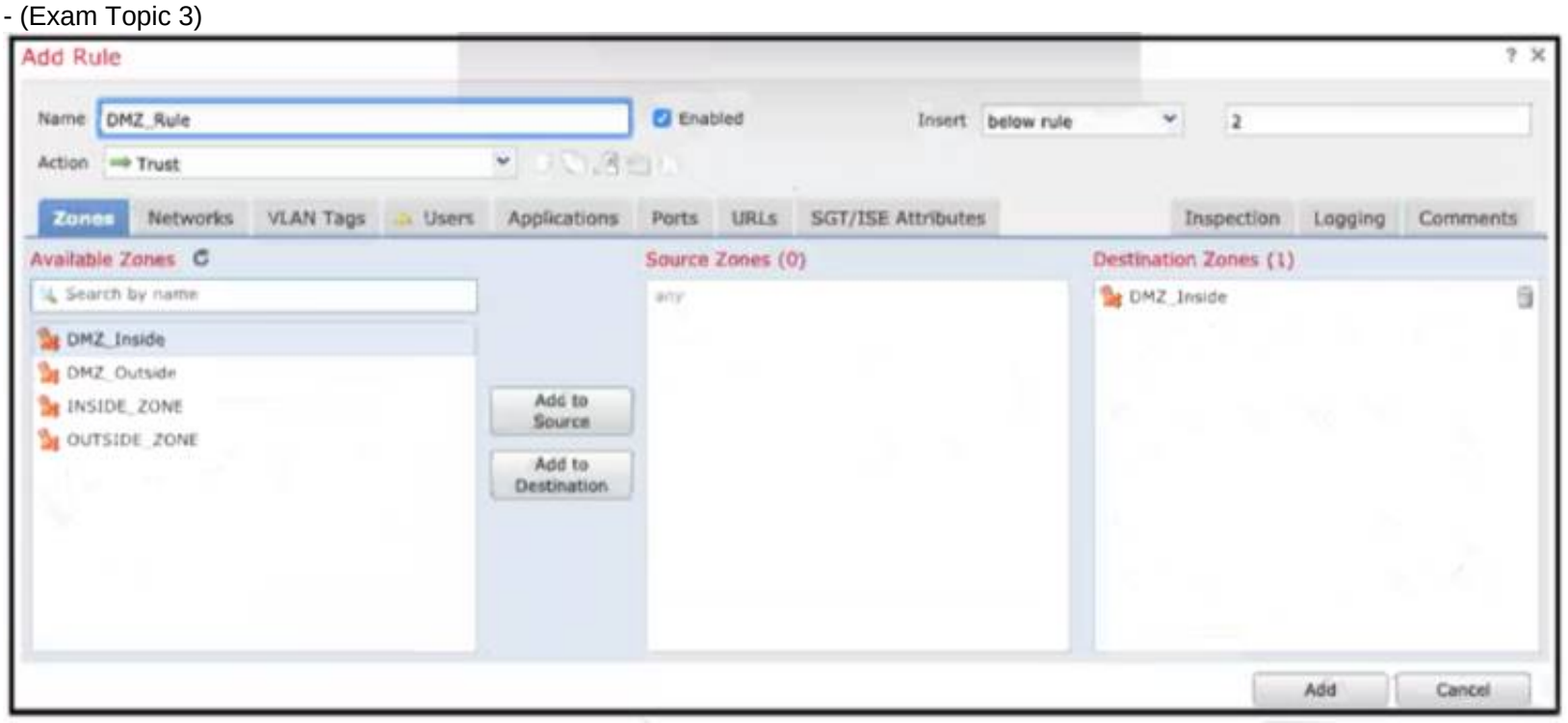
Answer: D

NEW QUESTION 241
- (Exam Topic 3)
Which two capabilities does an MDM provide? (Choose two.)

A. delivery of network malware reports to an inbox in a schedule
B. unified management of mobile devices, Macs, and PCs from a centralized dashboard
C. enforcement of device security policies from a centralized dashboard
D. manual identification and classification of client devices
E. unified management of Android and Apple devices from a centralized dashboard

Answer: BC

NEW QUESTION 246
- (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 250
- (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 252
- (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 253
- (Exam Topic 3)
An engineer adds a custom detection policy to a Cisco AMP deployment and encounters issues with the configuration. The simple detection mechanism is configured, but the dashboard indicates that the hash is not 64 characters and is non-zero. What is the issue?

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

Answer: A

NEW QUESTION 258
- (Exam Topic 3)
What does Cisco ISE use to collect endpoint attributes that are used in profiling?

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

Answer: A

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

NEW QUESTION 263
- (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 265
- (Exam Topic 3)
Refer to the exhibit.

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

An engineer is implementing a certificate based VPN. What is the result of the existing configuration?

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

Answer: A

NEW QUESTION 269
- (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 270
- (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

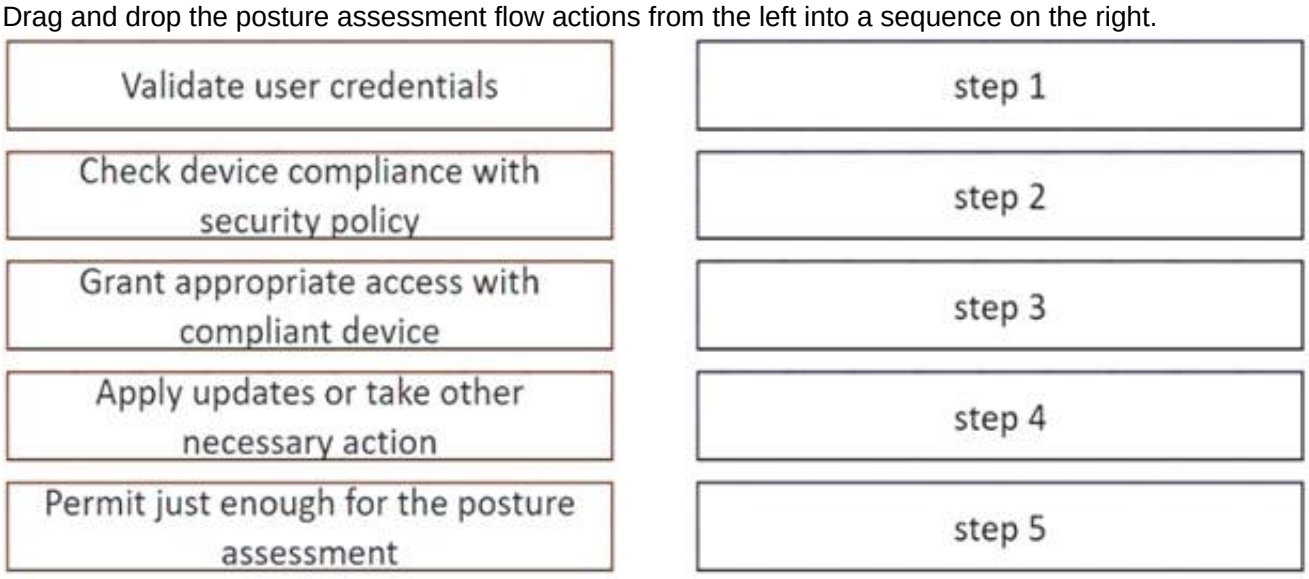
Answer: C

NEW QUESTION 272
- (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

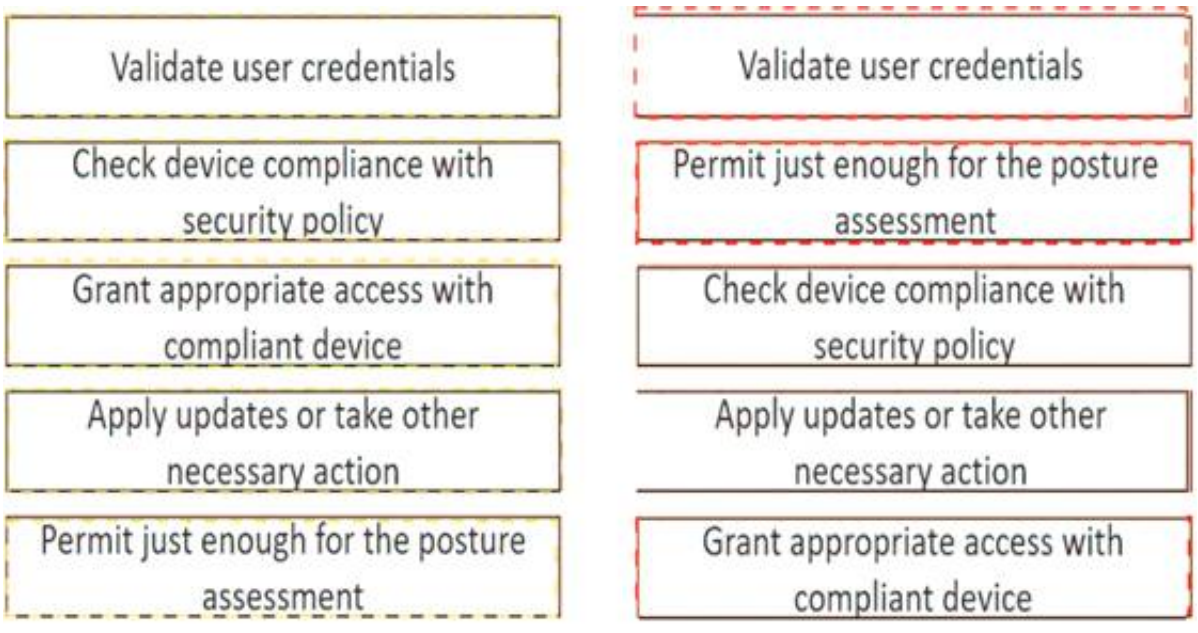
NEW QUESTION 274
- (Exam Topic 3)
Drag and drop the posture assessment flow actions from the left into a sequence on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 278
- (Exam Topic 3)
What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.)

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

Answer: AC

NEW QUESTION 279
- (Exam Topic 3)
Which two actions does the Cisco Identity Services Engine posture module provide that ensures endpoint security? (Choose two.)

A. Assignments to endpoint groups are made dynamically, based on endpoint attributes.
B. Endpoint supplicant configuration is deployed.
C. A centralized management solution is deployed.
D. Patch management remediation is performed.
E. The latest antivirus updates are applied before access is allowed.

Answer: AD

NEW QUESTION 280
- (Exam Topic 3)
An engineer is configuring web filtering for a network using Cisco Umbrella Secure Internet Gateway. The requirement is that all traffic needs to be filtered. Using the SSL decryption feature, which type of certificate should be presented to the end-user to accomplish this goal?

A. third-party
B. self-signed
C. organization owned root
D. SubCA

Answer: C

NEW QUESTION 283
- (Exam Topic 3)
A network engineer entered the snmp-server user asmith myv7 auth sha cisco priv aes 256 cisc0xxxxxxxxx command and needs to send SNMP information to a host at 10.255.255.1. Which
command achieves this goal?

A. snmp-server host inside 10.255.255.1 version 3 myv7
B. snmp-server host inside 10.255.255.1 snmpv3 myv7
C. snmp-server host inside 10.255.255.1 version 3 asmith
D. snmp-server host inside 10.255.255.1 snmpv3 asmith

Answer: C

NEW QUESTION 286
- (Exam Topic 3)
What is the purpose of joining Cisco WSAs to an appliance group?

A. All WSAs in the group can view file analysis results.
B. The group supports improved redundancy
C. It supports cluster operations to expedite the malware analysis process.
D. It simplifies the task of patching multiple appliances.

Answer: A

NEW QUESTION 287
- (Exam Topic 3)

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

Refer to the exhibit. What is the result of using this authentication protocol in the configuration?

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

Answer: D

NEW QUESTION 289
- (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 290
- (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 291
- (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

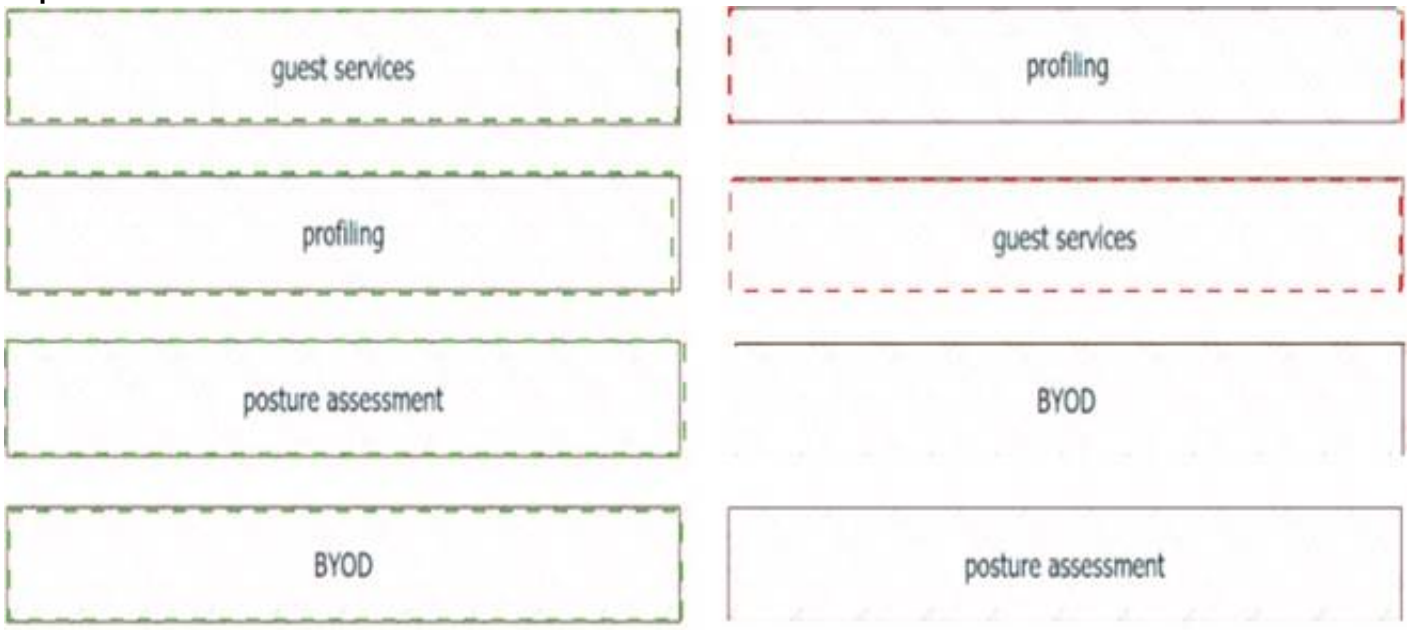
Answer: C

NEW QUESTION 292
- (Exam Topic 3)
Drag and drop the concepts from the left onto the correct descriptions on the right

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 295
- (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 297
- (Exam Topic 3)
What is the target in a phishing attack?

A. perimeter firewall
B. IPS
C. web server
D. endpoint

Answer: D

NEW QUESTION 299
- (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 301
- (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 303
- (Exam Topic 3)
Which action must be taken in the AMP for Endpoints console to detect specific MD5 signatures on endpoints and then quarantine the files?

A. Configure an advanced custom detection list.
B. Configure an IP Block & Allow custom detection list
C. Configure an application custom detection list
D. Configure a simple custom detection list

Answer: A

NEW QUESTION 308
- (Exam Topic 3)
Which RADIUS feature provides a mechanism to change the AAA attributes of a session after it is authenticated?

A. Authorization
B. Accounting
C. Authentication
D. CoA

Answer: D

NEW QUESTION 313
- (Exam Topic 3)
Drag and drop the exploits from the left onto the type of security vulnerability on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 315
- (Exam Topic 3)
A company recently discovered an attack propagating throughout their Windows network via a file named abc428565580xyz exe The malicious file was uploaded to a Simple Custom Detection list in the AMP for Endpoints Portal and the currently applied policy for the Windows clients was updated to reference the detection list Verification testing scans on known infected systems shows that AMP for Endpoints is not detecting the presence of this file as an indicator of compromise What must be performed to ensure detection of the malicious file?

A. Upload the malicious file to the Blocked Application Control List
B. Use an Advanced Custom Detection List instead of a Simple Custom Detection List
C. Check the box in the policy configuration to send the file to Cisco Threat Grid for dynamic analysis
D. Upload the SHA-256 hash for the file to the Simple Custom Detection List

Answer: D

NEW QUESTION 317
- (Exam Topic 3)
Which IETF attribute is supported for the RADIUS CoA feature?

A. 24 State
B. 30 Calling-Station-ID
C. 42 Acct-Session-ID
D. 81 Message-Authenticator

Answer: A

NEW QUESTION 320
- (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 325
- (Exam Topic 3)
Which endpoint solution protects a user from a phishing attack?

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

Answer: D

NEW QUESTION 330
- (Exam Topic 3)
Which endpoint protection and detection feature performs correlation of telemetry, files, and intrusion events that are flagged as possible active breaches?

A. retrospective detection
B. indication of compromise
C. file trajectory
D. elastic search

Answer: B

NEW QUESTION 332
- (Exam Topic 3)
Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)

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

Answer: AE

NEW QUESTION 333
- (Exam Topic 3)
Which two authentication protocols are supported by the Cisco WSA? (Choose two.)

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

Answer: BE

NEW QUESTION 337
- (Exam Topic 3)
An engineer is implementing DHCP security mechanisms and needs the ability to add additional attributes to profiles that are created within Cisco ISE Which action accomplishes this task?

A. Define MAC-to-IP address mappings in the switch to ensure that rogue devices cannot get an IP address
B. Use DHCP option 82 to ensure that the request is from a legitimate endpoint and send the information to Cisco ISE
C. Modify the DHCP relay and point the IP address to Cisco ISE.
D. Configure DHCP snooping on the switch VLANs and trust the necessary interfaces

Answer: D

NEW QUESTION 342
- (Exam Topic 3)
In which two ways does the Cisco Advanced Phishing Protection solution protect users? (Choose two.)

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

Answer: BC

NEW QUESTION 347
- (Exam Topic 3)
An organization is using DNS services for their network and want to help improve the security of the DNS infrastructure. Which action accomplishes this task?

A. Use DNSSEC between the endpoints and Cisco Umbrella DNS servers.
B. Modify the Cisco Umbrella configuration to pass queries only to non-DNSSEC capable zones.
C. Integrate Cisco Umbrella with Cisco CloudLock to ensure that DNSSEC is functional.
D. Configure Cisco Umbrella and use DNSSEC for domain authentication to authoritative servers.

Answer: D

NEW QUESTION 350
- (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 354
- (Exam Topic 3)
With regard to RFC 5176 compliance, how many IETF attributes are supported by the RADIUS CoA feature?

A. 3

B. 5
C. 10
D. 12

Answer: D

NEW QUESTION 357
- (Exam Topic 3)
What is the result of the ACME-Router(config)#login block-for 100 attempts 4 within 60 command on a Cisco IOS router?

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

Answer: D

NEW QUESTION 361
- (Exam Topic 3)
Refer to the exhibit.

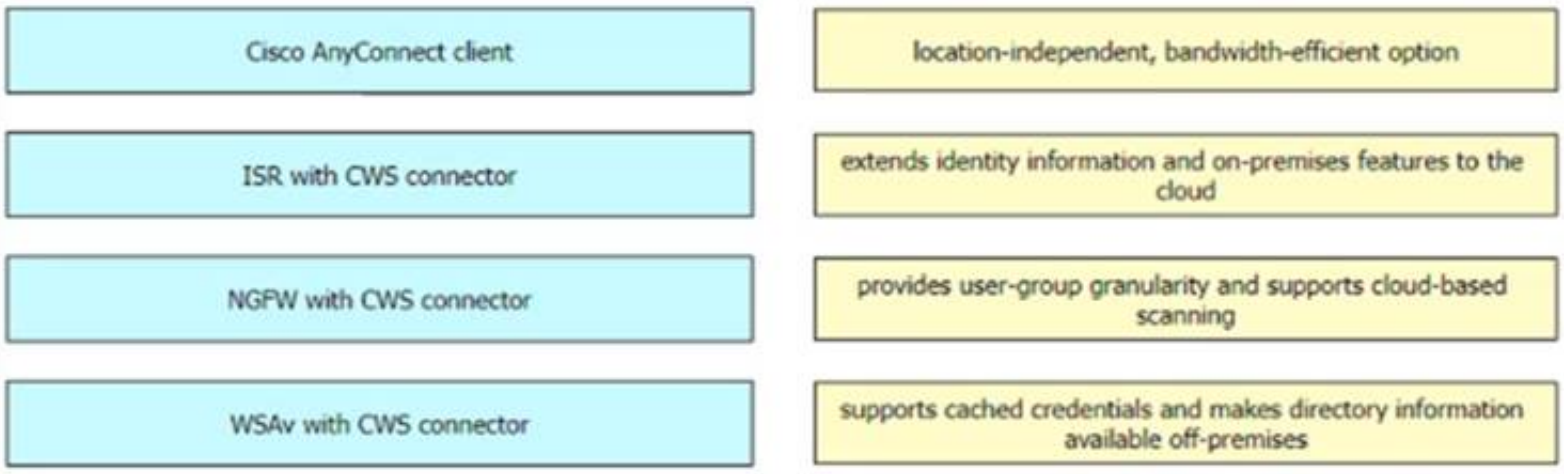
```
ntp authentication-key 10 md5 cisco123
ntp trusted-key 10
```

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 362
- (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 364
- (Exam Topic 3)
An engineer musí set up 200 new laptops on a network and wants to prevent the users from moving their laptops around to simplify administration Which switch port MAC address security setting must be used?

A. sticky
B. static
C. aging
D. maximum

Answer: A

NEW QUESTION 365
- (Exam Topic 3)
A Cisco FTD engineer is creating a new IKEv2 policy called s2s00123456789 for their organization to allow for additional protocols to terminate network devices with. They currently only have one policy established and need the new policy to be a backup in case some devices cannot support the stronger algorithms listed

in the primary policy. What should be done in order to support this?

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

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html

NEW QUESTION 368
- (Exam Topic 3)
Which two protocols must be configured to authenticate end users to the Cisco WSA? (Choose two.)

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

Answer: AD

NEW QUESTION 371
- (Exam Topic 3)

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

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

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

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

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

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

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

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

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

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

Answer: C

NEW QUESTION 374
- (Exam Topic 3)
What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?

A. Telemetry uses a pull mehod, which makes it more reliable than SNMP
B. Telemetry uses push and pull, which makes it more scalable than SNMP
C. Telemetry uses push and pull which makes it more secure than SNMP
D. Telemetry uses a push method which makes it faster than SNMP

Answer: D

Explanation:
SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts.The traditional use of the pull

model, where the client requests data from the network does not scale when what you want is near real-time data.Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc.Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics.
Referfence: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming telemetry

NEW QUESTION 377
- (Exam Topic 3)
Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using higher-level protocols without readdressing the network?

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

Answer: B

NEW QUESTION 381
- (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 383
- (Exam Topic 3)
An email administrator is setting up a new Cisco ESA. The administrator wants to enable the blocking of greymail for the end user. Which feature must the administrator enable first?

A. File Analysis
B. IP Reputation Filtering
C. Intelligent Multi-Scan
D. Anti-Virus Filtering

Answer: C

NEW QUESTION 388
- (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 392
- (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 395
- (Exam Topic 3)
When a Cisco WSA checks a web request, what occurs if it is unable to match a user-defined policy?

A. It blocks the request.
B. It applies the global policy.
C. It applies the next identification profile policy.
D. It applies the advanced policy.

Answer: B

NEW QUESTION 397

- (Exam Topic 3)
Which system performs compliance checks and remote wiping?

A. MDM
B. ISE
C. AMP
D. OTP

Answer: A

NEW QUESTION 399
- (Exam Topic 3)
An engineer integrates Cisco FMC and Cisco ISE using pxGrid Which role is assigned for Cisco FMC?

A. client
B. server
C. controller
D. publisher

Answer: D

NEW QUESTION 401
- (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 402
- (Exam Topic 3)
An engineer configures new features within the Cisco Umbrella dashboard and wants to identify and proxy traffic that is categorized as risky domains and may contain safe and malicious content. Which action accomplishes these objectives?

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

Answer: B

NEW QUESTION 406
- (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 410
- (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

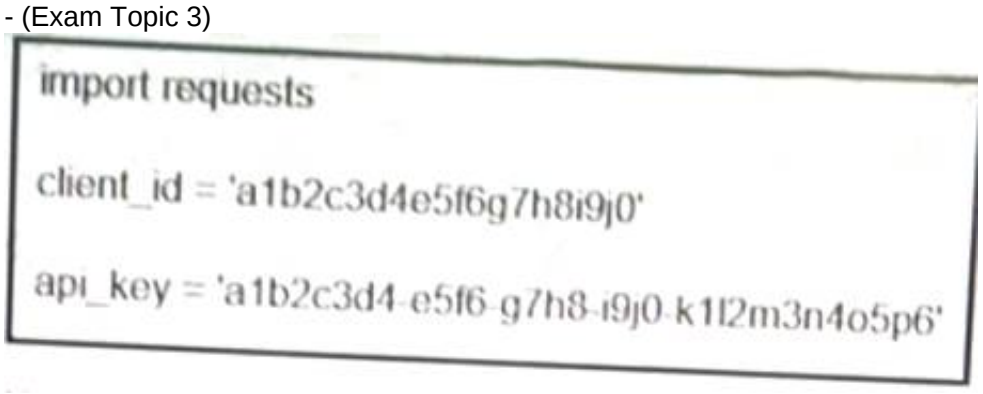
Answer: C

NEW QUESTION 413
- (Exam Topic 3)
Which solution detects threats across a private network, public clouds, and encrypted traffic?

A. Cisco Stealthwatch
B. Cisco CTA
C. Cisco Encrypted Traffic Analytics
D. Cisco Umbrella

Answer: A

NEW QUESTION 418
- (Exam Topic 3)



Refer to the exhibit. What function does the API key perform while working with https://api.amp.cisco.com/v1/computers?

A. imports requests
B. HTTP authorization
C. HTTP authentication
D. plays dent ID

Answer: C

NEW QUESTION 423
- (Exam Topic 3)
Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?

A. Cisco Umbrella
B. Cisco AMP for Endpoints
C. Cisco ISE
D. Cisco Stealthwatch

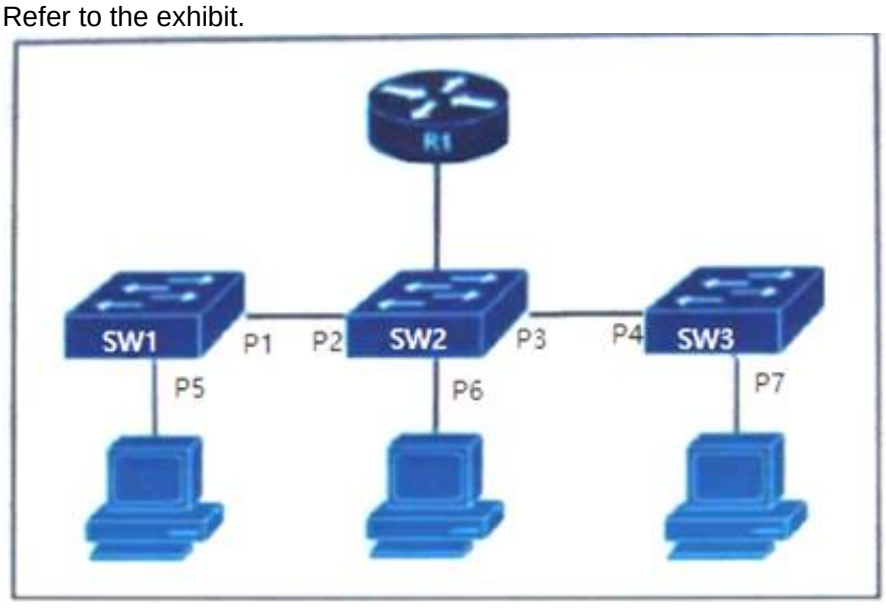
Answer: C

NEW QUESTION 425
- (Exam Topic 3)
Which VPN provides scalability for organizations with many remote sites?

A. DMVPN
B. site-to-site iPsec
C. SSL VPN
D. GRE over IPsec

Answer: A

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



The DHCP snooping database resides on router R1, and dynamic ARP inspection is configured only on switch SW2. Which ports must be configured as untrusted so that dynamic ARP inspection operates normally?

A. P2 and P3 only
B. P5, P6, and P7 only
C. P1, P2, P3, and P4 only
D. P2, P3, and P6 only

Answer: D

NEW QUESTION 429
- (Exam Topic 3)
Which two capabilities of Integration APIs are utilized with Cisco DNA center? (Choose two)

A. Upgrade software on switches and routers

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

Answer: BC

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

NEW QUESTION 432
- (Exam Topic 3)
Which two actions does the Cisco identity Services Engine posture module provide that ensures endpoint security?(Choose two.)

A. The latest antivirus updates are applied before access is allowed.
B. Assignments to endpoint groups are made dynamically, based on endpoint attributes.
C. Patch management remediation is performed.
D. A centralized management solution is deployed.
E. Endpoint supplicant configuration is deployed.

Answer: AD

NEW QUESTION 434
- (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 435
- (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 436
- (Exam Topic 3)
An engineer is configuring Dropbox integration with Cisco Cloudlock. Which action must be taken before granting API access in the Dropbox admin console?

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

Answer: A

NEW QUESTION 439
- (Exam Topic 3)
What is the function of the crypto is a kmp key cisc406397954 address 0.0.0.0 0.0.0.0 command when establishing an IPsec VPN tunnel?

A. It defines what data is going to be encrypted via the VPN
B. lt configures the pre-shared authentication key
C. It prevents all IP addresses from connecting to the VPN server.
D. It configures the local address for the VPN server.

Answer: B

NEW QUESTION 443
- (Exam Topic 3)
A network engineer is trying to figure out whether FlexVPN or DMVPN would fit better in their environment. They have a requirement for more stringent security multiple security associations for the connections, more efficient VPN establishment as well consuming less bandwidth. Which solution would be best for this and why?

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

D. DMVPN because it uses multiple SAs and FlexVPN does not

Answer: C

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

NEW QUESTION 448
- (Exam Topic 3)
What is a description of microsegmentation?

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

Answer: B

NEW QUESTION 450
- (Exam Topic 3)
Which two configurations must be made on Cisco ISE and on Cisco TrustSec devices to force a session to be adjusted after a policy change is made? (Choose two)

A. posture assessment
B. aaa authorization exec default local
C. tacacs-server host 10.1.1.250 key password
D. aaa server radius dynamic-author
E. CoA

Answer: DE

NEW QUESTION 454
- (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 456
- (Exam Topic 3)
What are two advantages of using Cisco Any connect over DMVPN? (Choose two)

A. It provides spoke-to-spoke communications without traversing the hub
B. It allows different routing protocols to work over the tunnel
C. It allows customization of access policies based on user identity
D. It allows multiple sites to connect to the data center
E. It enables VPN access for individual users from their machines

Answer: CE

NEW QUESTION 459
- (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 460
- (Exam Topic 3)
What provides total management for mobile and PC including managing inventory and device tracking, remote view, and live troubleshooting using the included native remote desktop support?

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

Answer: A

NEW QUESTION 465
- (Exam Topic 3)
What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?

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

Answer: A

NEW QUESTION 469
- (Exam Topic 3)
Which MDM configuration provides scalability?

A. pushing WPA2-Enterprise settings automatically to devices
B. enabling use of device features such as camera use
C. BYOD support without extra appliance or licenses
D. automatic device classification with level 7 fingerprinting

Answer: C

NEW QUESTION 470
- (Exam Topic 3)
Which security product enables administrators to deploy Kubernetes clusters in air-gapped sites without needing Internet access?

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

Answer: C

NEW QUESTION 474
- (Exam Topic 3)
Which Cisco ISE service checks the compliance of endpoints before allowing the endpoints to connect to the network?

A. posture
B. profiler
C. Cisco TrustSec
D. Threat Centric NAC

Answer: A

NEW QUESTION 476
- (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. It defines the format of data records.
D. It serves as a unique identification number to distinguish individual data records

Answer: C

NEW QUESTION 481
- (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 483
- (Exam Topic 3)
Based on the NIST 800-145 guide, which cloud architecture may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises?

A. hybrid cloud

B. private cloud
C. public cloud
D. community cloud

Answer: D

NEW QUESTION 484
- (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 486
- (Exam Topic 2)
What is a prerequisite when integrating a Cisco ISE server and an AD domain?

A. Place the Cisco ISE server and the AD server in the same subnet
B. Configure a common administrator account
C. Configure a common DNS server
D. Synchronize the clocks of the Cisco ISE server and the AD server

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_

NEW QUESTION 491
- (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 494
- (Exam Topic 2)
An engineer needs behavioral analysis to detect malicious activity on the hosts, and is configuring the organization’s public cloud to send telemetry using the cloud provider’s mechanisms to a security device.
Which mechanism should the engineer configure to accomplish this goal?

A. mirror port
B. Flow
C. NetFlow
D. VPC flow logs

Answer: C

NEW QUESTION 498
- (Exam Topic 2)
Which type of dashboard does Cisco DNA Center provide for complete control of the network?

A. service management
B. centralized management
C. application management
D. distributed management

Answer: B

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

NEW QUESTION 499
- (Exam Topic 2)
When planning a VPN deployment, for which reason does an engineer opt for an active/active FlexVPN configuration as opposed to DMVPN?

A. Multiple routers or VRFs are required.
B. Traffic is distributed statically by default.
C. Floating static routes are required.
D. HSRP is used for faliover.

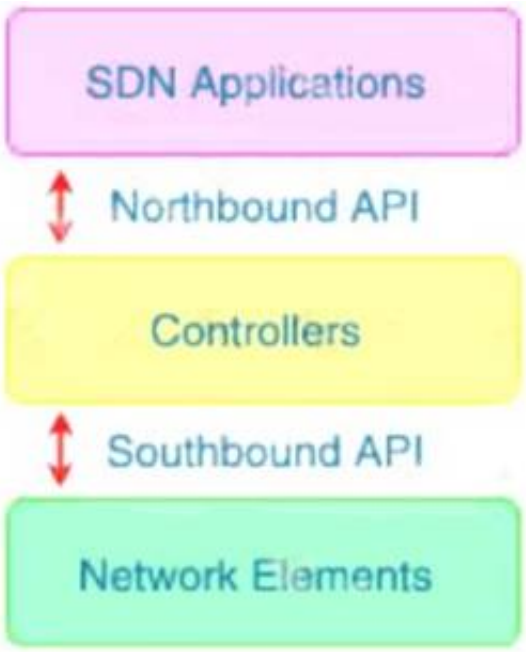
Answer: B

NEW QUESTION 503
- (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 506
- (Exam Topic 2)
Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats?

A. PSIRT
B. Talos
C. CSIRT
D. DEVNET

Answer: B

Explanation:
Reference: https://talosintelligence.com/newsletters

NEW QUESTION 509
- (Exam Topic 2)
Which type of API is being used when a security application notifies a controller within a software-defined network architecture about a specific security threat?

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

Answer: C

NEW QUESTION 511
- (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 516
- (Exam Topic 2)
An engineer is implementing NTP authentication within their network and has configured both the client and server devices with the command ntp authentication-key 1 md5 Cisc392368270. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however it is unable to do so. Which command is required to enable the client to accept the server's authentication key?

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

Answer: B

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

NEW QUESTION 520
- (Exam Topic 2)
Which Cisco platform ensures that machines that connect to organizational networks have the recommended antivirus definitions and patches to help prevent an organizational malware outbreak?

A. Cisco WiSM
B. Cisco ESA
C. Cisco ISE
D. Cisco Prime Infrastructure

Answer: C

Explanation:
A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. We can configure ISE to check for the Windows patch at Work Centers > Posture > Posture Elements > Conditions > File.In this example, we are going to use the predefined file check to ensure that our Windows 10 clients have the critical security patch installed to prevent the Wanna Cry malware; and we can also configure ISE to update the client with this patch.

NEW QUESTION 521
- (Exam Topic 2)
What is a benefit of performing device compliance?

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

Answer: A

NEW QUESTION 523
- (Exam Topic 2)
In an IaaS cloud services model, which security function is the provider responsible for managing?

A. Internet proxy
B. firewalling virtual machines
C. CASB
D. hypervisor OS hardening

Answer: B

Explanation:
In this IaaS model, cloud providers offer resources to users/machines that include computers as virtualmachines, raw (block) storage, firewalls, load balancers, and network devices.Note: Cloud access security broker (CASB) provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware such as ransomware.

NEW QUESTION 525
- (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 527
- (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 532
- (Exam Topic 2)
Which risk is created when using an Internet browser to access cloud-based service?

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

Answer: D

NEW QUESTION 535
- (Exam Topic 2)
What is the purpose of the certificate signing request when adding a new certificate for a server?

A. It is the password for the certificate that is needed to install it with.
B. It provides the server information so a certificate can be created and signed
C. It provides the certificate client information so the server can authenticate against it when installing
D. It is the certificate that will be loaded onto the server

Answer: B

Explanation:
A certificate signing request (CSR) is one of the first steps towards getting your own SSL Certificate. Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) that the Certificate Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key

NEW QUESTION 540
- (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 541
- (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 542

- (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 545
- (Exam Topic 2)
Which factor must be considered when choosing the on-premise solution over the cloud-based one?

A. With an on-premise solution, the provider is responsible for the installation and maintenance of the product, whereas with a cloud-based solution, the customer is responsible for it
B. With a cloud-based solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.
C. With an on-premise solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.
D. With an on-premise solution, the customer is responsible for the installation and maintenance of the product, whereas with a cloud-based solution, the provider is responsible for it.

Answer: D

NEW QUESTION 547
- (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 549
- (Exam Topic 2)
A Cisco ESA administrator has been tasked with configuring the Cisco ESA to ensure there are no viruses before quarantined emails are delivered. In addition, delivery of mail from known bad mail servers must be prevented. Which two actions must be taken in order to meet these requirements? (Choose two)

A. Use outbreak filters from SenderBase
B. Enable a message tracking service
C. Configure a recipient access table
D. Deploy the Cisco ESA in the DMZ
E. Scan quarantined emails using AntiVirus signatures

Answer: AE

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 Therefore Outbreak filters can be used to block emails from bad mail servers.Web servers and email gateways are generally located in the DMZ soNote: The recipient access table (RAT), not to be confused with remote-access Trojan (also RAT), is a Cisco ESA term that defines which recipients are accepted by a public listener.

NEW QUESTION 551
- (Exam Topic 2)
A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an undetermined verdict. What is causing this issue?

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

Answer: D

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

NEW QUESTION 554
- (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 556
- (Exam Topic 2)
What is the role of an endpoint in protecting a user from a phishing attack?

A. Use Cisco Stealthwatch and Cisco ISE Integration.
B. Utilize 802.1X network security to ensure unauthorized access to resources.
C. Use machine learning models to help identify anomalies and determine expected sending behavior.
D. Ensure that antivirus and anti malware software is up to date

Answer: C

NEW QUESTION 559
- (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 561
- (Exam Topic 2)
An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?

A. TCP 6514
B. UDP 1700
C. TCP 49
D. UDP 1812

Answer: B

Explanation:
CoA Messages are sent on two different udp ports depending on the platform. Cisco standardizes on UDP port1700, while the actual RFC calls out using UDP port 3799.

NEW QUESTION 562
- (Exam Topic 2)
An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?

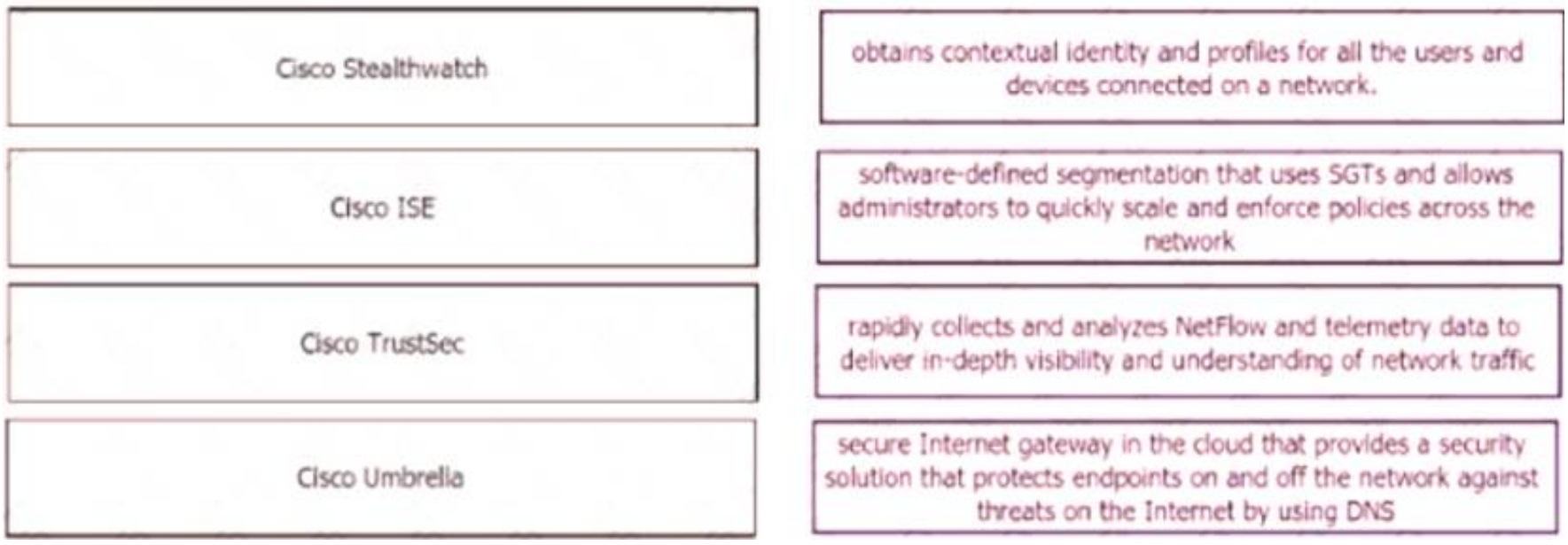
A. Cisco Defense Orchestrator
B. Cisco Secureworks

C. Cisco DNA Center
D. Cisco Configuration Professional

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html

NEW QUESTION 567
- (Exam Topic 2)
Drag and drop the solutions from the left onto the solution's benefits on the right.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 572
- (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 573
- (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 578
- (Exam Topic 2)
In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?

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

Answer: B

NEW QUESTION 583
.....

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