

Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies



NEW QUESTION 1

- (Exam Topic 2)

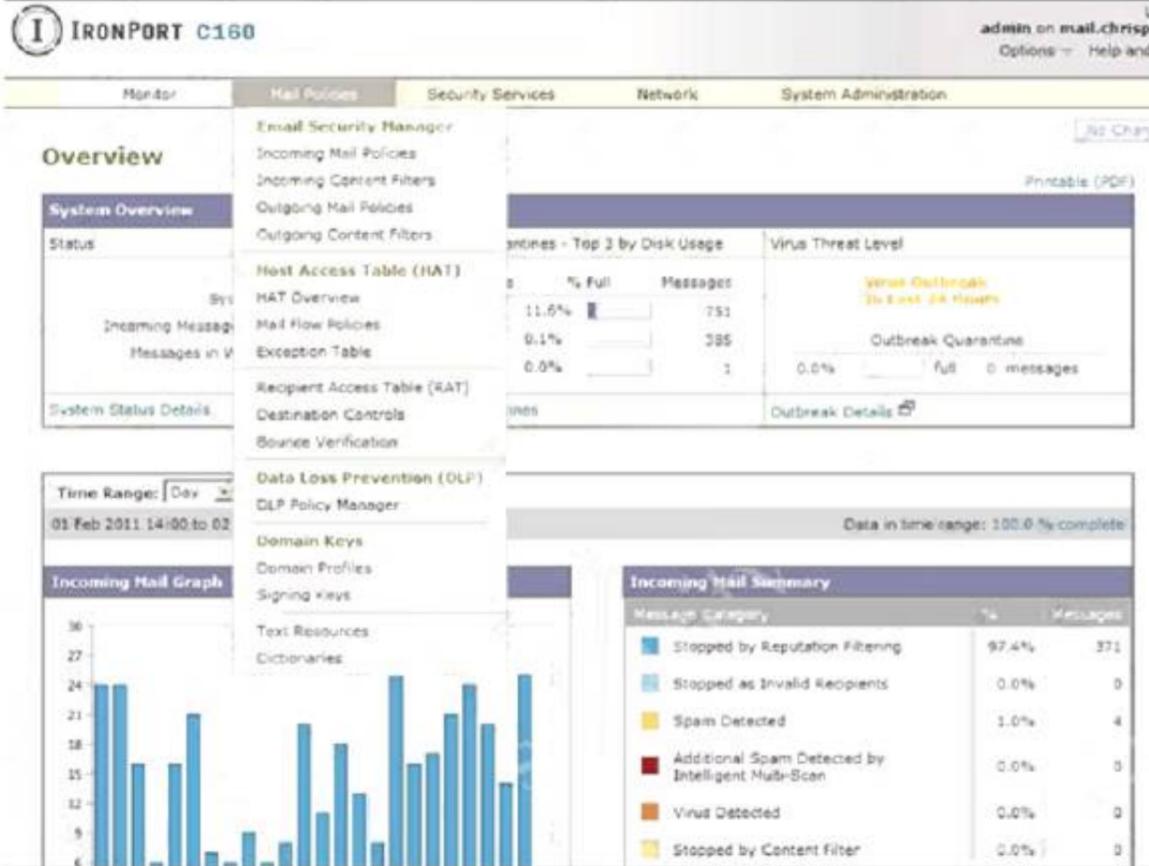
An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically. What must be configured to accomplish this?

- A. Configure the Cisco WSA to modify policies based on the traffic seen
- B. Configure the Cisco ESA to receive real-time updates from Talos
- C. Configure the Cisco WSA to receive real-time updates from Talos
- D. Configure the Cisco ESA to modify policies based on the traffic seen

Answer: D

Explanation:

The Mail Policies menu is where almost all of the controls related to email filtering happens. All the security and content filtering policies are set here, so it's likely that, as an ESA administrator, the pages on this menu are where you are likely to spend most of your time.



NEW QUESTION 2

- (Exam Topic 2)

Drag and drop the descriptions from the left onto the correct protocol versions on the right.

standard includes NAT-T

uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

IKEv1

IKEv2

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated with low confidence

NEW QUESTION 3

- (Exam Topic 2)

Which type of algorithm provides the highest level of protection against brute-force attacks?

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

Answer: D

NEW QUESTION 4

- (Exam Topic 2)

What is a function of 3DES in reference to cryptography?

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

Answer: C

NEW QUESTION 5

- (Exam Topic 2)

A network administrator is using the Cisco ESA with AMP to upload files to the cloud for analysis. The network is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?

- A. AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.
- B. The file is queued for upload when connectivity is restored.
- C. The file upload is abandoned.
- D. The ESA immediately makes another attempt to upload the file.

Answer: C

Explanation:

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technoteesa-00.html>In this question, it stated "the network is congested" (not the file analysis server was overloaded) so the appliance will not try to upload the file again.

NEW QUESTION 6

- (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 7

- (Exam Topic 2)

An organization has a Cisco ESA set up with policies and would like to customize the action assigned for violations. The organization wants a copy of the message to be delivered with a message added to flag it as a DLP violation. Which actions must be performed in order to provide this capability?

- A. deliver and send copies to other recipients
- B. quarantine and send a DLP violation notification
- C. quarantine and alter the subject header with a DLP violation
- D. deliver and add disclaimer text

Answer: D

Explanation:

Reference:

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

NEW QUESTION 8

- (Exam Topic 2)

How does Cisco Advanced Phishing Protection protect users?

- A. It validates the sender by using DKIM.

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

Answer: D

Explanation:

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

NEW QUESTION 9

- (Exam Topic 2)

Why is it important to have logical security controls on endpoints even though the users are trained to spot security threats and the network devices already help prevent them?

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

Answer: D

NEW QUESTION 10

- (Exam Topic 2)

Why is it important to implement MFA inside of an organization?

- A. To prevent man-the-middle attacks from being successful.
- B. To prevent DoS attacks from being successful.
- C. To prevent brute force attacks from being successful.
- D. To prevent phishing attacks from being successful.

Answer: C

NEW QUESTION 10

- (Exam Topic 2)

What are two DDoS attack categories? (Choose two)

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

Answer: BD

Explanation:

There are three basic categories of attack:+ volume-based attacks, which use high traffic to inundate the network bandwidth+ protocol attacks, which focus on exploiting server resources+ application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks

Reference: <https://www.esecurityplanet.com/networks/types-of-ddos-attacks/>

NEW QUESTION 11

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 13

- (Exam Topic 2)

Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 16

- (Exam Topic 1)

Refer to the exhibit.

```
Sysauthcontrol          Enabled
Dot1x Protocol Version    3

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

Which command was used to display this output?

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

Answer: A

NEW QUESTION 17

- (Exam Topic 1)

Which two descriptions of AES encryption are true? (Choose two)

- A. AES is less secure than 3DES.
- B. AES is more secure than 3DES.
- C. AES can use a 168-bit key for encryption.
- D. AES can use a 256-bit key for encryption.
- E. AES encrypts and decrypts a key three times in sequence.

Answer: BD

NEW QUESTION 21

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Configure a Crypto ISAKMP Key
 In order to configure a preshared
 configuration mode:

authentication key, enter the crypto isakmp key
 command in global

crypto isakmp key cisco123 address 172.16.1.1

<https://community.cisco.com/t5/vpn/isakmp-with-0-0-0-0-dmvpn/td-p/4312380>

It is a bad practice but it is valid. 172.16.0.0/16 the full range will be accepted as possible PEER

[https://www.examtactics.com/discussions/cisco/view/46191-exam-350-701-topic-1-question-71-discussion/#:~:t=Testing without a netmask shows that command interpretation has a preference for /16 and /24.](https://www.examtactics.com/discussions/cisco/view/46191-exam-350-701-topic-1-question-71-discussion/#:~:t=Testing%20without%20a%20netmask%20shows%20that%20command%20interpretation%20has%20a%20preference%20for%20%2F16%20and%20%2F24.)

CSR-1(config)#crypto isakmp key cisco123 address 172.16.0.0

CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.0.0 [255.255.0.0] cisco123

CSR-1(config)#no crypto isakmp key cisco123 address 172.16.0.0 CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.0 CSR-1(config)#do show crypto isakmp key | i cisco

default 172.16.1.0 [255.255.255.0] cisco123

CSR-1(config)#no crypto isakmp key cisco123 address 172.16.1.0 CSR-1(config)#crypto isakmp key cisco123 address 172.16.1.128

CSR-1(config)#do show crypto isakmp key | i cisco default 172.16.1.128 cisco123 CSR-1(config)#

NEW QUESTION 24

- (Exam Topic 1)

What are the two most commonly used authentication factors in multifactor authentication? (Choose two)

- A. biometric factor
- B. time factor
- C. confidentiality factor
- D. knowledge factor
- E. encryption factor

Answer: AD

Explanation:

Reference: <https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html>The two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint, face, and retina scans. Biometrics is used commonly in mobile devices).

NEW QUESTION 28

- (Exam Topic 1)

Why would a user choose an on-premises ESA versus the CES solution?

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

Answer: A

NEW QUESTION 29

- (Exam Topic 1)

Which two key and block sizes are valid for AES? (Choose two)

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

Answer: CD

Explanation:

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

NEW QUESTION 33

- (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 37

- (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 38

- (Exam Topic 1)

When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

- A. Application Control
- B. Security Category Blocking
- C. Content Category Blocking
- D. File Analysis

Answer: B

NEW QUESTION 43

- (Exam Topic 1)

What is a characteristic of traffic storm control behavior?

- A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
- B. Traffic storm control cannot determine if the packet is unicast or broadcast.
- C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
- D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

Answer: A

NEW QUESTION 46

- (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 the highest possible level of access privileges, similar to an 'Administrator' in Windows. The word 'kit' refers to the software that grants root-level access to the machine. Put the two together and you get 'rootkit', a program that gives 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 48

- (Exam Topic 1)

Which exfiltration method does an attacker use to hide and encode data inside DNS requests and queries?

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

Answer: A

Explanation:

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

NEW QUESTION 49

- (Exam Topic 1)

Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?

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

Answer: B

NEW QUESTION 53

- (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 56

- (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 60

- (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 61

- (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 62

- (Exam Topic 1)

When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, which name is used?

- A. Common Security Exploits
- B. Common Vulnerabilities and Exposures
- C. Common Exploits and Vulnerabilities
- D. Common Vulnerabilities, Exploits and Threats

Answer: B

Explanation:

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

NEW QUESTION 63

- (Exam Topic 1)

What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services? (Choose two)

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

Answer: BD

NEW QUESTION 64

- (Exam Topic 1)

Which two mechanisms are used to control phishing attacks? (Choose two)

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

Answer: AE

NEW QUESTION 69

- (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 73

- (Exam Topic 1)

An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch was not installed, which left the endpoint vulnerable to WannaCry ransomware. Which two solutions mitigate the risk of this ransom ware infection? (Choose two)

- A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.
- B. Set up a profiling policy in Cisco Identity Service Engine to check and endpoint patch level before allowing access on the network.
- C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.
- D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.
- E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.

Answer: AC

Explanation:

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

[File Conditions List > pc_W10_64_KB4012606_Ms17-010_1507_W](#)

File Condition

* Name	pc_W10_64_KB4012606_Ms1
Description	Cisco Predefined Check: Micro
* Operating System	Windows 10 (All)
Compliance Module	Any version
* File Type	FileVersion
* File Path	SYSTEM_32
* Operator	LaterThan
* File Version	10.0.10240.17318

NEW QUESTION 78

- (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 and quarantine. 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 79

- (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 84

- (Exam Topic 1)

Which two tasks allow NetFlow on a Cisco ASA 5500 Series firewall? (Choose two)

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

Answer: CE

NEW QUESTION 88

- (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 93

- (Exam Topic 1)

In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

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

Answer: C

Explanation:

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

NEW QUESTION 98

- (Exam Topic 1)

Which two deployment modes does the Cisco ASA FirePower module support? (Choose two)

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

Answer: CD

Explanation:

Reference:

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

NEW QUESTION 100

- (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 101

- (Exam Topic 1)

Which compliance status is shown when a configured posture policy requirement is not met?

- A. compliant
- B. unknown
- C. authorized
- D. noncompliant

Answer: D

Explanation:

Reference:

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

NEW QUESTION 104

- (Exam Topic 1)

Refer to the exhibit.

```
def add_device_to_dnac(dnac_ip, device_ip, snmp_version,
    snmp_ro_community, snmp_rw_community,
    snmp_retry, snmp_timeout,
    cli_transport, username, password, enable_password):
    device_object = {
        'ipAddress': [
            device_ip
        ],
        'type': 'NETWORK_DEVICE',
        'computeDevice': False,
        'snmpVersion': snmp_version,
        'snmpROCommunity': snmp_ro_community,
        'snmpRWCommunity': snmp_rw_community,
        'snmpRetry': snmp_retry,
        'snmpTimeout': snmp_timeout,
        'cliTransport': cli_transport,
        'userName': username,
        'password': password,
        'enablePassword': enable_password
    }
    response = requests.post(
        'https://{}/dna/intent/api/v1/network-
device'.format(dnac_ip),
        data=json.dumps(device_object),
        headers={
            'X-Auth-Token': '{}'.format(token),
            'Content-type': 'application/json'
        },
        verify=False
    )
    return response.json()
```

What is the result of this Python script of the Cisco DNA Center API?

- A. adds authentication to a switch
- B. adds a switch to Cisco DNA Center
- C. receives information about a switch
- D. deletes a switch from Cisco DNA Center

Answer: B

NEW QUESTION 107

- (Exam Topic 1)

What is a difference between FlexVPN and DMVPN?

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

Answer: C

NEW QUESTION 108

- (Exam Topic 1)

Which two activities can be done using Cisco DNA Center? (Choose two)

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

Answer: BE

Explanation:

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

NEW QUESTION 109

- (Exam Topic 1)

Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware? (Choose two)

- A. Sophos engine
- B. white list
- C. RAT
- D. outbreak filters
- E. DLP

Answer: AD

NEW QUESTION 114

- (Exam Topic 1)

Which command enables 802.1X globally on a Cisco switch?

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

Answer: A

NEW QUESTION 119

- (Exam Topic 1)

What provides the ability to program and monitor networks from somewhere other than the DNAC GUI?

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

Answer: D

NEW QUESTION 120

- (Exam Topic 1)

Which two behavioral patterns characterize a ping of death attack? (Choose two)

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

Answer: BD

Explanation:

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

NEW QUESTION 125

- (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 127

- (Exam Topic 1)

Which Cisco security solution protects remote users against phishing attacks when they are not connected to the VPN?

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

Answer: B

Explanation:

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

NEW QUESTION 132

- (Exam Topic 1)

Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application traffic?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 134

- (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 138

- (Exam Topic 1)

Which algorithm provides encryption and authentication for data plane communication?

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

Answer: A

Explanation:

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

NEW QUESTION 143

- (Exam Topic 1)

What is the difference between deceptive phishing and spear phishing?

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

Answer: B

Explanation:

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

NEW QUESTION 148

- (Exam Topic 1)

Which CLI command is used to register a Cisco FirePower sensor to Firepower Management Center?

- A. configure system add <host><key>
- B. configure manager <key> add host
- C. configure manager delete
- D. configure manager add <host><key>

Answer: D

NEW QUESTION 153

- (Exam Topic 1)

Which type of attack is social engineering?

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

Answer: B

Explanation:

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

NEW QUESTION 155

- (Exam Topic 1)

How many interfaces per bridge group does an ASA bridge group deployment support?

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

Answer: B

Explanation:

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

NEW QUESTION 160

- (Exam Topic 3)

Which command is used to log all events to a destination collector 209.165.201.107?

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

Answer: C

NEW QUESTION 163

- (Exam Topic 3)

Which Cisco security solution integrates with cloud applications like Dropbox and Office 365 while protecting data from being exfiltrated?

- A. Cisco Tajos
- B. Cisco Steathwatch Cloud
- C. Cisco Cloudlock
- D. Cisco Umbrella Investigate

Answer: C

NEW QUESTION 165

- (Exam Topic 3)

An administrator configures new authorization policies within Cisco ISE and has difficulty profiling the devices. Attributes for the new Cisco IP phones that are profiled based on the RADIUS authentication are seen however the attributes for CDP or DHCP are not. What should the administrator do to address this issue?

- A. Configure the ip dhcp snooping trust command on the DHCP interfaces to get the information to Cisco ISE
- B. Configure the authentication port-control auto feature within Cisco ISE to identify the devices that are trying to connect
- C. Configure a service template within the switch to standardize the port configurations so that the correct information is sent to Cisco ISE
- D. Configure the device sensor feature within the switch to send the appropriate protocol information

Answer: D

Explanation:

Reference:

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

NEW QUESTION 169

- (Exam Topic 3)

An engineer recently completed the system setup on a Cisco WSA Which URL information does the system send to SensorBase Network servers?

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

Answer: B

NEW QUESTION 171

- (Exam Topic 3)

Which two criteria must a certificate meet before the WSA uses it to decrypt application traffic? (Choose two.)

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

Answer: AB

NEW QUESTION 172

- (Exam Topic 3)

How does the Cisco WSA enforce bandwidth restrictions for web applications?

- A. It implements a policy route to redirect application traffic to a lower-bandwidth link.
- B. It dynamically creates a scavenger class QoS policy and applies it to each client that connects through the WSA.
- C. It sends commands to the uplink router to apply traffic policing to the application traffic.
- D. It simulates a slower link by introducing latency into application traffic.

Answer: C

NEW QUESTION 173

- (Exam Topic 3)

Why is it important to patch endpoints consistently?

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

Answer: B

NEW QUESTION 174

- (Exam Topic 3)

What is the term for the concept of limiting communication between applications or containers on the same node?

- A. container orchestration
- B. software-defined access
- C. microservicing
- D. microsegmentation

Answer: D

NEW QUESTION 175

- (Exam Topic 3)

Which open source tool does Cisco use to create graphical visualizations of network telemetry on Cisco IOS XE devices?

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

Answer: D

NEW QUESTION 180

- (Exam Topic 3)

An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users. Which action accomplishes this goal?

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

Answer: D

NEW QUESTION 183

- (Exam Topic 3)

Refer to the exhibit,

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

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

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

Answer: A

NEW QUESTION 187

- (Exam Topic 3)

An engineer is configuring their router to send NetFlow data to Stealthwatch which has an IP address of 1.1.1.1 using the flow record Stealthwatch406397954 command Which additional command is required to complete the flow record?

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

Answer: B

NEW QUESTION 191

- (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 192

- (Exam Topic 3)

Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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

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

Answer: D

NEW QUESTION 195

- (Exam Topic 3)

An engineer has been tasked with configuring a Cisco FTD to analyze protocol fields and detect anomalies in the traffic from industrial systems. What must be done to meet these requirements?

- A. Implement pre-filter policies for the CIP preprocessor
- B. Enable traffic analysis in the Cisco FTD
- C. Configure intrusion rules for the DNP3 preprocessor
- D. Modify the access control policy to trust the industrial traffic

Answer: C

Explanation:

"configure INTRUSION RULES for DNP3" -> Documentation states, that enabling INTRUSION RULES is mandatory for CIP to work + required preprocessors (in Network Access Policy - NAP) will be enabled automatically:

"If you want the CIP preprocessor rules listed in the following table to generate events, you MUST enable them. See Setting Intrusion Rule States for information on enabling rules."

"If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings, although the preprocessor remains disabled in the web interface for the corresponding network analysis policy."

[1]
<https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada>

NEW QUESTION 198

- (Exam Topic 3)

An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users.

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

Answer: A

NEW QUESTION 199

- (Exam Topic 3)

Which cloud service offering allows customers to access a web application that is being hosted, managed, and maintained by a cloud service provider?

- A. IaC
- B. SaaS
- C. IaaS
- D. PaaS

Answer: B

NEW QUESTION 203

- (Exam Topic 3)

Which technology provides a combination of endpoint protection endpoint detection, and response?

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

Answer: A

NEW QUESTION 204

- (Exam Topic 3)

Drag and drop the cloud security assessment components from the left onto the definitions on the right.

user entity behavior assessment	develop a cloud security strategy and roadmap aligned to business priorities
cloud data protection assessment	identify strengths and areas for improvement in the current security architecture during onboarding
cloud security strategy workshop	understand the security posture of the data or activity taking place in public cloud deployments
cloud security architecture assessment	detect potential anomalies in user behavior that suggest malicious behavior in a Software-as-a-Service application

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

user entity behavior assessment	cloud security strategy workshop
cloud data protection assessment	cloud security architecture assessment
cloud security strategy workshop	cloud data protection assessment
cloud security architecture assessment	user entity behavior assessment

NEW QUESTION 207

- (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 209

- (Exam Topic 3)

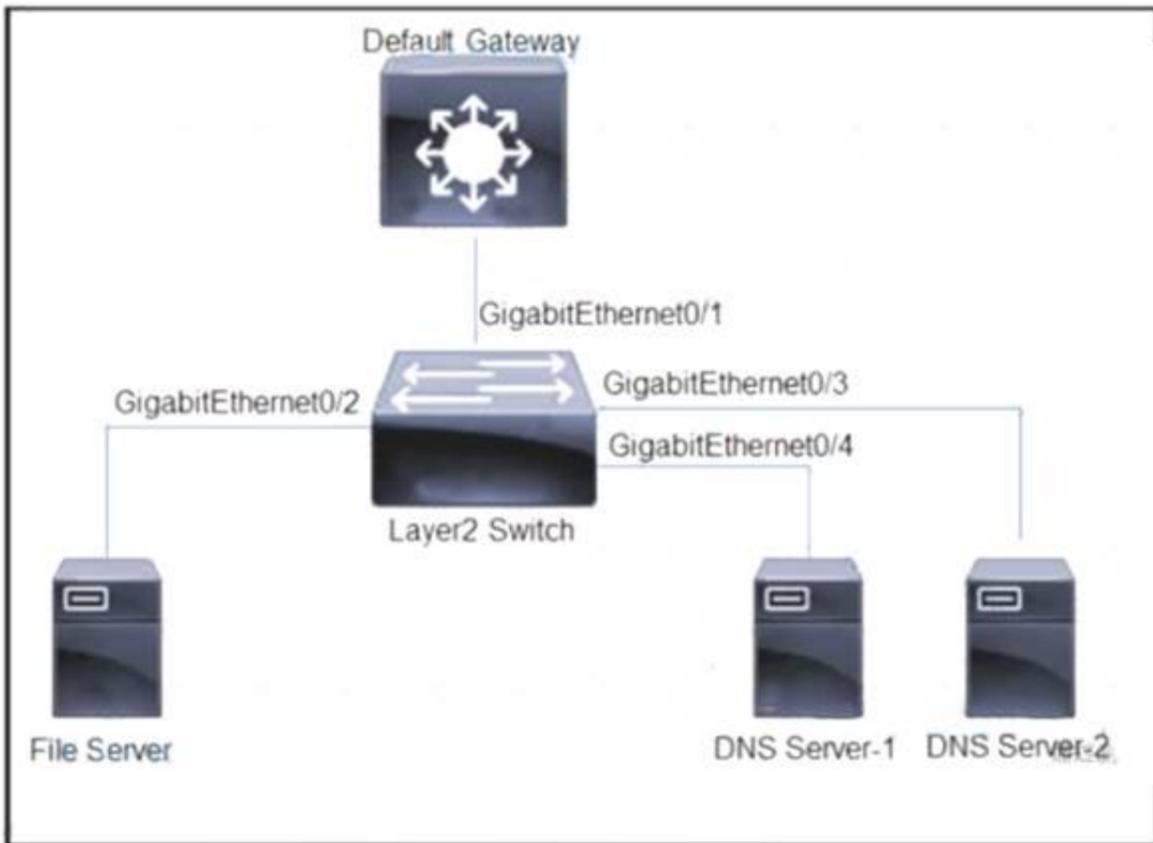
Which feature requires that network telemetry be enabled?

- A. per-interface stats
- B. SNMP trap notification
- C. Layer 2 device discovery
- D. central syslog system

Answer: D

NEW QUESTION 210

- (Exam Topic 3)



Refer to the exhibit. All servers are in the same VLAN/Subnet. DNS Server-1 and DNS Server-2 must communicate with each other, and all servers must communicate with default gateway multilayer switch. Which type of private VLAN ports should be configured to prevent communication between DNS servers and the file server?

- A. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as isolated port, and GigabitEthernet0/3 and GigabitEthernet0/4 as promiscuous ports.
- B. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as promiscuous port, Gigabit Ethernet0/3 and GigabitEthernet0/4 as isolated ports
- C. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as isolated port and GigabitEthernet0/3 and GrgabitEthernet0/4 as community ports
- D. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as community port, and GigabitEthernet0/3 and GrgabitEthernet0/4 as isolated ports.

Answer: C

NEW QUESTION 213

- (Exam Topic 3)

Which two protocols must be configured to authenticate end users to the Web Security Appliance? (Choose two.)

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

Answer: AB

NEW QUESTION 215

- (Exam Topic 3)

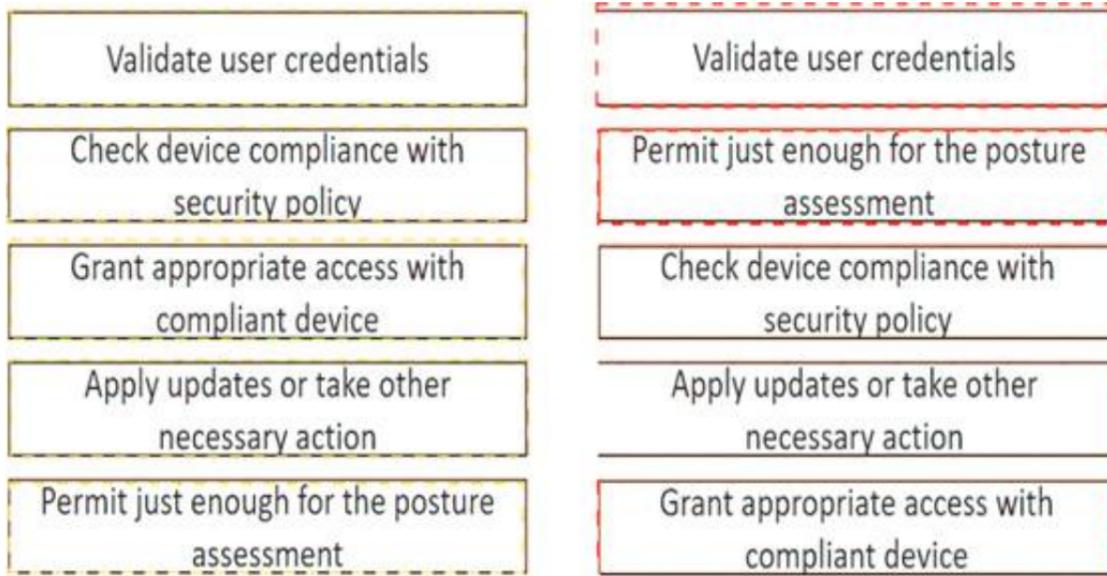
Drag and drop the posture assessment flow actions from the left into a sequence on the right.

Validate user credentials	step 1
Check device compliance with security policy	step 2
Grant appropriate access with compliant device	step 3
Apply updates or take other necessary action	step 4
Permit just enough for the posture assessment	step 5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 216

- (Exam Topic 3)

What is the process In DevSecOps where all changes In the central code repository are merged and synchronized?

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

Answer: C

NEW QUESTION 218

- (Exam Topic 3)

An engineer is adding a Cisco DUO solution to the current TACACS+ deployment using Cisco ISE. The engineer wants to authenticate users using their account when they log into network devices. Which action accomplishes this task?

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

Answer: B

NEW QUESTION 219

- (Exam Topic 3)

What is the term for when an endpoint is associated to a provisioning WLAN that is shared with guest access, and the same guest portal is used as the BYOD portal?

- A. single-SSID BYOD
- B. multichannel GUI
- C. dual-SSID BYOD
- D. streamlined access

Answer: C

NEW QUESTION 220

- (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/configuration

NEW QUESTION 225

- (Exam Topic 3)

What is a difference between GETVPN and IPsec?

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

Answer: C

NEW QUESTION 230

- (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 232

- (Exam Topic 3)

An engineer is configuring IPsec VPN and needs an authentication protocol that is reliable and supports ACK and sequence. Which protocol accomplishes this goal?

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

Answer: D

NEW QUESTION 236

- (Exam Topic 3)

What does endpoint isolation in Cisco AMP for Endpoints security protect from?

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

Answer: C

Explanation:

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

NEW QUESTION 240

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 243

- (Exam Topic 3)

Which action must be taken in the AMP for Endpoints console to detect specific MD5 signatures on endpoints and then quarantine the files?

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

Answer: A

NEW QUESTION 246

- (Exam Topic 3)

A network administrator is configuring a role 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. 3
- B. 5
- C. 10
- D. 1

Answer: C

NEW QUESTION 249

- (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 254

- (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 259

- (Exam Topic 3)

Drag and drop the exploits from the left onto the type of security vulnerability on the right.

causes memory access errors	path transversal
makes the client the target of attack	cross-site request forgery
gives unauthorized access to web server files	SQL injection
accesses or modifies application data	buffer overflow

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

causes memory access errors	gives unauthorized access to web server files
makes the client the target of attack	makes the client the target of attack
gives unauthorized access to web server files	accesses or modifies application data
accesses or modifies application data	causes memory access errors

NEW QUESTION 264

- (Exam Topic 3)

An engineer must configure Cisco AMP for Endpoints so that it contains a list of files that should not be executed by users. These files must not be quarantined. Which action meets this configuration requirement?

- A. Identify the network IPs and place them in a blocked list.
- B. Modify the advanced custom detection list to include these files.
- C. Create an application control blocked applications list.

D. Add a list for simple custom detection.

Answer: C

NEW QUESTION 268

- (Exam Topic 3)

What is a difference between a DoS attack and a DDoS attack?

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

Answer: A

NEW QUESTION 270

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 271

- (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 272

- (Exam Topic 3)

Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)

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

Answer: AE

NEW QUESTION 277

- (Exam Topic 3)

Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

- A. OpenC2
- B. OpenIOC
- C. CybOX
- D. STIX

Answer: D

NEW QUESTION 280

- (Exam Topic 3)

Which two authentication protocols are supported by the Cisco WSA? (Choose two.)

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

Answer: BE

NEW QUESTION 285

- (Exam Topic 3)

An engineer is implementing DHCP security mechanisms and needs the ability to add additional attributes to profiles that are created within Cisco ISE. Which action accomplishes this task?

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

Answer: D

NEW QUESTION 287

- (Exam Topic 3)

What is a benefit of flexible NetFlow records?

- A. They are used for security
- B. They are used for accounting
- C. They monitor a packet from Layer 2 to Layer 5
- D. They have customized traffic identification

Answer: D

Explanation:

<https://confluence.netvizura.com/display/NVUG/Traditional+vs.+Flexible+NetFlow>

NEW QUESTION 288

- (Exam Topic 3)

An organization deploys multiple Cisco FTD appliances and wants to manage them using one centralized solution. The organization does not have a local VM but does have existing Cisco ASAs that must migrate over to Cisco FTDs. Which solution meets the needs of the organization?

- A. Cisco FMC
- B. CSM
- C. Cisco FDM
- D. CDO

Answer: B

NEW QUESTION 289

- (Exam Topic 3)

An administrator needs to configure the Cisco ASA via ASDM such that the network management system can actively monitor the host using SNMPv3. Which two tasks must be performed for this configuration? (Choose two.)

- A. Specify the SNMP manager and UDP port.
- B. Specify an SNMP user group
- C. Specify a community string.
- D. Add an SNMP USM entry
- E. Add an SNMP host access entry

Answer: BE

NEW QUESTION 292

- (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 293

- (Exam Topic 3)

What are two security benefits of an MDM deployment? (Choose two.)

- A. robust security policy enforcement
- B. privacy control checks
- C. on-device content management
- D. distributed software upgrade
- E. distributed dashboard

Answer: AC

NEW QUESTION 294

- (Exam Topic 3)
 What is the most commonly used protocol for network telemetry?

- A. SMTP
- B. SNMP
- C. TFTP
- D. NctFlow

Answer: D

NEW QUESTION 298

- (Exam Topic 3)
 Which security solution protects users leveraging DNS-layer security?

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

Answer: C

NEW QUESTION 300

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

Cisco AnyConnect client	location-independent, bandwidth-efficient option
ISR with CWS connector	extends identity information and on-premises features to the cloud
NGFW with CWS connector	provides user-group granularity and supports cloud-based scanning
WSAv with CWS connector	supports cached credentials and makes directory information available off-premises

- 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 305

- (Exam Topic 3)
 A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to ensure that bandwidth is available for VPN users needing access to corporate resources on the 10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the network?

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

Answer: A

NEW QUESTION 307

- (Exam Topic 3)
 A university policy must allow open access to resources on the Internet for research, but internal workstations are exposed to malware. Which Cisco AMP feature allows the engineering team to determine whether a file is installed on a selected few workstations?

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

Answer: A

NEW QUESTION 309

- (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 311

- (Exam Topic 3)

Based on the NIST 800-145 guide, which cloud architecture is provisioned for exclusive use by a specific group of consumers from different organizations and may be owned, managed, and operated by one or more of those organizations?

- A. hybrid cloud
- B. private cloud
- C. community cloud
- D. public cloud

Answer: C

NEW QUESTION 312

- (Exam Topic 3)

What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?

- A. Telemetry uses a pull method, 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

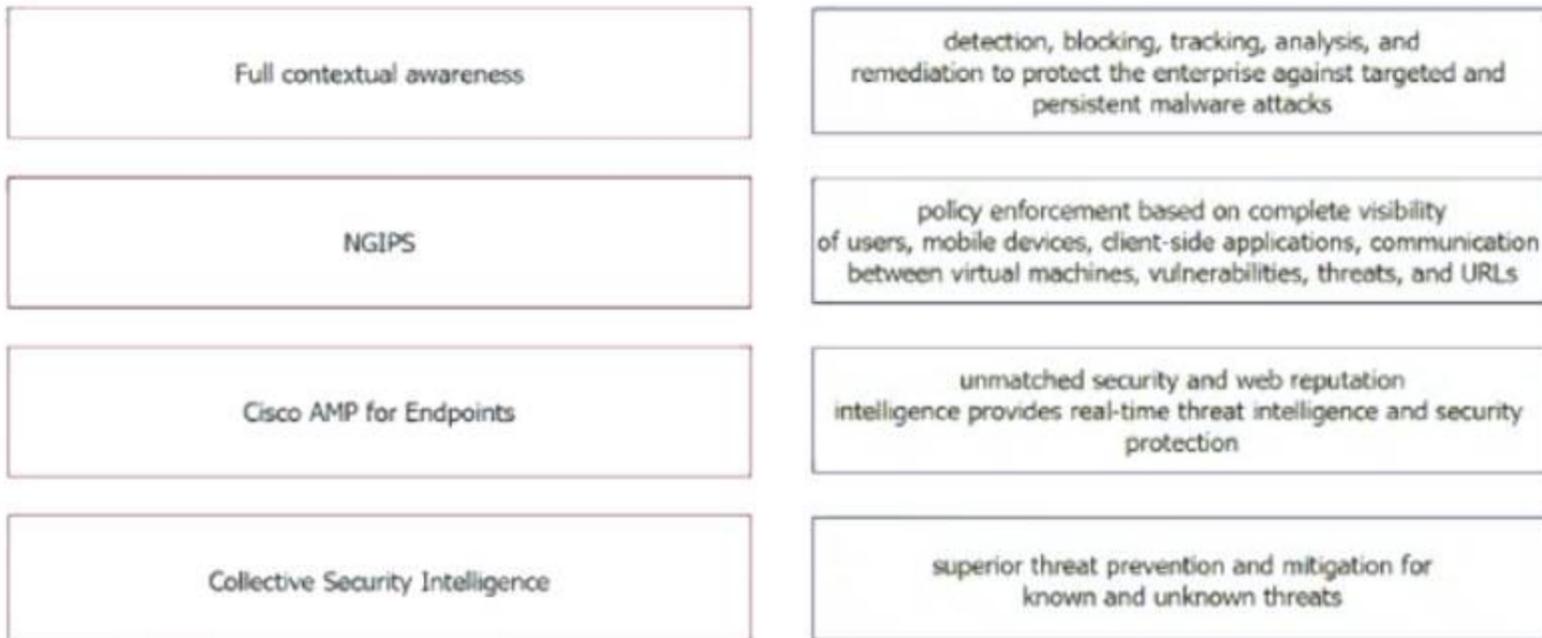
Explanation:

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

NEW QUESTION 317

- (Exam Topic 3)

Drag and drop the security solutions from the left onto the benefits they provide on the right.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Diagram Description automatically generated

NEW QUESTION 319

- (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 320

- (Exam Topic 3)

Which technology provides the benefit of Layer 3 through Layer 7 innovative deep packet inspection, enabling the platform to identify and output various applications within the network traffic flows?

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

Answer: A

NEW QUESTION 322

- (Exam Topic 3)

An engineer is implementing Cisco CES in an existing Microsoft Office 365 environment and must route inbound email to Cisco CE.. record must be modified to accomplish this task?

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

Answer: B

NEW QUESTION 326

- (Exam Topic 3)

When a Cisco WSA checks a web request, what occurs if it is unable to match a user-defined policy?

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

Answer: B

NEW QUESTION 328

- (Exam Topic 3)

Which Cisco network security device supports contextual awareness?

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

Answer: D

NEW QUESTION 330

- (Exam Topic 3)

An engineer is adding a Cisco router to an existing environment. NTP authentication is configured on all devices in the environment with the command `ntp authentication-key 1 md5 Clsc427128380`. There are two routers on the network that are configured as NTP servers for redundancy, 192.168.1.110 and 192.168.1.111. 192.168.1.110 is configured as the authoritative time source. What command must be configured on the new router to use 192.168.1.110 as its primary time source without the new router attempting to offer time to existing devices?

- A. `ntp server 192.168.1.110 primary key 1`
- B. `ntp peer 192.168.1.110 prefer key 1`
- C. `ntp server 192.168.1.110 key 1 prefer`
- D. `ntp peer 192.168.1.110 key 1 primary`

Answer: A

NEW QUESTION 332

- (Exam Topic 3)

Which Cisco Umbrella package supports selective proxy for Inspection of traffic from risky domains?

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

Answer: C

NEW QUESTION 333

- (Exam Topic 3)

Which encryption algorithm provides highly secure VPN communications?

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

Answer: B

NEW QUESTION 337

- (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 342

- (Exam Topic 3)

An organization has a requirement to collect full metadata information about the traffic going through their AWS cloud services They want to use this information for behavior analytics and statistics Which two actions must be taken to implement this requirement? (Choose two.)

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

Answer: BE

NEW QUESTION 347

- (Exam Topic 3)

Why is it important to have a patching strategy for endpoints?

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

Answer: C

NEW QUESTION 349

- (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 354

- (Exam Topic 3)

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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 356

- (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 358

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 363

- (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, and enable 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 367

- (Exam Topic 3)

Which CLI command is used to enable URL filtering support for shortened URLs on the Cisco ESA?

- A. webadvancedconfig
- B. websecurity advancedconfig
- C. outbreakconfig
- D. websecurity config

Answer: B

NEW QUESTION 368

- (Exam Topic 3)

What is an advantage of network telemetry over SNMP pulls?

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

Answer: D

NEW QUESTION 370

- (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 373

- (Exam Topic 3)

How does Cisco AMP for Endpoints provide next-generation protection?

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

Answer: B

NEW QUESTION 376

- (Exam Topic 3)

How does Cisco Umbrella protect clients when they operate outside of the corporate network?

- A. by modifying the registry for DNS lookups
- B. by using Active Directory group policies to enforce Cisco Umbrella DNS servers
- C. by using the Cisco Umbrella roaming client
- D. by forcing DNS queries to the corporate name servers

Answer: C

NEW QUESTION 379

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 384

- (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 385

- (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 389

- (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 394

- (Exam Topic 3)

Which security product enables administrators to deploy Kubernetes clusters in air-gapped sites without needing Internet access?

- A. Cisco Content Platform
- B. Cisco Container Controller

NEW QUESTION 407

- (Exam Topic 2)

Which type of dashboard does Cisco DNA Center provide for complete control of the network?

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

Answer: B

Explanation:

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

NEW QUESTION 410

- (Exam Topic 2)

When planning a VPN deployment, for which reason does an engineer opt for an active/active FlexVPN configuration as opposed to DMVPN?

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

Answer: B

NEW QUESTION 413

- (Exam Topic 2)

Drag and drop the common security threats from the left onto the definitions on the right.

phishing	a software program that copies itself from one computer to another, without human interaction
botnet	unwanted messages in an email inbox
spam	group of computers connected to the Internet that have been compromised by a hacker using a virus or Trojan horse
worm	fraudulent attempts by cyber criminals to obtain private information

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A picture containing application Description automatically generated

NEW QUESTION 418

- (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 419

- (Exam Topic 2)

Which type of API is being used when a security application notifies a controller within a software-defined network architecture about a specific security threat?

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

Answer: C

NEW QUESTION 421

- (Exam Topic 2)

What is the role of Cisco Umbrella Roaming when it is installed on an endpoint?

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

Answer: B

Explanation:

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

NEW QUESTION 423

- (Exam Topic 2)

What are two characteristics of Cisco DNA Center APIs? (Choose two)

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

Answer: DE

NEW QUESTION 425

- (Exam Topic 2)

Which type of protection encrypts RSA keys when they are exported and imported?

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

Answer: B

NEW QUESTION 429

- (Exam Topic 2)

What is the purpose of the certificate signing request when adding a new certificate for a server?

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

Answer: B

Explanation:

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

NEW QUESTION 431

- (Exam Topic 2)

Refer to the exhibit.

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

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

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

Answer: D

Explanation:

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

DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized

DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle". The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response. DHCP snooping can prevent DHCP spoofing attacks. DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.

Only ports that connect to an authorized DHCP server are trusted, and allowed to send all types of DHCP messages. All other ports on the switch are untrusted and can send only DHCP requests. If a DHCP response is seen on an untrusted port, the port is shut down.

The port connected to a DHCP server should be configured as trusted port with the "ip dhcp snooping trust" command. Other ports connecting to hosts are untrusted ports by default.

In this question, we need to configure the uplink to "trust" (under interface Gi1/0/1) as shown below.

NEW QUESTION 434

- (Exam Topic 2)

An organization is implementing URL blocking using Cisco Umbrella. The users are able to go to some sites but other sites are not accessible due to an error. Why is the error occurring?

- A. Client computers do not have the Cisco Umbrella Root CA certificate installed.
- B. IP-Layer Enforcement is not configured.
- C. Client computers do not have an SSL certificate deployed from an internal CA server.
- D. Intelligent proxy and SSL decryption is disabled in the policy

Answer: A

Explanation:

Reference: <https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information>

NEW QUESTION 437

- (Exam Topic 2)

Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks	Cisco Firepower
provides superior threat prevention and mitigation for known and unknown threats	
provides outbreak control through custom detections	
provides the root cause of a threat based on the indicators of compromise seen	Cisco AMP
provides the ability to perform network discovery	
provides intrusion prevention before malware compromises the host	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Application Description automatically generated with low confidence explanation The Firepower System uses network discovery and identity policies to collect host, application, and user data for traffic on your network. You can use certain types of discovery and identity data to build a comprehensive map of your network assets, perform forensic analysis, behavioral profiling, access control, and mitigate and respond to the vulnerabilities and exploits to which your organization is susceptible. The Cisco Advanced Malware Protection (AMP) solution enables you to detect and block malware, continuously analyze for malware, and get retrospective alerts. AMP for Networks delivers network-based advanced malware protection that goes beyond point-in-time detection to protect your organization across the entire attack continuum – before, during, and after an attack. Designed for Cisco Firepower® network threat appliances, AMP for Networks detects, blocks, tracks, and contains malware threats across multiple threat vectors within a single system. It also provides the visibility and control necessary to protect your organization against highly sophisticated, targeted, zero-day, and persistent advanced malware threats.

NEW QUESTION 439

- (Exam Topic 2)

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

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

D. The policy was created to disable file analysis

Answer: D

Explanation:

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

NEW QUESTION 444

- (Exam Topic 2)

Refer to the exhibit.

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

What will happen when the Python script is executed?

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

Answer: C

NEW QUESTION 449

- (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 452

- (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 457

- (Exam Topic 2)

Drag and drop the VPN functions from the left onto the description on the right.

RSA	ensures data integrity
AES	defines IKE SAs
SHA-1	ensures data confidentiality
ISAKMP	provides authentication

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 461

- (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 463

- (Exam Topic 2)

Which algorithm provides asymmetric encryption?

- A. RC4
- B. AES
- C. RSA
- D. 3DES

Answer: C

NEW QUESTION 467

- (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 470

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

350-701 Practice Exam Features:

- * 350-701 Questions and Answers Updated Frequently
- * 350-701 Practice Questions Verified by Expert Senior Certified Staff
- * 350-701 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 350-701 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 350-701 Practice Test Here](#)