Q1

What is the difference a vulnerability and an exploit?

A. A vulnerability is a weakness that can be exploited by an attacker.

B. An exploit is a weakness that can cause a vulnerability in the network

C. An exploit is a hypothetical event that causes a vulnerability in the network

D. A vulnerability is a hypothetical event for an attacker to exploit.

Answer: C

Q2

What must be enabled to secure SaaS-based applications?

A. modular policy framework

B. two-factor authentication

C. application security gateway

D. end-to-end encryption

Answer: C

Q3

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 ISE

B. Cisco Tetration

C. Cisco AnyConnect

D. Cisco AMP for Network

Answer: B

Q4

Which attribute has the ability to change during the RADIUS CoA?

A. authorization

B. accessibility

C. membership

D. NTP

Answer: A

Q5

An organization wants to improve its cybersecurity processes and to add intelligence to its data The organization wants to utilize the most current intelligence data for URL filtering reputations and vulnerability information that can be integrated with the Cisco FTD and Cisco WSA What must be done to

accomplish these objectives'?

A. Download the threat intelligence feed from the IETF and import it into the Cisco FTD and Cisco WSA databases

B. Configure the integrations with Talos Intelligence to take advantage of the threat intelligence that it provides

C. Create an automated download of the Internet Storm Center intelligence feed into the Cisco FTD and Cisco WSA databases to the to the dynamic access

control policies.

D. Create a Cisco pxGrid connection to NIST to import this information into the security products for policy use

Answer: B

Q6

An engineer configures new features within the Cisco Umbrella dashboard and wants to identify and proxy traffic that is categorized as risky domains and may contain safe and malicious content Which action accomplishes these objectives?

A. Create a new site within Cisco Umbrella to block requests from those categories so they can be sent to the proxy device

B. Upload the threat intelligence database to Cisco Umbrella for the most current information on reputations and to have the destination lists block them

C. Configure intelligent proxy within Cisco Umbrella to intercept and proxy the requests for only those categories

D. Configure URL filtering within Cisco Umbrella to track the URLs and proxy the requests for those categories and below.

Answer:C

Q7

An engineer is trying to decide between using L2TP or GRE over IPsec for their sit-to-sit VPN implementation. What must be understood before choosing a

solution?

A. GRE over IPsec adds its own header, and L2TP does not.

B. L2TP is an IP packet encapsulation protocol and GRE over IPsec is a tunneling protocol

C. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701.

D. GRE over IPsec cannot be used as a standalone protocol and L2TP can

Answer: D

Q8

What is an advantage of network telemetry over SNMP pulls'?

A. scalability

B. encapsulation

C. accuracy

D. security

Answer: A

Q9

What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two)

A. Deploy a separate eDirectory server the client IP address is recorded in this server.

B. Deploy a separate Active Directory agent such as Cisco Context Directory Agent

C. The eDirectory client must be installed on each client workstation

D. Create NTLM or Kerberos authentication realm and enable transparent user identification

E. Create an LDAP authentication realm and disable transparent user identification

Answer: BD

Q10

What are two advantages of using Cisco AnyConnect over DMVPN? (Choose two)

A. It allows multiple sites to connect to the data center

B. It allows different routing protocols to work over the tunnel.

C. It enables VPN access for individual users from their machines

D. It provides spoke-to-spoke communications without traversing the hub.

E. It allows customization of access policies based on user identity

Answer: CE

Q11

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. Seed IP

C. Cisco Prime Infrastructure

D. CDP Auto Discovery

E. Power On Auto Provisioning

Answer: BE

Q12

Which role is a default guest type in Cisco ISE?

A. Yearly

B. Monthly

C. Contractor

D. Full-Time

Answer: C

Q13

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 GigabitEthernetO/1 as promiscuous port GigabitEthenetO/2 as

community port and GigabitEthernetO/3 and GigabitEthernetO/4 as isolated

ports.

B. Configure GigabitEthernetO/1 as community port. GigabitEthermnetO/2 as

isolated port, and GigabitEthernetO/3 and GigabitEthernetO/4 as promiscuous ports

C. Configure GigabitEthernetO/1 as community port GigabitEthemetO/2 as

promiscuous port GigabitEtheretO/3 and GigabitEthernetO/4 as isolated ports

D. Configure GigabitEthernetO/1 as promiscuous port GigabitEthemetO/2 as

isolated port and GigabitEtheretO/3 and GigabitEthernetO/4 as community ports

Answer: D

Q14

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

A. Cisco Container Platform

B. Cisco Content Platform

C. Cisco Cloud Platform

O. Cisco Container Controller

Answer: A

Q15

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. Manually change the management port on Cisco FMC and all managed Cisco FTD devices

C. Set the sftunnel port to 8305.

D. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices

Answer:B

Q16

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. 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.

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. Use the track movement option within the authorization profile for the

authorization policy line that the unauthenticated devices hit

Answer: B

Q17

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

A. If four log in attempts fail in 100 seconds wait for 60 seconds to next log in prompt

B. After four unsuccessful log in attempts the line is blocked for 100 seconds and only permit IP addresses are permitted in ACL 60

C. After four unsuccessful log in attempts the line is blocked for 60 seconds and only permit IP addresses are permitted in ACL 100

D. If four failures occur in 60 seconds the router goes to quiet mode for 100 seconds

Answer: D

Q18

Refer to the exhibit. Which configuration item makes it possible to have the session on the network?

A. aaa authorization network default ise

B. aaa authentication login console ise

C. aaa authentication enable default enable

D. aaa authorization exec default ise

Answer: A

Q19

Which feature is leveraged by advanced antimalware capabilities to be an effective endpoint protection platform?

A. sandboxing

B. big data

C. blocklisting

D. storm centers

Answer: A

Q20

How does Cisco Workload Optimization Manager help mitigate application performance issues'?

A. It automates resource resizing

B. It sets up a workload forensic score

C. It optimizes a flow path.

D. It deploys an AWS Lambda system.

Answer: A

Q21

A network engineer has entered the snrnp-server user andy myv3 auth sha cisco priv aes 256 ciscoxxxxxxxx command and needs to send SNMP information to a host at 10255 254 1. Which command achieves this goal?

A. snmp-server host inside 10.255.254.1 snmpv3 andy

B. snrnp-server hotst inside10.255.254.1 version3 andy

C. snmp-server host inside 10.255.254.1 snmpv3 myv3

D. snmp-server host inside 10.255.254.1 version 3 myva

Answer: B

Q22

What are two functionalities of SDN Northbound APIs'? (Choose two)

A. OpenFlow is a standardized northbound API protocol.

B. Northbound APIs form the interface between the SDN controller and the network switches or routers

C. Northbound APIs provide a programmable interface for applications to dynamically configure the network

D. Northbound APIs form the interface between the SDN controller and business applications

E. Northbound APIs use the NETCONF protocol to communicate with applications

Answer: CD

Q23

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 APK must be uploaded for the application that the detection is intended.

B. The MD5 hash uploaded to the simple detection policy is in the incorrect format

C. The administrator must upload the file instead of the hash for Cisco AMP to use

D. Detections for MD5 signatures must be configured in the advanced custom detection policies

Answer: D

Q24

What is the intent of a basic SYN flood attack?

A. to cause the buffer to overflow

B. to exceed the threshold limit of the connection queue

C. to solicit DNS responses

D.to flush the register stack to re-initiate the buffers

Answer: B

Q25

Refer to the exhibit An engineer is implementing a certificate based VPN What is the result of the existing configuration'?

A. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER.

B. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.

C. The OU of the IKEv2 peer certificate is set to MANGLER.

D. Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully.

Answer: B

Q26

An administrator enables Cisco Threat Intelligence Director on a Cisco FMC Which process uses STIX and allows uploads and downloads of block lists?

A. consumption

B. sharing

C. editing

D. authoring

Answer: A

Q27

Which component of Cisco Umbrella architecture increases reliability of the service'?

A. Cisco Talos

B. BGP route reflector

C. anycast IP

D. AMP Threat Grid

Answer: A

Q28

What is a difference between Cisco AMP for Endpoints and Cisco Umbrella'?

A. Cisco AMP for Endpoints presents detects and responds to attacks before damage can be done and Cisco Umbrella provides the first line of defense against Internet threats

B. Cisco AMP for Endpoints automatically researches indicators of compromise and confirms threats and Cisco Umbrella does not

C. Cisco AMP for Endpoints is a cloud-based service, and Cisco Umbrella is not.

D. Cisco AMP for Endpoints prevents connections to malicious destinations, and Cisco Umbrella works at the file level to prevent the initial execution of malware

Answer: A

Q29

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

A.It authenticates to a Cisco ISE with an SSH connection

B. It allows authentication with TLSvl SSL protocol

C. It authenticates to a Cisco ISE server using the username of ersad

D. It lists the LDAP users from the external identity store configured on Cisco ISE.

Answer: C

Q30

Refer to the exhibit A Cisco ISE administrator adds a new switch to an G02 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 printers and video cameras cannot Based on the interface configuration provided what must be done to get these devices onto the network using Cisco ISE for authentication and authorization while maintaining security controls?

A. Add mab to the interface configuration

B. Change the default policy in Cisco ISE to allow all devices not using machine authentication

C. Configure authentication event fail retry 2 action authorize vlan 41 on the interface

D. Enable insecure protocols within Cisco ISE in the allowed protocols configuration

Answer: A

Q31

What is the benefit of integrating Cisco ISE with a MDM solution?

A. It provides the ability to update other applications on the mobile device.

B. It provides network device administration access.

C. It provides the ability to add applications to the mobile device through Cisco ISE.

D. It provides compliance checks for access to the network.

Answer: D

Q32

A company discovered an attack propagating through their network via a file A custom file detection policy was created in order to track this in the future and ensure no other endpoints execute the infected file In addition it was discovered during testing that the scans are not detecting the file as an indicator of

compromise What must be done in order to ensure that the policy created is functioning as it should'?

A. Send the file to Cisco Threat Grid for dynamic analysis

B. Upload the hash for the file into the policy.

C. Create an IP block list for the website from which the file was downloaded

D. Block the application that the file was using to open

Answer: A

Q33

An engineer must modify a policy to block specific addresses using Cisco Umbrella The policy is created already and is actively used by devices using many of the default policy elements What else must be done to accomplish this task?

A. Use content categories to block or allow specific addresses

B. Add the specified addresses to the identities list and create a block action

C. Create a destination list for addresses to be allowed or blocked

D. Modify the application settings to allow only applications to connect to required addresses

Answer: C

Q34

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. Map sender IP addresses to a host interface

B. B Provision the email appliance

C. Deploy an encryption appliance.

D. Enable flagged message handling

Answer: D

Q35

What is a benefit of performing device compliance'?

A. device classification and authorization

B. providing attribute-driven policies

C. verification of the latest OS patches

D. providing multi-factor authentication

Answer: B

Q36

What is a description of microsegmentation?

A. Environments apply a zero-trust model and specify how applications on different servers or containers can communicate

B. Environments deploy a container orchestration platform such as Kubernetes to manage the application delivery.

C. Environments deploy centrally managed host-based firewall rules on each server or container

D. Environments implement private VLAN segmentation to group servers with similar applications

Answer: A

Q37

A network engineer must configure a Cisco ESA to prompt users to enter two forms of information before gaining access The Cisco ESA must also join a cluster machine using preshared keys What must be configured to meet these requirements'?

A. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA GUI

B. B Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA GUI

C. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA CLI.

D. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA CLI.

Answer: C

Q38

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. Modify the current policy with the condition MFA Source Sequence. DUO=true in the authorization conditions within Cisco ISE.

B. Create an identity policy within Cisco ISE to send all authentication requests to Cisco DUO.

C. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE

D. Configure Cisco DUO with the external Active Directory connector and tie it to the policy set within Cisco ISE

Answer: C

Q39

What are two functionalities of northbound and southbound APIs within Cisco SDN architecture?(Choose two)

A. Southbound APIs are used to define how SDN controllers Integrate with applications.

B. Northbound APIs utilize RESTful API methods such as GET POST, and DELETE

C. Southbound interfaces utilize device configurations such as VLANs and IP addresses.

D. Northbound interfaces utilize OpenFlow and OpFlex to integrate with network devices

E. Southbound APIs utilize CLI. SNMP, and RESTCONF

Answer: BE

Q40

What is the function of the crypto isakmp key cisc address 192 168 50 1 255 255 255 255 command when establishing an IPsec VPN tunnel?

A. It configures the local address for the VPN server 192 168 50 1

B. It prevents 192 168 50 1 from connecting to the VPN server

C. It configures the pre-shared authentication key for host 192 168 50 1

D. It defines that data destined to 192 168 50 1 is going to be encrypted

Answer: C

Q41

Which Cisco DNA Center Intent API action is used to retrieve the number of devices known to a DMA Center?

A. GET https://fqdnOrlPofDnaCenterPlatform/dna/intent/api/v1/network-device

B.GEThttps://fqdnOrlPofDnaCenterPlatform/dna/intent'api/v1/network-device?parameter1=value&parameter2=value&

C. GET https://fqdnOrlPofDnaCenterPlatform'dna/intentapi'VI- network-devicelcount

D.GET https://fqdnOrlPofDnaCenterPlatform;dna/intent/api/v1;network-device/startindexlrecordsToRetum

Answer: C

Q42

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 WSAv

C. Cisco Stealthwatch Cloud

D. Cisco ASAv

Answer: D

Q43

Which technology enables integration between Cisco ISE and Other platforms to gather and share network and vulnerability data and SIEM and location information?

A. SNMP

B. NetFlow

C. Cisco Talos

B. pxGrid

Answer: D

Q44

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. allow

B. block

C. monitor

D. trust

Answer: A

Q45

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 a community string.

B. Add an SNMP host access entry

C. Specify the SNMP manager and UDP port.

D. Specify an SNMP user group

E. Add an SNMP USM entry.

Answer: BD

Q46

Which function is performed by certificate authorities but is a limitation of registration authorities'?

A. certificate re-enrollment

B. verifying user identity

C. CRL publishing

D. accepts enrollment requests

Answer: C

Q47

Which Cisco ASA Platform mode disables the threat detection features except for Advanced Threat Statistics?

A. multiple context

B. routed

C. cluster

D. transparent

Answer: A

Q48

When NetFlow is applied to an interface which component creates the flow monitor cache that is used to collect traffic based on the key and nonkey fields in the configured record'?

A. records

B. flow exporter

C. flow monitor

D. flow sampler

Answer: A

Q49

What is a feature of NetFlow Secure Event Logging?

A. It delivers data records to NSEL collectors through NetFlow over TCP only

B. It exports only records that indicate significant events in a flow.

C. It filters NSEL events based on the traffic and event type through RSVP

D. It supports v5 and v8 templates

Answer: B

Q50

An engineer is configuring Cisco WSA and needs to enable a separated email transfer flow from the Internet and from the LAN Which deployment mode must be used to accomplish this goal'?

A. multi-context

B. Transparent

C. Two-Interface

D. single Interface

Answer: C

Q51

Which encryption algorithm provides highly secure VPN communications

A. AES 256

B. DES

C. AES 128

D. 3DES

Answer: A

Q52

Which Cisco security solution stops exfiltration using HTTPS

A. Cisco ASA

B. Cisco CTA

C. Cisco FTD

D. Cisco AnyConnect

Answer: B

Q53

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. compile-time instrumentation

C. cloud application security broker

D. container orchestration

Answer: A

Q54

A hacker initiated a social engineering attack and stole username and passwords of some users within a company Which product should be used as a solution to this problem?

A. Cisco AMP for Endpoints

B. Cisco NGFW

C. Cisco Any Connect

D. Cisco Duo

Answer: D

Q55

Which RADIUS feature provides a mechanism to change the AAA attributes of a session after it is authenticated'?

A. Authentication

B. Authorization

C. CoA

D. Accounting

Answer: C

Q56

Why is it important for the organization to have an endpoint patching strategy?

A. so the network administrator is no fed when an existing bug is encountered

B. so the latest security fixes are installed on the endpoints

C. so the organization can identify endpoint vulnerabilities

D. so the in ternal PSIRT organization is aware of the latest bugs

Answer: B

Q57

Which two parameters are used to prevent a data breach in the cloud? (Choose two.)

A. strong user authentication

B. antispoofing programs

C. encryption

D. complex cloud-based web proxies

E. DLP solutions

Answer: CE

Q58

Which benefit does DMVPN provide over GETVPN?

A. DMVPN is a tunnel-less VPN and GET VPN is tunnel-based

B. DMVPN supports QoS. multicast and routing and GETVPN supports only QoS.

C. DMVPN supports non-IP protocols and GETVPN supports only IP protocols

D. DMVPN can be used over the public Internet and GET VPN requires a private network

Answer: D

Q59

There are individual sites specified to be block listed in Cisco Umbrella'?

A. destination lists

B. application settings

C. security settings

D. content categories

Answer: A

Q60

What is the primary deference between an Endpoint Protection Platform and an Endpoint Detection and Response?

A. EPP focuses on network security, and EDR focuses on device security.

B. EPP focuses on prevention and EDR focuses on advanced threats that evade perimeter defenses

C. EDR focuses on network security, and EPP focuses on device security.

D. EDR focuses on prevention and EPP focuses on advanced threats that evade perimeter defenses.

Answer: B

Q61

Which SNMPv3 configuration must be used to support the strongest security possible?

A. asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXX asa-host (config) #snmp-server host inside 10 255.254 1 version 3 andy

B. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXX asa-host(config)#snmp-sen/er host inside 10 255 254 1 version 3 andy

C. asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 266 ciscXXXXX asa-host(config)#snmp-server host inside 10 255 254 1 version 3 andy

D. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXX asa-host(config)#snmp-server host inside 10 255 254 1 version 3 andy

Answer: D

Q62

What must be integrated with Cisco Threat Intelligence Director to provide information about security threats which allows the SOC to proactively automate responses to those threats'?

A. External Threat Feeds

B. Cisco Stealthwatch

C. Cisco Umbrella

D. Cisco Threat Grid

Answer: D

Q63

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

Q64

Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System (Choose two)

A. inline normalization

B. SIP

C. Modbus

D. SSL

E. packet decoder

Answer: BD

Q65

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. Add the public IP address that the client computers are behind to a Core identity

B. Enable the Intelligent Proxy to validate that traffic is being routed correctly

C. Ensure that the client computers are pointing to the on-premises DNS servers.

D. Browse to http welcome umbrella com; to validate that the new identity is working

Answer: B

Q66

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

A. MX

B. SPF

C. DKIM

D. CNAME

Answer: A

Q67

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. Make the correct policy first in the policy order

B. Place the policy with the most-specific configuration last in the policy order

C. Configure the default policy to redirect the requests to the correct policy.

D. Configure only the policy with the most recently changed timestamp

Answer: A

Q68

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

A. Cisco DNA Center

B. Cisco Umbrella

C. Cisco Duo Security

D. Cisco ISE

E. Cisco TrustSec

Answer: BC

Q69

What are two functions of TAXII in threat intelligence sharing?(Choose two)

A. exchanges trusted anomaly intelligence information

B. determines how threat intelligence information is relayed

C. allows users to describe threat motivations and abilities

D. determines the "what" of threat intelligence

E. supports STIX information

Answer: AB

Q70

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 file instead of a hash.

B. The hash being uploaded is part of a set in an incorrect format

C. The file being uploaded is incompatible with simple detections and must use advanced detections

D. The engineer is attempting to upload a hash created using MD5 instead of SHA-256.

Answer: D

Q71

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 the device sensor feature within the switch to send the appropriate protocol information

D. Configure a service template within the switch to standardize the port configurations so that the correct information is sent to Cisco ISE.

Answer: C

Q72

An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems. Why should the

organization select either Platform as a Service or Infrastructure as a Service for this environment'?

A. Infrastructure as a Service because the service provider manages the operating system

B. Platform as a Service because the customer manages the operating system

C. Platform as a Service because the service provider manages the operating system

D. Infrastructure as a Service because the customer manages the operating system

Answer: C

Q73

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

A. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA

B. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA

C. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not.

D. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA

Answer: D

Q74

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 FQDW?

A. Add the DNS entry for the new Cisco ISE node into the DNS server

B. Change the IP address of the new Cisco ISE node to the same network as the others.

C. Make the new Cisco ISE node a secondary PAN before registering it with the primary.

D. Open port 8905 on the firewall between the Cisco ISE nodes

Answer: A

Q75

Which portion of the network do EPP solutions solely focus on and EDR solutions do not?

A. perimeter

B. core

C. East-West gateways

D. server farm

Answer: A

Q76

What is a benefit of using a multifactor authentication strategy'?

A. It protects data by enabling the use of a second validation of identity

B. It provides secure remote access for applications

C. It provides visibility into devices to establish device trust

D. It provides an easy, single sign-on experience against multiple applications

Answer: A

Q77

How does a cloud access security broker function?

A. It scans other cloud solutions being used within the network and identifies vulnerabilities

B. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution

C. It acts as a security information and event management solution and receives syslog from other cloud solutions.

D. It is an authentication broker to enable single sign-on and multi-factor authentication for a cloud solution

Answer: B

Q78

How is data sent out to the attacker during a DNS tunneling attack'?

A. as part of the domain name

B. as part of the TCP/53 packet header

C. as part of the UDP/53 packet payload

D. as part of the DNS response packet

Answer: C

Q79

Which method of attack is used by a hacker to send malicious code through a web application to an unsuspecting user to request that the victims web browser executes the code'?

A. cross-site scripting

B. SQL injection

C.browser WGET

D. buffer overflow

Answer: A

Q80

Which posture assessment requirement provides options to the client for remediation and requires the remediation within a certain timeframe'?

A. visibility

B. audit

C. optional

D. mandatory

Answer: D

Q81

An organization wants to use Cisco FTD or Cisco ASA devices Specific URLs must be blocked from being accessed via the firewall which requires that the administrator input the bad URL categories that the organization wants blocked into the access policy. Which solution should be used to meet this requirement?

A. Cisco ASA because it enables URL filtering and blocks malicious URLS by default whereas Cisco FTD does not

B. Cisco FTD because it enables URL filtering and blocks malicious URLs by default whereas Cisco ASA does not.

C. Cisco FTD because it includes URL filtering in the access control policy capabilities whereas Cisco ASA does not

D. Cisco ASA because it includes URL filtering in the access control policy capabilities whereas Cisco FTD does not

Answer: C

Q82

Refer to the exhibit What is the function of the Python script code snippet for the cisco

A. obtains the saved configuration of the Cisco ASA firewall

B. adds a global rule into policies

C. changes the hostname of the Cisco ASA

D. deletes a global rule from policies

Answer: B

Q83

Which endpoint solution protects a user from a phishing attack'?

A. Cisco Identity Services Engine

B. Cisco AnyConnect with Network Access Manager module

C. Cisco AnyConnect with Umbrella Roaming Security module

D. Cisco AnyConnect with ISE Posture module

Answer: C

Q84

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

Q84

Refer to the exhibit When configuring a remote access VPN solution terminating on the Cisco ASA an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication using machine certificates Which configuration item must be modified to allow this?

A. SAUL Server

B. Group Policy

C. AAA Server Group

D. Method

Answer: D

Q86

A network engineer must migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vfvlotion What is a requirement for both physical hosts?

A. The hosts must use a different datastore than the virtual appliance.

B. The hosts must run Cisco AsyncOS 10 0 or greater

C. The hosts must have access to the same defined network

D. The hosts must run different versions of Cisco AsyncOS.

Answer: C

Q87

An organization configures Cisco Umbrella to be used for its DNS services The organization must be able to block traffic based on the subnet that the endpoint is on but it sees only the requests from its public IP address instead of each internal IP address What must be done to resolve this issue?

A. Install the Microsoft Active Directory Connector to give IP address information stitched to the requests in the Cisco Umbrella dashboard.

B. Use the tenant control features to identify each subnet being used and track the connections within the Cisco Umbrella dashboard

C. Configure an internal domain within Cisco Umbrella to help identify each address and create policy from the domains

D. Set up a Cisco Umbrella virtual appliance to internally field the requests and see the traffic of each IP address

Answer: D

Q88

Which kind of API that is used with Cisco DMA Center provisions SSIDs QoS policies and update software versions on switches?

A. event

B. intent

C. multivendor

D. integration

Answer: B

Q89

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'5 (Choose two.)

A. Configure Cisco Stealthwatch Cloud to ingest AWS information.

B. Send VPC Flow Logs to Cisco Stealthwatch Cloud

C. Send syslog from AWS to Cisco Stealthwatch Cloud

D. Configure Cisco ACI to ingest AWS information

E. Configure Cisco Thousand Eyes to ingest AWS information.

Answer: BD

Q90

A network engineer must monitor user and device behavior within the on-premises network This data must be sent to the Cisco Stealthwatch Cloud analytics platform for analysis What must be done to meet this requirement, using the Ubuntu-based VM appliance deployed in a VMware-based hypervisor'?

A. Deploy the Cisco Stealthwatch Cloud PNM sensor that sends data to Cisco Stealthwatch Cloud

B. Configure a Cisco FMC to send NetFlow to Cisco Stealthwatch Cloud

C. Deploy a Cisco FTD sensor to send network events to Cisco Stealthwatch Cloud

D. Configure a Cisco FMC to send syslogs to Cisco Stealthwatch Cloud

Answer: A

Q91

Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container"?

A. SDLC

B. Lambda

C. Docker

D. Contiv

Answer: D

Q92

An administrator is adding a new switch onto the network and has configured AAA for network access control When testing the configuration the RADIUS authenticates to Cisco ISE but is being rejected Why is the ip radius source-interface command needed for this configuration?

A. The RADIUS authentication key is transmitted only from the defined RADIUS source interface.

B. Encrypted RADIUS authentication requires the RADIUS source interface be defined

C. RADIUS requests are generated only by a router if a RADIUS source interface is defined.

D. Only requests that originate from a configured NAS IP are accepted by a RADIUS server

Answer: D

Q93

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

A. OpenC2

B. STIX

C. OpenlOC

D. CybOX

Answer: C

Q94

An organization wants to implement a cloud-delivered and SaaS based solution to provide visibility and threat detection across the AWS network The solution must be deployed without software agents and rely on AWS VPC flow logs instead Which solution meets these requirements'?

A. Cisco Stealthwatch Cloud

B. Cisco Umbrella

C. Cisco Cloudlock

D. NetFlow collectors

Answer: A

Q95

An organization has a Cisco Stealthwatch Cloud deployment in their environment Cloud logging is working as expected but logs are not being received from the on-premise network What action will resolve this issue?

A. Configure security appliances to send NetFlow to Cisco Stealthwatch Cloud.

B. Deploy a Cisco Stealthwatch Cloud sensor on the network to send data to Cisco Stealthwatch Cloud

C. Deploy a Cisco FTD sensor to send events to Cisco Stealthwatch Cloud

D. Configure security appliances to send svslogs to Cisco Stealthwatch Cloud.

Answer: B

Q96

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

A. The module fails to receive redirected traffic

B. Traffic continues to flow if the module fails

C. Traffic is blocked if the module fails

D. The module is operating in IDS mode

E. The module is operating in IPS mode

Answer: BD

Q97

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 enables interactive blocking and blocking with reset natively whereas Cisco ASA does not

B. Cisco FTD because it supports system rate level traffic blocking whereas Cisco ASA does not

C. Cisco ASA because it allows for interactive blocking and blocking with reset to be configured via the GUI. whereas Cisco FTD does not

D. Cisco ASA because it has an additional module that can be installed to provide multiple blocking capabilities, whereas Cisco FTD does not.

Answer: A

Q98

Which security solution uses NetFlow to provide visibility across the network data center branch offices and cloud?

A. Cisco Encrypted Traffic Analytics

B. Cisco Umbrella

C. Cisco Stealth watch

D. Cisco CTA

Answer: C

Q99

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

A. InfluxDB

B. Grafana

C. Splunk

D. SNMP

Answer: A

Q100

Which type of data exfiltration technique encodes data in outbound DNS requests to specific servers and can be stopped by Cisco Umbrella?

A. DNS tunneling

B. cache poisoning

C. DNS flood attack

D. DNS hijacking

Answer: A

Q101

An email administrator is setting up a new Cisco ESA The administrator wants to enable the blocking of greymail for the end user Which feature must the administrator enable first?

A. Intelligent Multi-Scan

B. File Analysis

C. iP Reputation Filtering

D. Anti-Virus Filtering

Answer: A

Q102

Which standard is used to automate exchanging cyber threat information?

A. loC

B. TAXII

C. MITRE

D. STIX

Answer: A

Q103

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. multichannel GUI

B. streamlined access

C. dual-SSID BYOD

D. single-SSID BYOD

Answer: C

Q104

Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks'? (Choose two.)

A. determines if the email messages are malicious

B. does a real-time user web browsing behavior analysis

C. blocks malicious websites and adds them to a block list

D. uses a static algorithm to determine malicious

E. provides a defense for on-premises email deployments

Answer: AE

Q105

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

A. Websecurityadvancedconfig

B. webadvancedconfig

C. outbreakconfig

D. websecurityconfig

Answer: A

Q106

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 ASAv

B. Cisco NBAR2

C. Account on Resolution

D. Cisco Prime Infrastructure

Answer: B

Q107

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

A. SubCA

B. self-signed

C. organization owned root

D. third-party

Answer: B

Q108

What is indicated by an AMP verdict score that is greater than 3?

A. the reputation score of the email sender

B. a malicious file

C. the malware type

D. a failed scan

Answer: A

Q109

How does a WCCP-configured router identify if the Cisco WSA is functional'?

A. If an ICMP ping fails three consecutive times between a router and the WSA. traffic is no longer transmitted to the router

B. The router sends a Here-I-Am message every 10 seconds and the WSA acknowledges with an l-See-You message

C. The WSA sends a Here-I-Am message every 10 seconds and the router acknowledges with an l-See-You message

D. If an ICMP ping fails three consecutive times between a router and the WSA. traffic is no longer transmitted to the WSA.

Answer: C

Q110

Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using higher-level protocols without re addressing the network'?

A. multiple context mode

B. transparent mode

C. single context mode

D. routed mode

Answer:B

Q111

Which solution detects threats across a private network public clouds and encrypted traffic?

A. Cisco Umbrella

B. Cisco Stealthwatch

C. Cisco CTA

D. Cisco Encrypted Traffic Analytics

Answer: B

Q112

What are two benefits of using Cisco Duo as an MFA solution? (Choose two)

A. allows for centralized management of endpoint device applications and configurations

B. encrypts data that is stored on endpoints

C. native integration that helps secure applications across multiple cloud platforms or on-premises environments

D. grants administrators a way to remotely wipe a lost or stolen device

E. provides simple and streamlined login experience for multiple applications and users

Answer: CE

Q113

In which scenario is endpoint-based security the solution'?

A. device profiling and authorization

B. inspecting encrypted traffic

C. performing signature-based application control

D. inspecting a password-protected archive

Answer: C

Q114

Which metric is used by the monitoring agent to collect and output packet loss and jitter information?

A. AVC performance

B. TCP performance

C. WSAv performance

D. RTP performance

Answer: D

Q115

What are two characteristics of the RESTful architecture used within Cisco DNA Center? (Choose two)

A. REST uses HTTP to send a request to a web service

B. REST is a Linux platform-based architecture.

C. REST codes can be compiled with any programming language

D. The POST action replaces existing data at the URL path

E. REST uses methods such as GET PUT POST, and DELETE

Answer: CE

Q116

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



Item 116 of 122 (Drag&Drop, Q1)

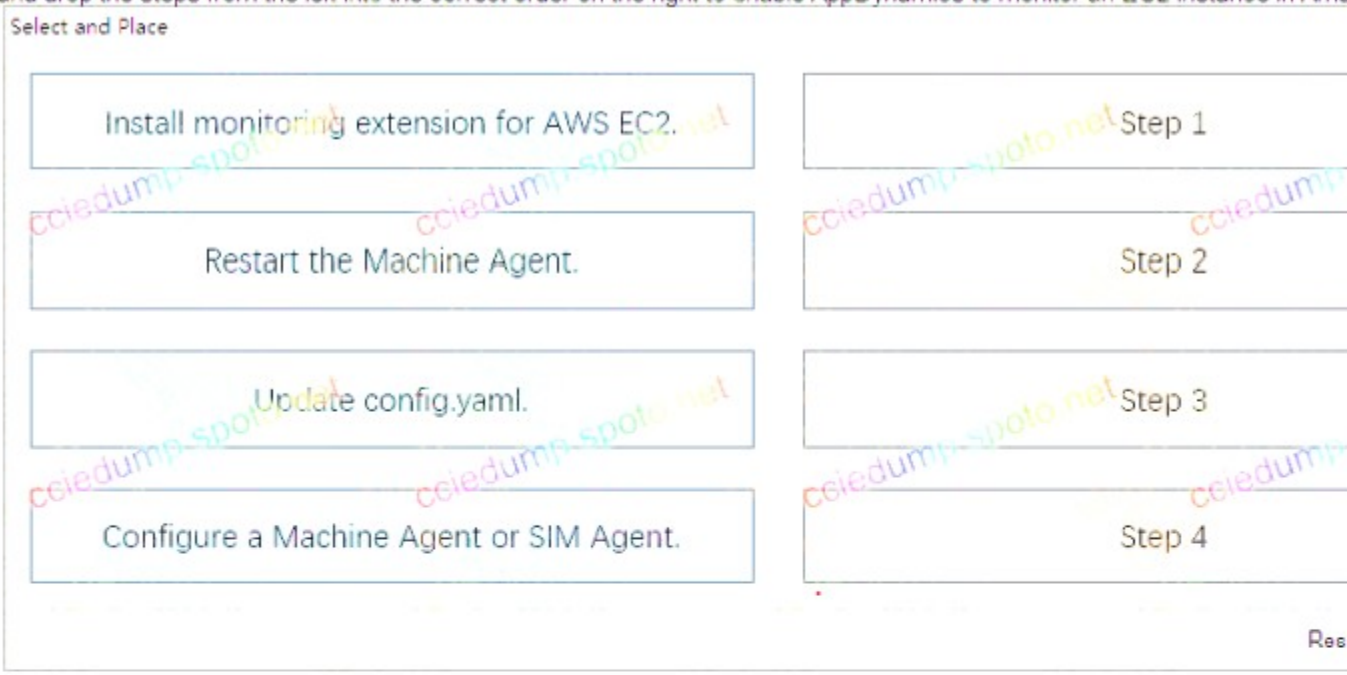
Drag and drop the exploits from the left onto the type of security vulnerability on the right.



Q117

Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Ama

Select and Place

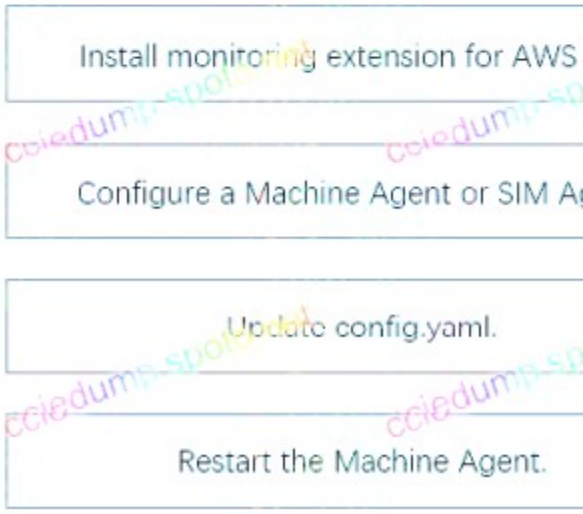


Item 117 of 122 (Drag&Drop, Q2)

Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazo

Select and Place

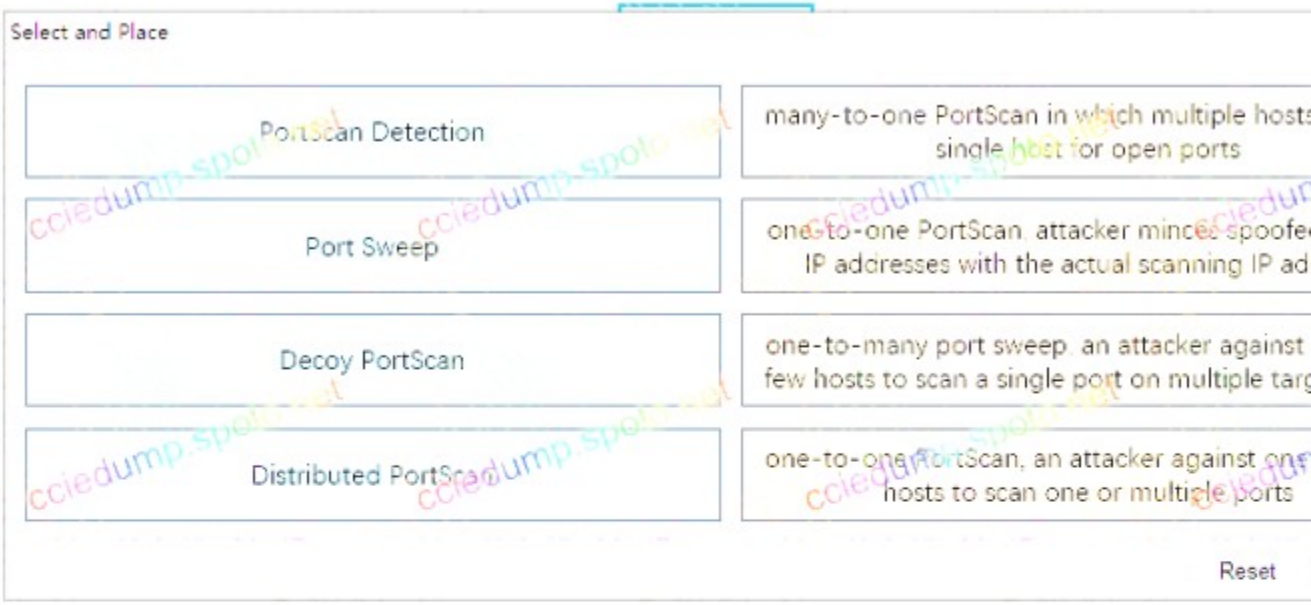
Answer:



https://www.appdynamics.com/community/exchange/extension/aws-ec2-monitoring-extension/

Q118

Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the



Item 118 of 122 (Drag&Drop, Q3)

Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the

Select and Place

Answer:



https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Detecting_Specific_Threats

Q119

Drag and drop the features of Cisco ASA with Firepower from the left onto the benefits on the right.

Select and Place

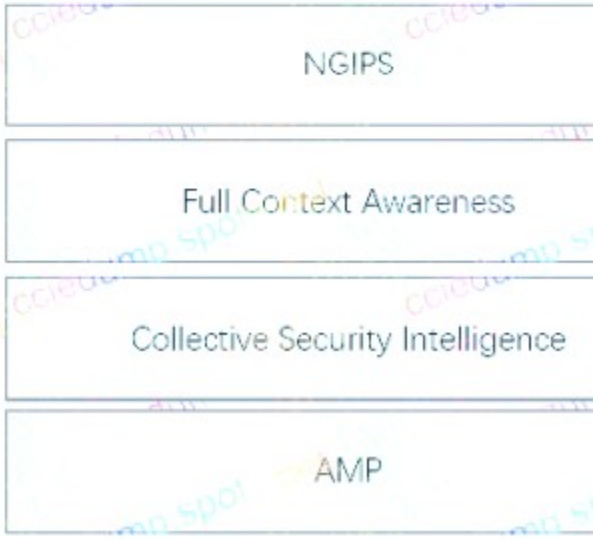


Item 119 of 122 (Drag&Drop, Q4)

Drag and drop the features of Cisco ASA with Firepower from the left onto the benefits on the right.

Select and Place

Answer:



Q120

Drag and Select and Place

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

Reset

☐ Mark

Item 120 of 122 (Drag&Drop, Q5)

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

Select and Place

Answer:

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

Q121

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

Select and Place



Item 121 of 122 (Drag&Drop, Q6)

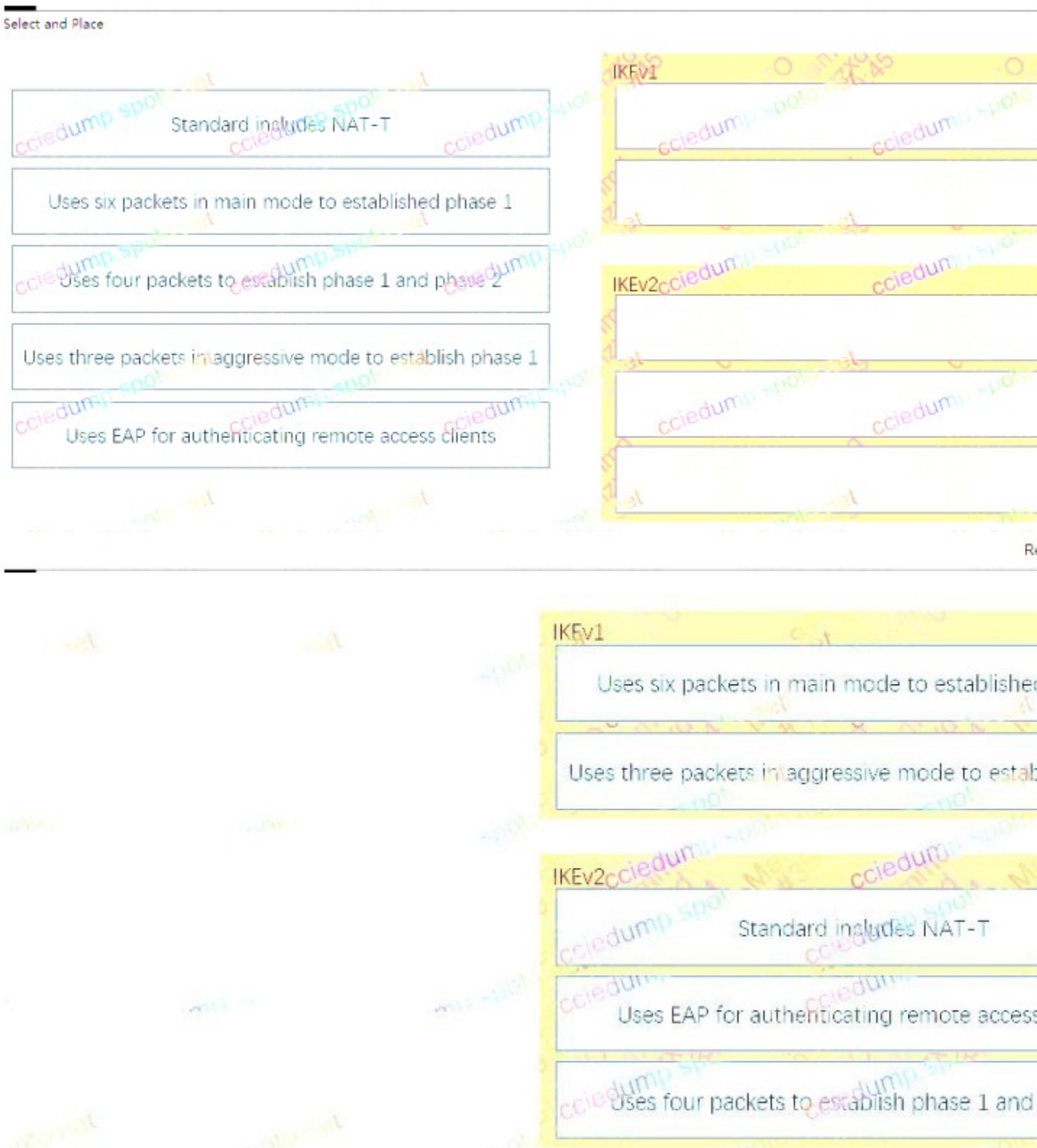
Drag and drop the concepts from the left onto the correct descriptions on the right.

Select and Place

Answer:



Q122


Select and Place
Standard includes NAT-T
Uses six packets in main mode to established 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
IKEv1
Uses six packets in main mode to establishe
Uses three packets in aggressive mode to estab
IKEv2
Standard includes NAT-T
Uses EAP for authenticating remote access
Uses four packets to establish phase 1 and