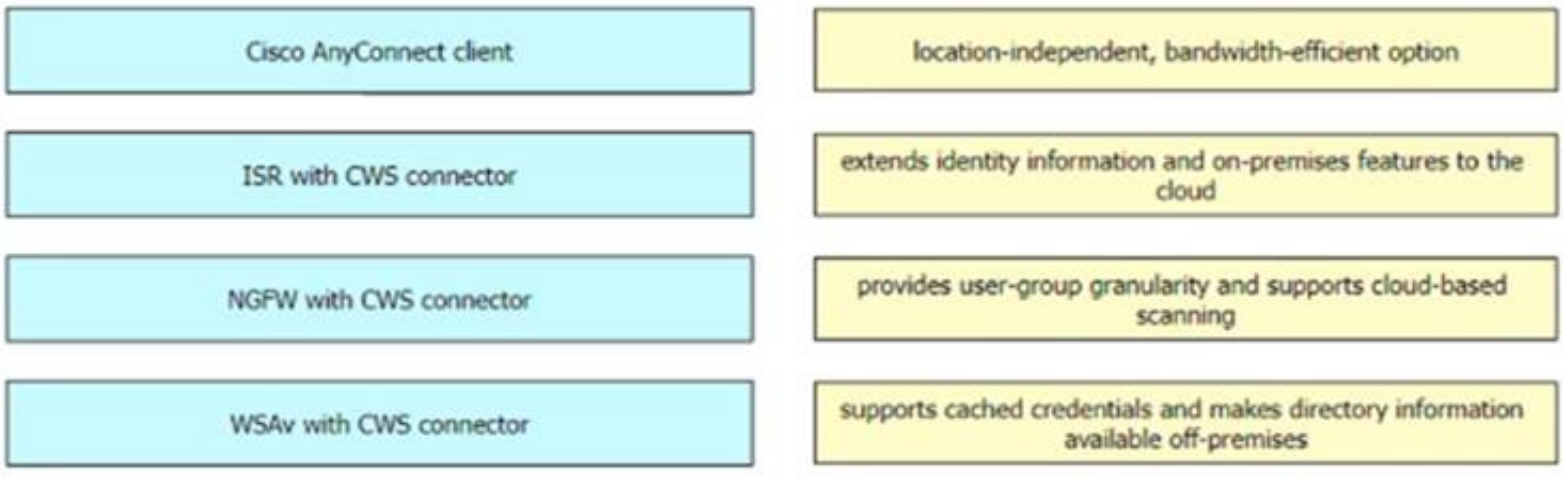
Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

https://www.2passeasy.com/dumps/350-701/

NEW QUESTION 1
- (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 2
- (Exam Topic 3)
What do tools like Jenkins, Octopus Deploy, and Azure DevOps provide in terms of application and infrastructure automation?

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

Answer: A

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

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

Answer: D

NEW QUESTION 4
- (Exam Topic 3)
What is the purpose of the Cisco Endpoint loC feature?

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

Answer: C

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

NEW QUESTION 5
- (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 6
- (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 7
- (Exam Topic 3)
What is a benefit of using GET VPN over FlexVPN within a VPN deployment?

A. GET VPN supports Remote Access VPNs
B. GET VPN natively supports MPLS and private IP networks
C. GET VPN uses multiple security associations for connections
D. GET VPN interoperates with non-Cisco devices

Answer: B

NEW QUESTION 8
- (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 9
- (Exam Topic 3)
Which type of DNS abuse exchanges data between two computers even when there is no direct connection?

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

Answer: D

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

NEW QUESTION 10
- (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 10
- (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 13

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

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

Answer: AB

Explanation:

- Transparently identify users with authentication realms – This option is available when one or more authentication realms are configured to support transparent identification using one of the following authentication servers:
- Active Directory – Create an NTLM or Kerberos authentication realm and enable transparent user identification. In addition, you must deploy a separate Active Directory agent such as Cisco's Context Directory Agent. For more information, see Transparent User Identification with Active Directory.
- LDAP – Create an LDAP authentication realm configured as an eDirectory, andenable transparent user identification. For more information, see Transparent User Identification with LDAP.

Details:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGui

NEW QUESTION 17
- (Exam Topic 3)
What are two facts about WSA HTTP proxy configuration with a PAC file? (Choose two.)

A. It is defined as a Transparent proxy deployment.
B. In a dual-NIC configuration, the PAC file directs traffic through the two NICs to the proxy.
C. The PAC file, which references the proxy, is deployed to the client web browser.
D. It is defined as an Explicit proxy deployment.
E. It is defined as a Bridge proxy deployment.

Answer: CD

NEW QUESTION 19
- (Exam Topic 3)
Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?

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

Answer: B

NEW QUESTION 20
- (Exam Topic 3)
Which DevSecOps implementation process gives a weekly or daily update instead of monthly or quarterly in the applications?

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

Answer: B

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

NEW QUESTION 21
- (Exam Topic 3)
DoS attacks are categorized as what?

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

Answer: B

NEW QUESTION 26
- (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 31
- (Exam Topic 3)
Which Cisco platform provides an agentless solution to provide visibility across the network including encrypted traffic analytics to detect malware in encrypted traffic without the need for decryption?

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

Answer: B

NEW QUESTION 33
- (Exam Topic 3)
An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices The default management port conflicts with other communications on the network and must be changed What must be done to ensure that all devices can communicate together?

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

Answer: D

NEW QUESTION 35
- (Exam Topic 3)
Which Talos reputation center allows for tracking the reputation of IP addresses for email and web traffic?

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

Answer: A

NEW QUESTION 39
- (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 42
- (Exam Topic 3)
A Cisco ISE engineer configures Central Web Authentication (CWA) for wireless guest access and must have the guest endpoints redirect to the guest portal for authentication and authorization. While testing the policy, the engineer notices that the device is not redirected and instead gets full guest access. What must be done for the redirect to work?

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

Answer: D

NEW QUESTION 43
- (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 46
- (Exam Topic 3)
An engineer needs to configure an access control policy rule to always send traffic for inspection without using the default action. Which action should be configured for this rule?

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

Answer: B

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

NEW QUESTION 51
- (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 55
- (Exam Topic 3)
What is a function of the Layer 4 Traffic Monitor on a Cisco WSA?

A. blocks traffic from URL categories that are known to contain malicious content
B. decrypts SSL traffic to monitor for malicious content
C. monitors suspicious traffic across all the TCP/UDP ports
D. prevents data exfiltration by searching all the network traffic for specified sensitive information

Answer: C

NEW QUESTION 60
- (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 64
- (Exam Topic 3)
Which Cisco DNA Center Intent API action is used to retrieve the number of devices known to a DNA Center?

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

Answer: A

NEW QUESTION 67
- (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 71
- (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 74
- (Exam Topic 3)
An engineer needs to add protection for data in transit and have headers in the email message Which configuration is needed to accomplish this goal?

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

Answer: D

NEW QUESTION 75
- (Exam Topic 3)
What is an advantage of the Cisco Umbrella roaming client?

A. the ability to see all traffic without requiring TLS decryption
B. visibility into IP-based threats by tunneling suspicious IP connections
C. the ability to dynamically categorize traffic to previously uncategorized sites
D. visibility into traffic that is destined to sites within the office environment

Answer: C

NEW QUESTION 77
- (Exam Topic 3)
Which two methods must be used to add switches into the fabric so that administrators can control how switches are added into DCNM for private cloud management? (Choose two.)

A. Cisco Cloud Director
B. Cisco Prime Infrastructure
C. PowerOn Auto Provisioning
D. Seed IP
E. CDP AutoDiscovery

Answer: CD

NEW QUESTION 79
- (Exam Topic 3)
An organization has DHCP servers set up to allocate IP addresses to clients on the LAN. What must be done to ensure the LAN switches prevent malicious DHCP traffic while also distributing IP addresses to the correct endpoints?

A. Configure Dynamic ARP inspection and add entries in the DHCP snooping database.
B. Configure DHCP snooping and set trusted interfaces for all client connections.
C. Configure Dynamic ARP inspection and antispoofing ACLs in the DHCP snooping database.
D. Configure DHCP snooping and set a trusted interface for the DHCP server.

Answer: B

Explanation:
Reference: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuratio

NEW QUESTION 83
- (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 88
- (Exam Topic 3)
Refer to the exhibit.

```
interface GigabitEthernet1/0/18
 description ISE dot1x Port
 switchport access vlan 41
 switchport mode access
 switchport voice vlan 44
 device-tracking attach-policy IPDT_MAX_10
 authentication periodic
 authentication timer reauthenticate server
 access-session host-mode multi-domain
 access-session port-control auto
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 spanning-tree portfast
 service-policy type control subscriber POLICY_Gi1/0/18
```

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

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

Answer: B

NEW QUESTION 90
- (Exam Topic 3)
An administrator is establishing a new site-to-site VPN connection on a Cisco IOS router. The organization needs to ensure that the ISAKMP key on the hub is used only for terminating traffic from the IP address of 172.19.20.24. Which command on the hub will allow the administrator to accomplish this?

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

Answer: B

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

NEW QUESTION 93
- (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 98
- (Exam Topic 3)
Which Cisco WSA feature supports access control using URL categories?

A. transparent user identification
B. SOCKS proxy services
C. web usage controls
D. user session restrictions

Answer: A

NEW QUESTION 102
- (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 103
- (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 107
- (Exam Topic 3)
What is the recommendation in a zero-trust model before granting access to corporate applications and resources?

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

Answer: A

NEW QUESTION 109
- (Exam Topic 3)
Which Cisco Firewall solution requires zone definition?

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

Answer: C

NEW QUESTION 114
- (Exam Topic 3)
A company identified a phishing vulnerability during a pentest What are two ways the company can protect employees from the attack? (Choose two.)

A. using Cisco Umbrella
B. using Cisco ESA
C. using Cisco FTD
D. using an inline IPS/IDS in the network
E. using Cisco ISE

Answer: AB

NEW QUESTION 115
- (Exam Topic 3)
Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks? (Choose two.)

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

Answer: CE

NEW QUESTION 118
- (Exam Topic 3)
An organization wants to provide visibility and to identify active threats in its network using a VM. The organization wants to extract metadata from network packet flow while ensuring that payloads are not retained or transferred outside the network. Which solution meets these requirements?

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

Answer: B

Explanation:
Reference:

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

NEW QUESTION 121
- (Exam Topic 3)
Which Cisco ISE feature helps to detect missing patches and helps with remediation?

A. posture assessment
B. profiling policy
C. authentication policy
D. enabling probes

Answer: B

NEW QUESTION 124
- (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 125
- (Exam Topic 3)
Which Cisco security solution provides patch management in the cloud?

A. Cisco Umbrella
B. Cisco ISE
C. Cisco CloudLock
D. Cisco Tetration

Answer: C

NEW QUESTION 126
- (Exam Topic 3)
Refer to the exhibit.

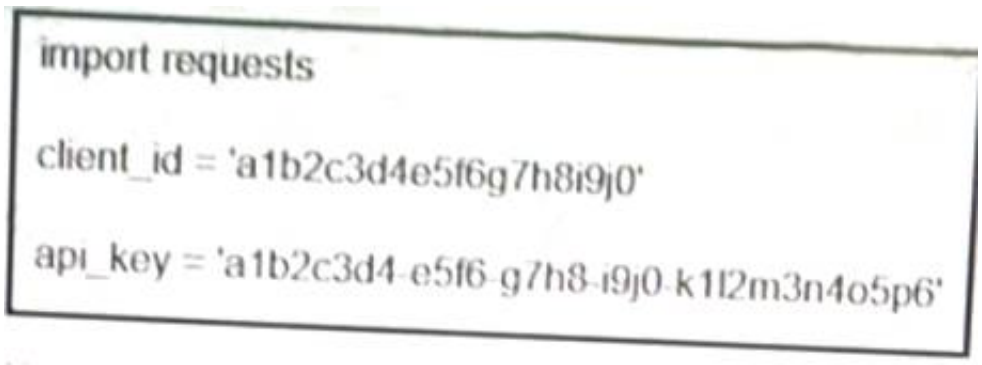
```
interface GigabitEthernet1/0/18
switchport access vlan 41
switchport mode access
switchport voice vlan 44
device-tracking attach-policy IPDT_MAX_10
authentication periodic
authentication timer reauthenticate server
access-session host-mode multi-domain
access-session port-control auto
dot1x pae authenticator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

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 128
- (Exam Topic 3)
Refer to the exhibit.

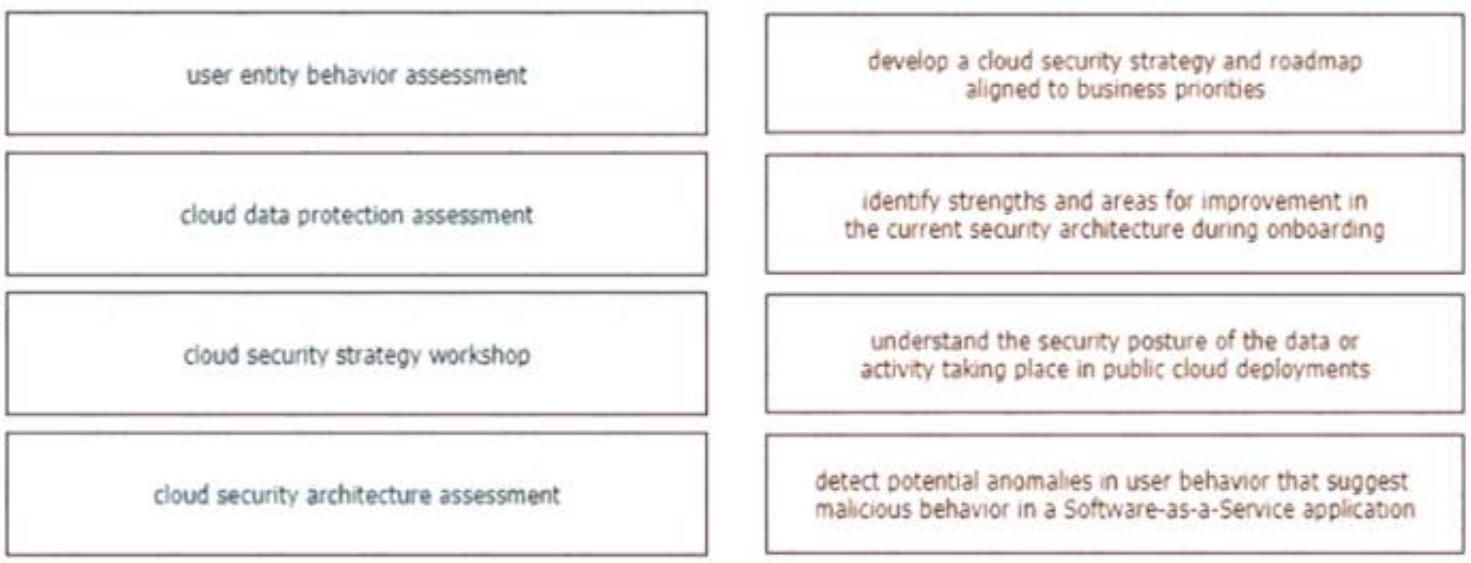


What function does the API key perform while working with https://api.amp.cisco.com/v1/computers?

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

Answer: C

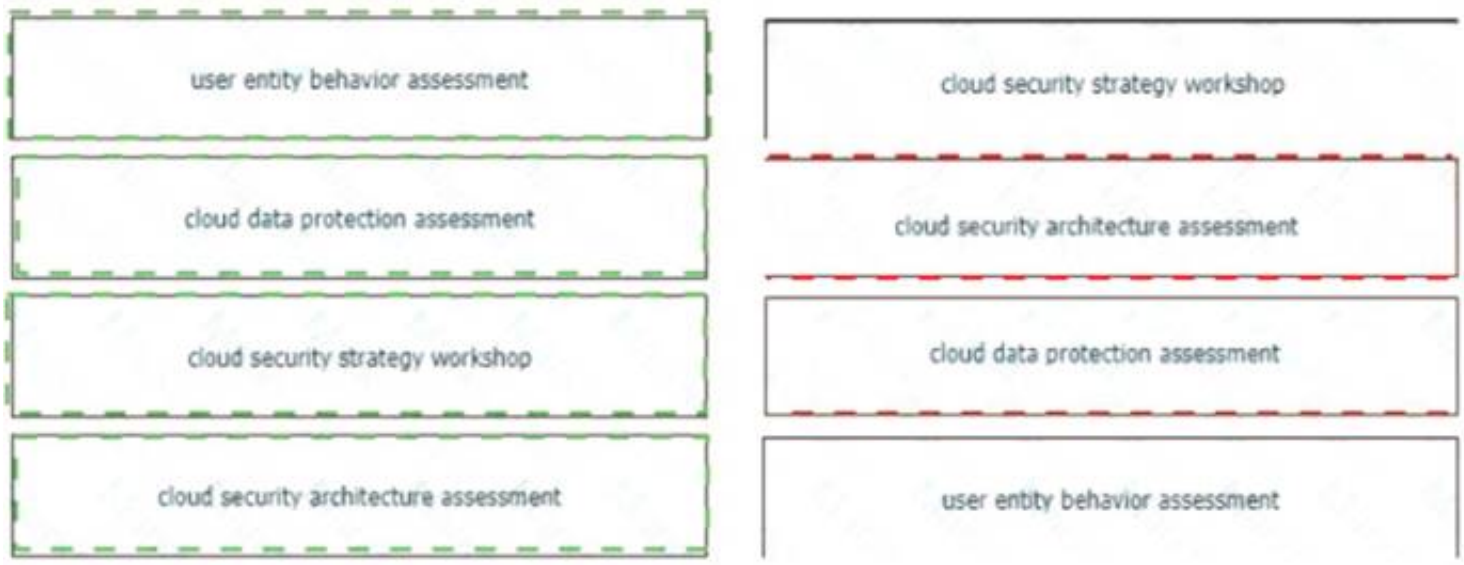
NEW QUESTION 131
- (Exam Topic 3)
Drag and drop the cloud security assessment components from the left onto the definitions on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 134
- (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 Clienttracks only URL-based threats.

Answer: D

NEW QUESTION 135
- (Exam Topic 3)
Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or Microsoft vSwitch?

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

Answer: C

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

NEW QUESTION 140
- (Exam Topic 3)
A customer has various external HTTP resources available including Intranet Extranet and Internet, with a proxy configuration running in explicit mode. Which method allows the client desktop browsers to be
configured
to select when to connect direct or when to use the proxy?

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

Answer: C

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

NEW QUESTION 141
- (Exam Topic 3)
An administrator is configuring N I P on Cisco ASA via ASDM and needs to ensure that rogue NTP servers cannot insert themselves as the authoritative time source Which two steps must be taken to accomplish this task? (Choose two)

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

Answer: CD

NEW QUESTION 145
- (Exam Topic 3)
An administrator is adding a new Cisco ISE node to an existing deployment. What must be done to ensure that the addition of the node will be successful when inputting the FQDN?

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

Answer: D

NEW QUESTION 147
- (Exam Topic 3)
For a given policy in Cisco Umbrella, how should a customer block website based on a custom list?

A. by specifying blocked domains in me policy settings
B. by specifying the websites in a custom blocked category
C. by adding the websites to a blocked type destination list
D. by adding the website IP addresses to the Cisco Umbrella blocklist

Answer: C

NEW QUESTION 149
- (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 153
- (Exam Topic 3)
Which technology enables integration between Cisco ISE and other platforms to gather and share network and vulnerability data and SIEM and location information?

A. pxGrid
B. NetFlow
C. SNMP
D. Cisco Talos

Answer: A

NEW QUESTION 157
- (Exam Topic 3)
A Cisco AMP for Endpoints administrator configures a custom detection policy to add specific MD5 signatures The configuration is created in the simple detection policy section, but it does not work What is the reason for this failure?

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

Answer: D

NEW QUESTION 160
- (Exam Topic 3)
Which standard is used to automate exchanging cyber threat information?

A. TAXII
B. MITRE
C. IoC
D. STIX

Answer: A

NEW QUESTION 163
- (Exam Topic 3)
Which feature must be configured before implementing NetFlow on a router?

A. SNMPv3
B. syslog
C. VRF
D. IP routing

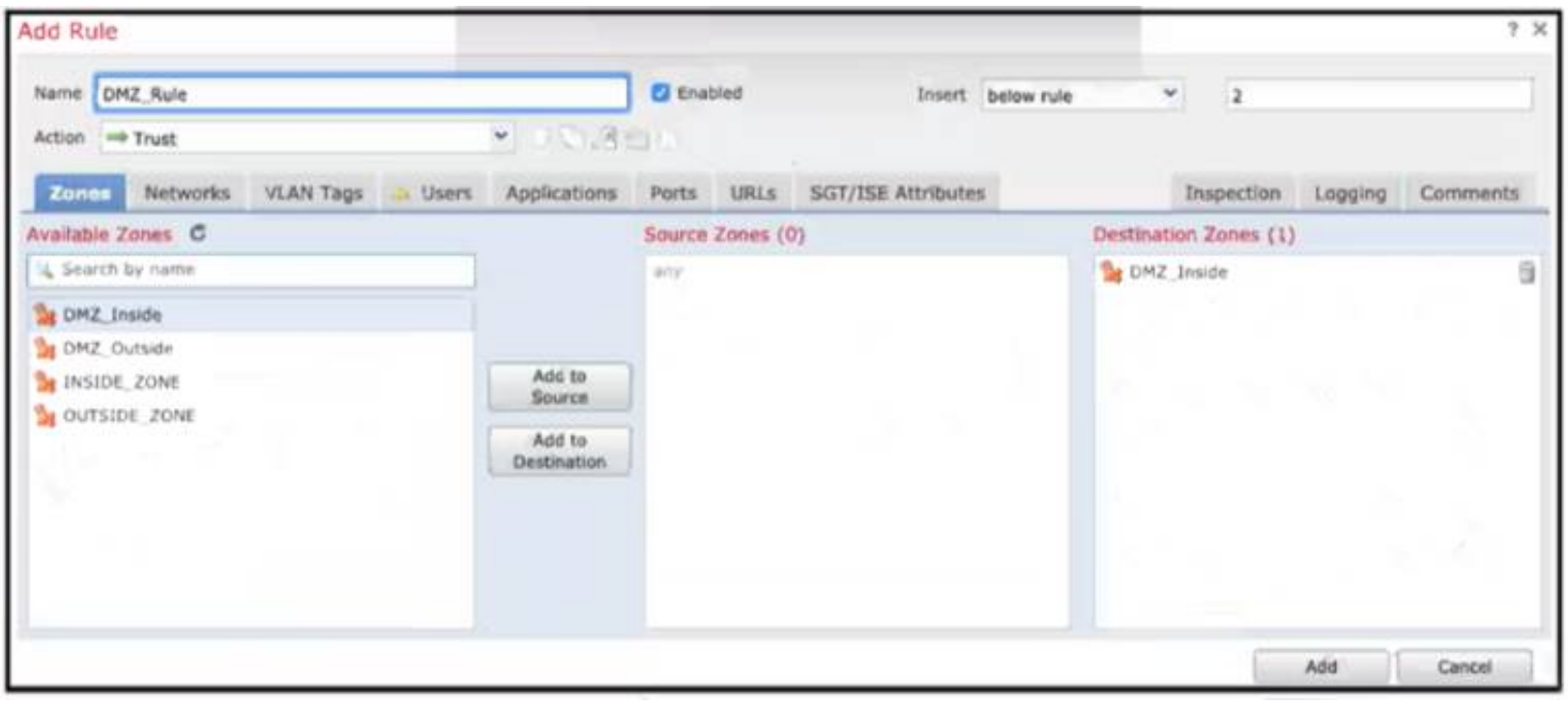
Answer: D

NEW QUESTION 165
- (Exam Topic 3)
In which scenario is endpoint-based security the solution?

A. inspecting encrypted traffic
B. device profiling and authorization
C. performing signature-based application control
D. inspecting a password-protected archive

Answer: C

NEW QUESTION 169
- (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 171
- (Exam Topic 3)
Which ESA implementation method segregates inbound and outbound email?

A. one listener on a single physical Interface
B. pair of logical listeners on a single physical interface with two unique logical IPv4 addresses and one IPv6 address
C. pair of logical IPv4 listeners and a pair Of IPv6 listeners on two physically separate interfaces
D. one listener on one logical IPv4 address on a single logical interface

Answer: D

NEW QUESTION 173
- (Exam Topic 3)
What are two workloaded security models? (Choose two)

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

Answer: CD

NEW QUESTION 174
- (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 179
- (Exam Topic 2)
Which component of Cisco umbrella architecture increases reliability of the service?

A. Anycast IP
B. AMP Threat grid
C. Cisco Talos
D. BGP route reflector

Answer: C

NEW QUESTION 180
- (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 185
- (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 190
- (Exam Topic 2)
What are two functions of secret key cryptography? (Choose two)

A. key selection without integer factorization
B. utilization of different keys for encryption and decryption
C. utilization of large prime number iterations
D. provides the capability to only know the key on one side
E. utilization of less memory

Answer: BD

NEW QUESTION 193
- (Exam Topic 2)
Refer to the exhibit.

```
> show crypto ipsec sa
interface: Outside
    Crypto map tag: CSM_Outside_map, seq num: 1, local addr:
209.165.200.225

      access-list CSM_IPSEC_ACL_1 extended permit ip 10.0.11.0
255.255.255.0 10.0.10.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.0.11.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.0.10.0/255.255.255.0/0/0)
      current_peer: 209.165.202.129


      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 17, #pkts decrypt: 17, #pkts verify: 17
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp
failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.200.225/500, remote crypto endpt.:
209.165.202.129/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: B6F5EA53
      current inbound spi : 84348DEE
```

Traffic is not passing through IPsec site-to-site VPN on the Firepower Threat Defense appliance. What is causing this issue?

A. No split-tunnel policy is defined on the Firepower Threat Defense appliance.
B. The access control policy is not allowing VPN traffic in.
C. Site-to-site VPN peers are using different encryption algorithms.
D. Site-to-site VPN preshared keys are mismatched.

Answer: A

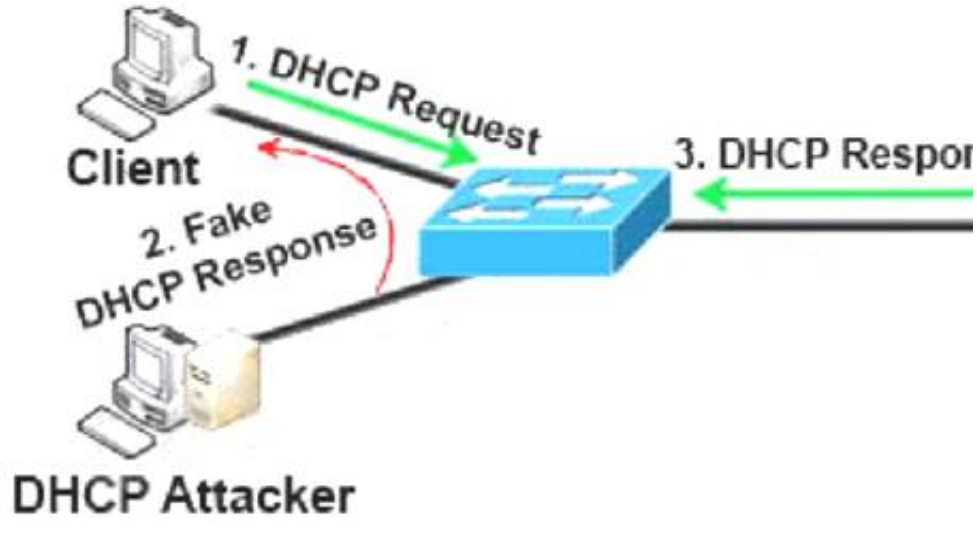
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470- site-to-site-vpn-configuration-on-ftd-ma.html

NEW QUESTION 195
- (Exam Topic 2)
An administrator is configuring a DHCP server to better secure their environment. They need to be able to ratelimit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?

A. Set a trusted interface for the DHCP server
B. Set the DHCP snooping bit to 1
C. Add entries in the DHCP snooping database
D. Enable ARP inspection for the required VLAN

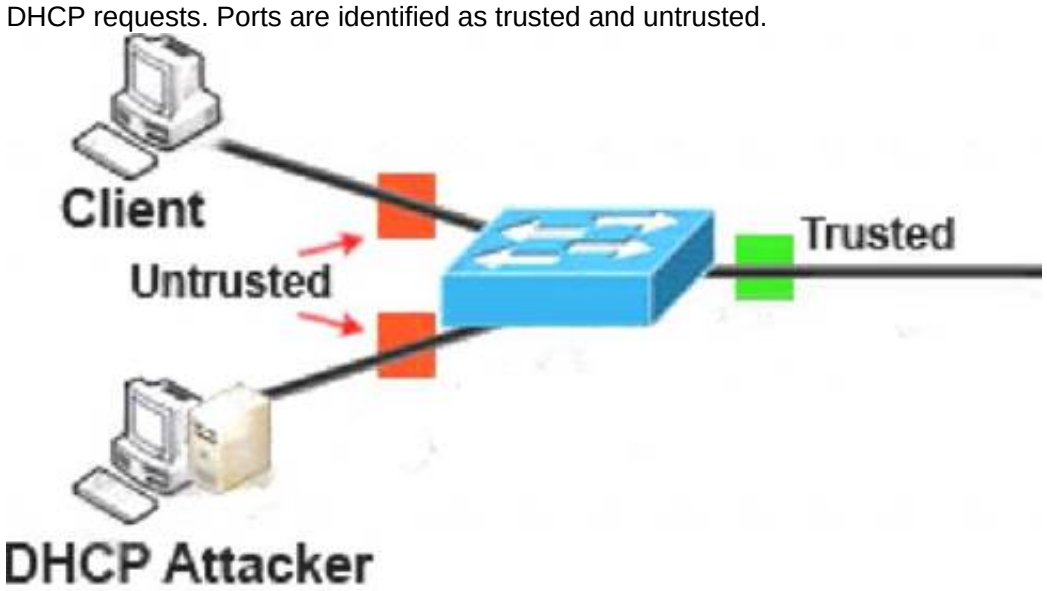
Answer: A

Explanation:
To understand DHCP snooping we need to learn about DHCP spoofing attack first.



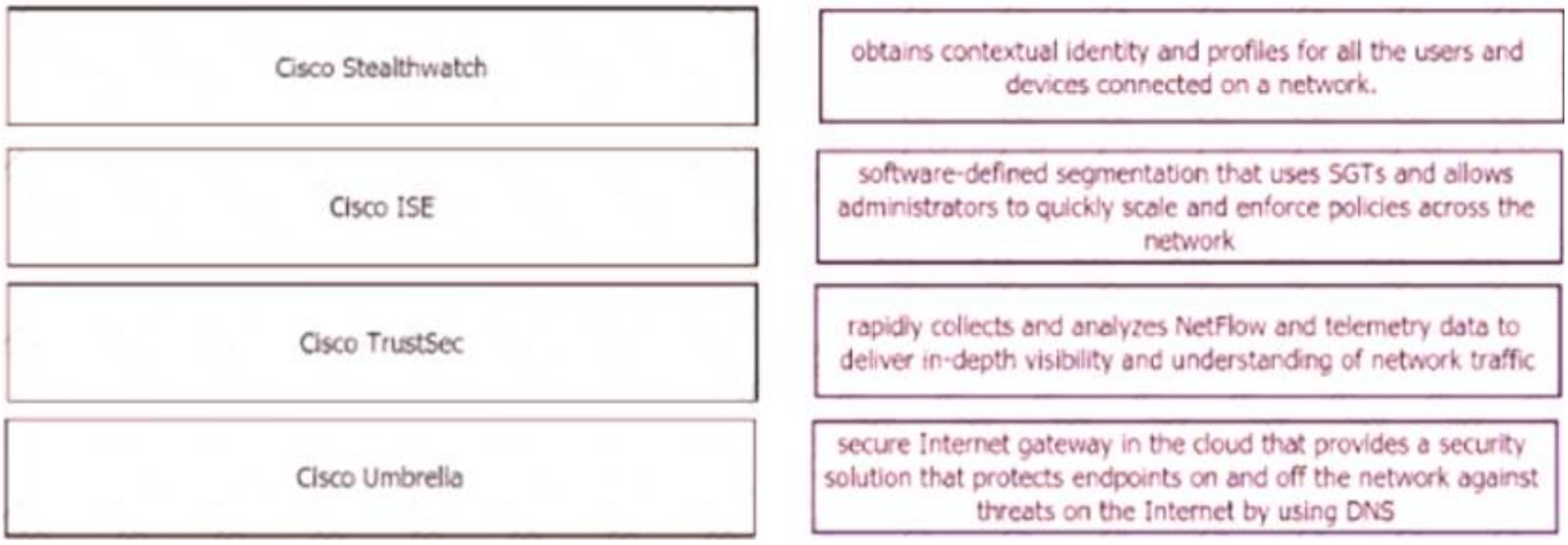
DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from 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 DHCPmessages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP responseis seen on an untrusted port, the port is shut down.

NEW QUESTION 199
- (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 204
- (Exam Topic 2)
Refer to the exhibit.

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

What will happen when this Python script is run?

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

Answer: D

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

NEW QUESTION 205
- (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 207
- (Exam Topic 2)
Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 209
- (Exam Topic 2)
Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps.
Which two actions must be taken to ensure that interfaces are put back into service? (Choose two)

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

Answer: CE

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

NEW QUESTION 210
- (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 213

- (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 218
- (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 221
- (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 224
- (Exam Topic 2)
An attacker needs to perform reconnaissance on a target system to help gain access to it. The system has weak passwords, no encryption on the VPN links, and software bugs on the system's applications. Which
vulnerability allows the attacker to see the passwords being transmitted in clear text?

A. weak passwords for authentication
B. unencrypted links for traffic
C. software bugs on applications
D. improper file security

Answer: B

NEW QUESTION 227
- (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 229
- (Exam Topic 2)
What is managed by Cisco Security Manager?

A. access point
B. WSA
C. ASA
D. ESA

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/products/security/security-manager/index.html

NEW QUESTION 234
- (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 235
- (Exam Topic 2)
An engineer has enabled LDAP accept queries on a listener. Malicious actors must be prevented from quickly identifying all valid recipients. What must be done on the Cisco ESA to accomplish this goal?

A. Configure incoming content filters
B. Use Bounce Verification
C. Configure Directory Harvest Attack Prevention
D. Bypass LDAP access queries in the recipient access table

Answer: C

Explanation:
A Directory Harvest Attack (DHA) is a technique used by spammers to find valid/existent email addresses at a domain either by using Brute force or by guessing valid e-mail addresses at a domain using differentpermutations of common username. Its easy for attackers to get hold of a valid email address if yourorganization uses standard format for official e-mail alias (for example: jsmith@example.com). We canconfigure DHA Prevention to prevent malicious actors from quickly identifying valid recipients.Note: Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email programs use to look up contact information from a server, such as ClickMail Central Directory. For example, here's an LDAP search translated into plain English: "Search for all people located in Chicago who's name contains "Fred" that have an email address. Please return their full name, email, title, and description.

NEW QUESTION 239
- (Exam Topic 2)
What is an attribute of the DevSecOps process?

A. mandated security controls and check lists
B. security scanning and theoretical vulnerabilities
C. development security
D. isolated security team

Answer: C

Explanation:
DevSecOps (development, security, and operations) is a concept used in recent years to describe how to movesecurity activities to the start of the development life cycle and have built-in security practices in the continuousintegration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closerto IT and business objectives.Three key things make a real DevSecOps environment:+ Security testing is done by the development team.+ Issues found during that testing is managed by the development team.+ Fixing those issues stays within the development team.

NEW QUESTION 241
- (Exam Topic 2)
An organization is trying to implement micro-segmentation on the network and wants to be able to gain visibility on the applications within the network. The solution must be able to maintain and force compliance. Which product should be used to meet these requirements?

A. Cisco Umbrella
B. Cisco AMP

C. Cisco Stealthwatch
D. Cisco Tetration

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/solutionoverview-c22

NEW QUESTION 246
- (Exam Topic 2)
A network engineer is deciding whether to use stateful or stateless failover when configuring two ASAs for high availability. What is the connection status in both cases?

A. need to be reestablished with stateful failover and preserved with stateless failover
B. preserved with stateful failover and need to be reestablished with stateless failover
C. preserved with both stateful and stateless failover
D. need to be reestablished with both stateful and stateless failover

Answer: B

NEW QUESTION 249
- (Exam Topic 2)
In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint Protection Platform?

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

Answer: D

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

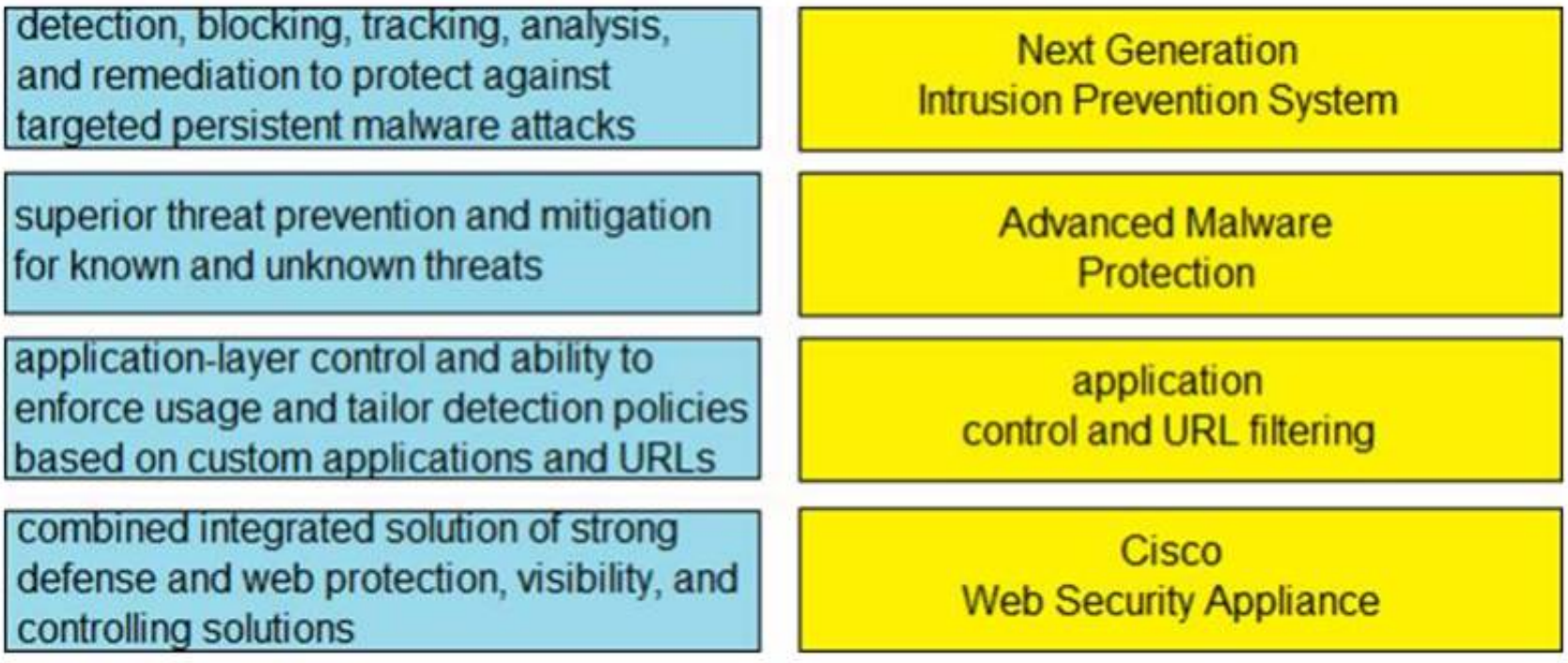
NEW QUESTION 253
- (Exam Topic 2)
A Cisco Firepower administrator needs to configure a rule to allow a new application that has never been seen on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose
two)

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 258
- (Exam Topic 2)
Drag and drop the capabilities from the left onto the correct technologies on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, chat or text message Description automatically generated

NEW QUESTION 259
- (Exam Topic 1)
Which option is the main function of Cisco Firepower impact flags?

A. They alert administrators when critical events occur.
B. They highlight known and suspected malicious IP addresses in reports.
C. They correlate data about intrusions and vulnerability.
D. They identify data that the ASA sends to the Firepower module.

Answer: C

NEW QUESTION 263
- (Exam Topic 1)
What is the primary benefit of deploying an ESA in hybrid mode?

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

Answer: D

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

NEW QUESTION 268
- (Exam Topic 1)
For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two)

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

Answer: AD

NEW QUESTION 272
- (Exam Topic 1)
Refer to the exhibit.

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

What does the number 15 represent in this configuration?

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

Answer: B

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

NEW QUESTION 274
- (Exam Topic 1)
Refer to the exhibit.

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

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

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

Answer: C

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

NEW QUESTION 277
- (Exam Topic 1)
Which ASA deployment mode can provide separation of management on a shared appliance?

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

Answer: C

NEW QUESTION 281
- (Exam Topic 1)
Refer to the exhibit.

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

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

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

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

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

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

service-policy inside-policy global
```

What is a result of the configuration?

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

Answer: D

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

NEW QUESTION 285
- (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 290
- (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 295
- (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 298
- (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 301
- (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 306
- (Exam Topic 1)
What are two rootkit types? (Choose two)

A. registry
B. virtual

C. bootloader
D. user mode
E. buffer mode

Answer: CD

Explanation:
The term ‘rootkit’ originally comes from the Unix world, where the word ‘root’ is used to describe a user with thehighest possible level of access privileges, similar to an ‘Administrator’ in Windows. The word ‘kit’ refers to thesoftware that grants root-level access to the machine. Put the two together and you get ‘rootkit’, a program thatgives someone – with legitimate or malicious intentions – privileged access to a computer.There are four main types of rootkits: Kernel rootkits, User mode rootkits, Bootloader rootkits, Memory rootkits

NEW QUESTION 311
- (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 316
- (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 317
- (Exam Topic 1)
Which two characteristics of messenger protocols make data exfiltration difficult to detect and prevent? (Choose two)

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

Answer: CE

NEW QUESTION 321
- (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 322
- (Exam Topic 1)
Which network monitoring solution uses streams and pushes operational data to provide a near real-time view of activity?

A. SNMP
B. SMTP
C. syslog

D. model-driven telemetry

Answer: D

Explanation:
Reference: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide

NEW QUESTION 323
- (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 327
- (Exam Topic 1)
Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

A. Correlation
B. Intrusion
C. Access Control
D. Network Discovery

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/introd

NEW QUESTION 332
- (Exam Topic 1)
Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

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

Answer: A

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

NEW QUESTION 337
- (Exam Topic 1)
Which two kinds of attacks are prevented by multifactor authentication? (Choose two)

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

Answer: BC

NEW QUESTION 342
- (Exam Topic 1)
Which statement about the configuration of Cisco ASA NetFlow v9 Secure Event Logging is true?

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

Answer: D

NEW QUESTION 344

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

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

Answer: C

NEW QUESTION 345
- (Exam Topic 1)
What must be used to share data between multiple security products?

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

Answer: B

NEW QUESTION 350
- (Exam Topic 1)
An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA. Which Cisco ASA command must be used?

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

Answer: A

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

NEW QUESTION 351
- (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 356
- (Exam Topic 1)
Refer to the exhibit.

Interface	MAC Address	Method	Domain	Status	Fg Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth	0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth	0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth	0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth	0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth	0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth	0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth	0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth	0A02198200000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth	0A02198200001
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth	0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth	0A02198200000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth	0A02198200000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth	0A02198200001
Gi7/4	54ee.75db.d766	dot1x	DATA	Auth	0A02198200001
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth	0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth	0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth	0A02198200000

Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

A. show authentication registrations
B. show authentication method

C. show dot1x all
D. show authentication sessions

Answer: D

Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-c Displaying the Summary of All Auth Manager Sessions on the Switch
Enter the following:
Switch# show authentication sessions
Interface MAC Address Method Domain Status Session ID
Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58
Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

NEW QUESTION 358
- (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 360
- (Exam Topic 1)
When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?

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

Answer: B

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

NEW QUESTION 361
- (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 364
- (Exam Topic 1)
Which functions of an SDN architecture require southbound APIs to enable communication?

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

Answer: A

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

NEW QUESTION 367
- (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 372
- (Exam Topic 1)
Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

A. File Analysis
B. SafeSearch
C. SSL Decryption
D. Destination Lists

Answer: C

Explanation:
Reference:
https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-IntelligentProxy

NEW QUESTION 373
- (Exam Topic 1)
Which two statements about a Cisco WSA configured in Transparent mode are true? (Choose two)

A. It can handle explicit HTTP requests.
B. It requires a PAC file for the client web browser.
C. It requires a proxy for the client web browser.
D. WCCP v2-enabled devices can automatically redirect traffic destined to port 80.
E. Layer 4 switches can automatically redirect traffic destined to port 80.

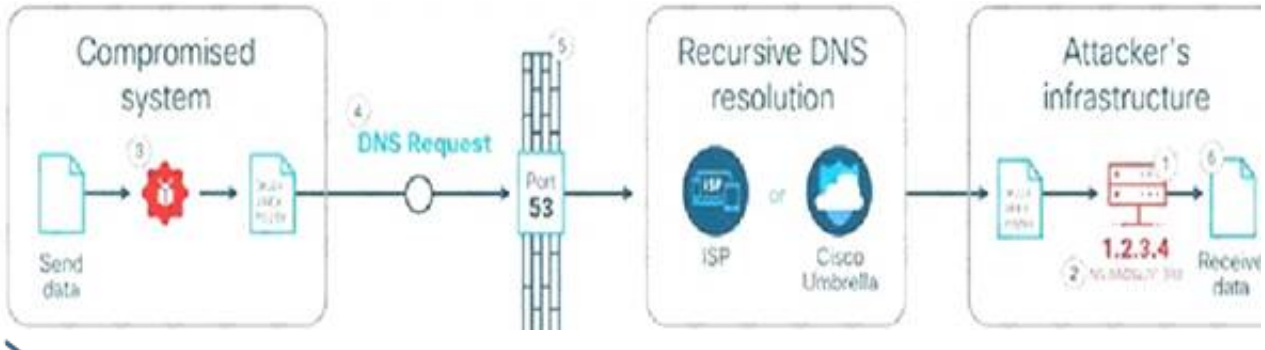
Answer: DE

NEW QUESTION 376
- (Exam Topic 1)
How is DNS tunneling used to exfiltrate data out of a corporate network?

A. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.
B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.
C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damageand theft on the network.
D. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.

Answer: B

Explanation:
Domain name system (DNS) is the protocol that translates human-friendly URLs, such as securitytut.com, into IP addresses, such as 183.33.24.13. Because DNS messages are only used as the beginning of each communication and they are not intended for data transfer, many organizations do not monitor their DNS traffic for malicious activity. As a result, DNS-based attacks can be effective if launched against their networks. DNS tunneling is one such attack.An example of DNS Tunneling is shown below:



The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNSnameserver (NS) and malicious payload.2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. attackerdomain.com) is registered or reused. The registrar informs the top-level domain (.com) nameservers to refer requests for attackerdomain.com to ns.attackerdomain.com, which has a DNS record mapped to 1.2.3.43. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, P028X977W,…).4. The payload initiates thousands of unique DNS record requests to the attacker's domain with each string as

Reference: https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0

NEW QUESTION 381
- (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 385
- (Exam Topic 1)
What is a characteristic of a bridge group in ASA Firewall transparent mode?

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

Answer: A

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

NEW QUESTION 386
- (Exam Topic 1)
What Cisco command shows you the status of an 802.1X connection on interface gi0/1?

A. show authorization status
B. show authen sess int gi0/1
C. show connection status gi0/1
D. show ver gi0/1

Answer: B

NEW QUESTION 391
- (Exam Topic 1)
Which technology reduces data loss by identifying sensitive information stored in public computing environments?

A. Cisco SDA
B. Cisco Firepower
C. Cisco HyperFlex
D. Cisco Cloudlock

Answer: D

NEW QUESTION 394
- (Exam Topic 1)
A malicious user gained network access by spoofing printer connections that were authorized using MAB on four different switch ports at the same time. What two catalyst switch security features will prevent further violations? (Choose two)

A. DHCP Snooping
B. 802.1AE MacSec
C. Port security
D. IP Device track
E. Dynamic ARP inspection
F. Private VLANs

Answer: AE

NEW QUESTION 398
- (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 401
- (Exam Topic 1)
How does Cisco Umbrella archive logs to an enterprise owned storage?

A. by using the Application Programming Interface to fetch the logs
B. by sending logs via syslog to an on-premises or cloud-based syslog server
C. by the system administrator downloading the logs from the Cisco Umbrella web portal
D. by being configured to send logs to a self-managed AWS S3 bucket

Answer: D

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

NEW QUESTION 402
- (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 403
- (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 408
- (Exam Topic 1)
Which two are valid suppression types on a Cisco Next Generation Intrusion Prevention System? (Choose two)

A. Port
B. Rule
C. Source
D. Application
E. Protocol

Answer: BC

NEW QUESTION 411
- (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 413
- (Exam Topic 1)
What is a characteristic of Dynamic ARP Inspection?

A. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCPsnooping binding database.
B. In a typical network, make all ports as trusted except for the ports connecting to switches, which are untrusted
C. DAI associates a trust state with each switch.
D. DAI intercepts all ARP requests and responses on trusted ports only.

Answer: A

NEW QUESTION 414
- (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 417
- (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 419
- (Exam Topic 1)
When wired 802.1X authentication is implemented, which two components are required? (Choose two)

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

Answer: AC

NEW QUESTION 423
- (Exam Topic 1)
How is ICMP used an exfiltration technique?

A. by flooding the destination host with unreachable packets
B. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address
C. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host
D. by overwhelming a targeted host with ICMP echo-request packets

Answer: C

NEW QUESTION 425
- (Exam Topic 1)
What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?

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

Answer: A

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

NEW QUESTION 427
- (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 430
- (Exam Topic 1)
How is Cisco Umbrella configured to log only security events?

A. per policy
B. in the Reporting settings
C. in the Security Settings section
D. per network in the Deployments section

Answer: A

Explanation:
Reference: https://docs.umbrella.com/deployment-umbrella/docs/log-management

NEW QUESTION 435
- (Exam Topic 1)
What is the function of Cisco Cloudlock for data security?

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

Answer: A

NEW QUESTION 439
- (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 440
- (Exam Topic 1)
Which two conditions are prerequisites for stateful failover for IPsec? (Choose two)

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

Answer: CE

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

NEW QUESTION 442
- (Exam Topic 1)
An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?

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

Answer: D

NEW QUESTION 444
- (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 446
- (Exam Topic 3)
Which security solution uses NetFlow to provide visibility across the network, data center, branch offices, and cloud?

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

Answer: B

NEW QUESTION 451
- (Exam Topic 3)
An engineer is trying to decide whether to use Cisco Umbrella, Cisco CloudLock, Cisco Stealthwatch, or Cisco AppDynamics Cloud Monitoring for visibility into data transfers as well as protection against data exfiltration Which solution best meets these requirements?

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

Answer: D

NEW QUESTION 454
- (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 458
- (Exam Topic 3)
When network telemetry is implemented, what is important to be enabled across all network infrastructure devices to correlate different sources?

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

Answer: B

NEW QUESTION 459
- (Exam Topic 3)
Which attribute has the ability to change during the RADIUS CoA?

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

Answer: B

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

NEW QUESTION 462
- (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 465
- (Exam Topic 3)
Which Cisco security solution stops exfiltration using HTTPS?

A. Cisco FTD
B. Cisco AnyConnect
C. Cisco CTA
D. Cisco ASA

Answer: C

Explanation:
https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-7365

NEW QUESTION 468
- (Exam Topic 3)
What is the difference between EPP and EDR?

A. EPP focuses primarily on threats that have evaded front-line defenses that entered the environment.
B. Having an EPP solution allows an engineer to detect, investigate, and remediate modern threats.
C. EDR focuses solely on prevention at the perimeter.
D. Having an EDR solution gives an engineer the capability to flag offending files at the first sign of malicious behavior.

Answer: B

NEW QUESTION 473
- (Exam Topic 3)
Which Cisco platform processes behavior baselines, monitors for deviations, and reviews for malicious processes in data center traffic and servers while performing software vulnerability detection?

A. Cisco Tetration
B. Cisco ISE
C. Cisco AMP for Network
D. Cisco AnyConnect

Answer: A

NEW QUESTION 474
- (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 475
- (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 477
- (Exam Topic 3)
Which Cisco security solution determines if an endpoint has the latest OS updates and patches installed on the system?

A. Cisco Endpoint Security Analytics

B. Cisco AMP for Endpoints
C. Endpoint Compliance Scanner
D. Security Posture Assessment Service

Answer: A

NEW QUESTION 478
- (Exam Topic 3)
Which type of data does the Cisco Stealthwatch system collect and analyze from routers, switches, and firewalls?

A. NTP
B. syslog
C. SNMP
D. NetFlow

Answer: D

NEW QUESTION 480
- (Exam Topic 3)
A network engineer is tasked with configuring a Cisco ISE server to implement external authentication against Active Directory. What must be considered about the authentication requirements? (Choose two.)

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

Answer: BC

NEW QUESTION 482
- (Exam Topic 3)
Which baseline form of telemetry is recommended for network infrastructure devices?

A. SDNS
B. NetFlow
C. passive taps
D. SNMP

Answer: D

NEW QUESTION 484
- (Exam Topic 3)
Which type of attack is MFA an effective deterrent for?

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

Answer: B

NEW QUESTION 488
- (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 490
- (Exam Topic 3)
What are two functionalities of SDN Northbound APIs? (Choose two.)

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

Answer: AB

NEW QUESTION 491

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

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

Answer: B

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

NEW QUESTION 495
- (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 497
- (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 498
- (Exam Topic 3)
Client workstations are experiencing extremely poor response time. An engineer suspects that an attacker is eavesdropping and making independent connections while relaying messages between victims to make them think they are talking to each other over a private connection. Which feature must be enabled and configured to provide relief from this type of attack?

A. Link Aggregation
B. Reverse ARP
C. private VLANs
D. Dynamic ARP Inspection

Answer: D

NEW QUESTION 502
- (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 505
- (Exam Topic 3)
Which function is included when Cisco AMP is added to web security?

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

Answer: B

NEW QUESTION 509
- (Exam Topic 3)
Which type of encryption uses a public key and private key?

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

Answer: A

NEW QUESTION 513
- (Exam Topic 3)
When a transparent authentication fails on the Web Security Appliance, which type of access does the end user get?

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

Answer: C

NEW QUESTION 514
- (Exam Topic 3)
Why should organizations migrate to an MFA strategy for authentication?

A. Single methods of authentication can be compromised more easily than MFA.
B. Biometrics authentication leads to the need for MFA due to its ability to be hacked easily.
C. MFA methods of authentication are never compromised.
D. MFA does not require any piece of evidence for an authentication mechanism.

Answer: A

NEW QUESTION 519
- (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 521
- (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 523
- (Exam Topic 3)
An engineer is configuring Cisco Umbrella and has an identity that references two different policies. Which action ensures that the policy that the identity must use takes precedence over the second one?

A. Configure the default policy to redirect the requests to the correct policy
B. Place the policy with the most-specific configuration last in the policy order
C. Configure only the policy with the most recently changed timestamp
D. Make the correct policy first in the policy order

Answer: D

NEW QUESTION 526
- (Exam Topic 3)
A large organization wants to deploy a security appliance in the public cloud to form a site-to-site VPN and link the public cloud environment to the private cloud in the headquarters data center. Which Cisco
security appliance meets these requirements?

A. Cisco Cloud Orchestrator
B. Cisco ASAV
C. Cisco WSAV
D. Cisco Stealthwatch Cloud

Answer: B

NEW QUESTION 528
- (Exam Topic 3)
Which threat intelligence standard contains malware hashes?

A. structured threat information expression
B. advanced persistent threat
C. trusted automated exchange or indicator information
D. open command and control

Answer: A

NEW QUESTION 529
- (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 532
- (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 537
- (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 [redacted] 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 538
- (Exam Topic 3)
Which category includes DoS Attacks?

A. Virus attacks

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

Answer: C

NEW QUESTION 539
- (Exam Topic 3)
Which Cisco solution extends network visibility, threat detection, and analytics to public cloud environments?

A. Cisco Umbrella
B. Cisco Stealthwatch Cloud
C. Cisco Appdynamics
D. Cisco CloudLock

Answer: B

NEW QUESTION 541
- (Exam Topic 3)
Refer to the exhibit.

```
"remarks" [],
"destinationService" {
"kind" serviceKind,
"value": destinationServic
},
"permit" trueORfalse,
"active" "true",
"position" "1",
"sourceAddress" {
"kind" sourceAddressKind,
"value" sourceAddress
}
}

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

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


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

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

Answer: A

NEW QUESTION 542
- (Exam Topic 3)
An organization must add new firewalls to its infrastructure and wants to use Cisco ASA or Cisco FTD.
The chosen firewalls must provide methods of blocking traffic that include offering the user the option to bypass the block for certain sites after displaying a warning page and to reset the connection. Which solution should the organization choose?

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

Answer: C

NEW QUESTION 546
- (Exam Topic 3)
What is the difference between a vulnerability and an exploit?

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

Answer: B

NEW QUESTION 548
- (Exam Topic 3)
Which threat intelligence standard contains malware hashes?

A. advanced persistent threat
B. open command and control
C. structured threat information expression
D. trusted automated exchange of indicator information

Answer: C

NEW QUESTION 550
- (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 551
- (Exam Topic 2)
How does DNS Tunneling exfiltrate data?

A. An attacker registers a domain that a client connects to based on DNS records and sends malware through that connection.
B. An attacker opens a reverse DNS shell to get into the client's system and install malware on it.
C. An attacker uses a non-standard DNS port to gain access to the organization's DNS servers in order to poison the resolutions.
D. An attacker sends an email to the target with hidden DNS resolvers in it to redirect them to a malicious domain.

Answer: A

NEW QUESTION 552
- (Exam Topic 2)
What is a functional difference between a Cisco ASA and a Cisco IOS router with Zone-based policy firewall?

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

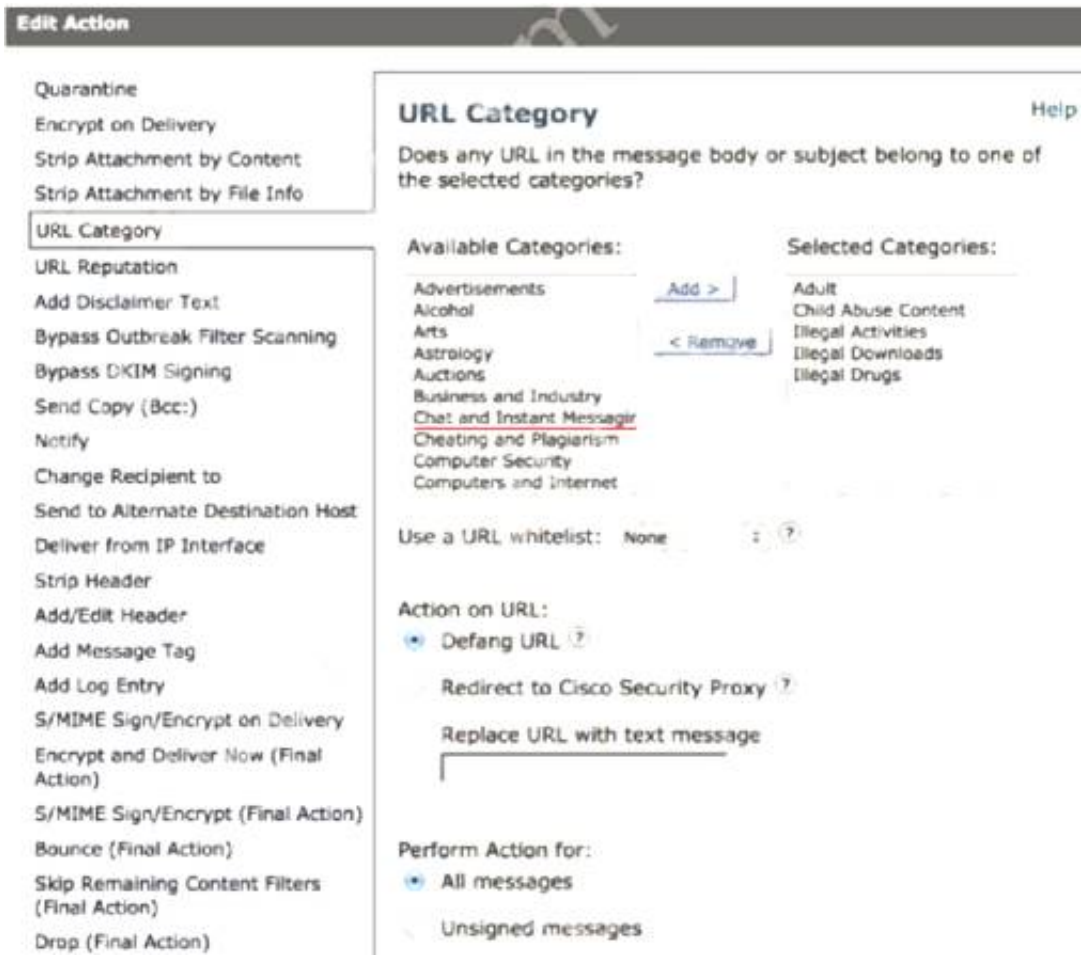
Answer: A

NEW QUESTION 557
- (Exam Topic 2)
A network administrator is configuring a rule in an access control policy to block certain URLs and selects the "Chat and Instant Messaging" category. Which reputation score should be selected to accomplish this goal?

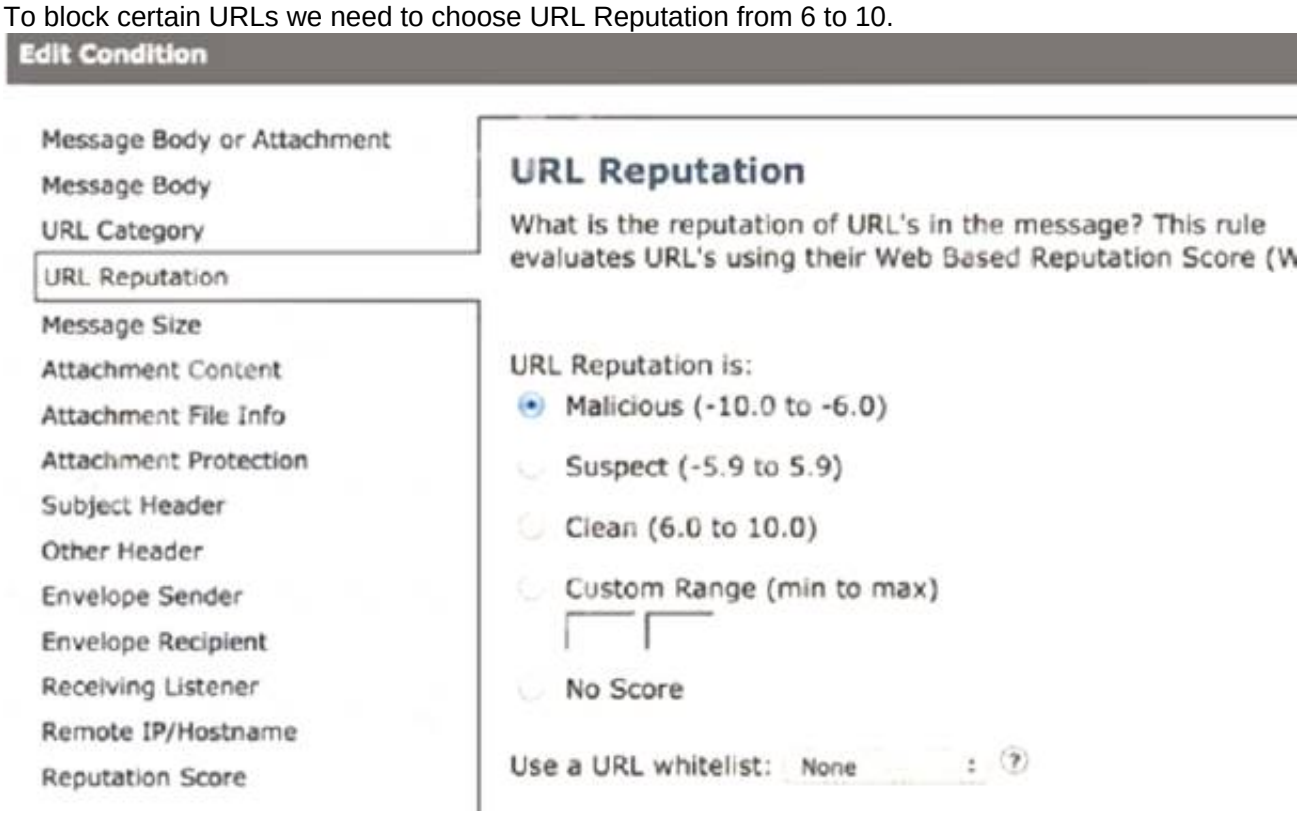
A. 1
B. 3
C. 5
D. 10

Answer: D

Explanation:
We choose "Chat and Instant Messaging" category in "URL Category":



To block certain URLs we need to choose URL Reputation from 6 to 10.



NEW QUESTION 558
- (Exam Topic 2)
Which attack type attempts to shut down a machine or network so that users are not able to access it?

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

Answer: A

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

NEW QUESTION 562
- (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 563
- (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 568
- (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 572
- (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 576
- (Exam Topic 2)
What is provided by the Secure Hash Algorithm in a VPN?

A. integrity
B. key exchange
C. encryption
D. authentication

Answer: A

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

NEW QUESTION 580
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 350-701 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 350-701 Product From:

https://www.2passeasy.com/dumps/350-701/

Money Back Guarantee

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