

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

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



NEW QUESTION 1

- (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 2

- (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 3

- (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 4

- (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 5

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 6

- (Exam Topic 3)

What is the purpose of CA in a PKI?

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

Answer: A

Explanation:

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

NEW QUESTION 7

- (Exam Topic 3)

Which type of DNS abuse exchanges data between two computers even when there is no direct connection?

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

Answer: D

Explanation:

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

NEW QUESTION 8

- (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 9

- (Exam Topic 3)

Which DevSecOps implementation process gives a weekly or daily update instead of monthly or quarterly in the applications?

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

Answer: B

Explanation:

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

NEW QUESTION 10

- (Exam Topic 3)

Which two commands are required when configuring a flow-export action on a Cisco ASA? (Choose two.)

- A. flow-export event-type
- B. policy-map
- C. access-list
- D. flow-export template timeout-rate 15
- E. access-group

Answer: AB

NEW QUESTION 10

- (Exam Topic 3)

Which Cisco platform provides an agentless solution to provide visibility across the network including encrypted traffic analytics to detect malware in encrypted traffic without the need for decryption?

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

Answer: B

NEW QUESTION 13

- (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 14

- (Exam Topic 3)

Which Cisco ISE service checks the compliance of endpoints before allowing the endpoints to connect to the network?

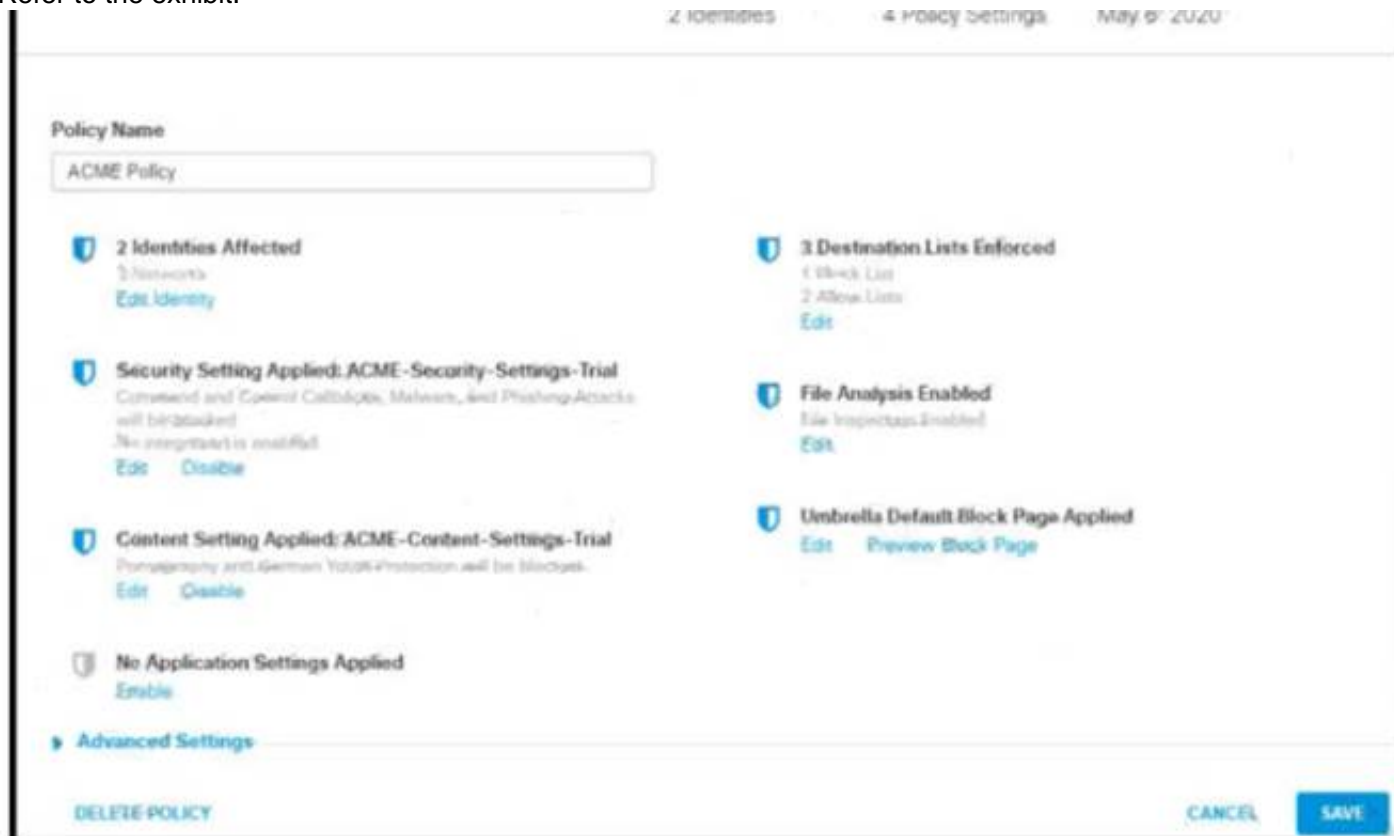
- A. posture
- B. profiler
- C. Cisco TrustSec
- D. Threat Centric NAC

Answer: A

NEW QUESTION 18

- (Exam Topic 3)

Refer to the exhibit.



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

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

Answer: B

NEW QUESTION 20

- (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 22

- (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 26

- (Exam Topic 3)

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. single interface
- B. multi-context
- C. transparent
- D. two-interface

Answer: D

NEW QUESTION 31

- (Exam Topic 3)

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

- A. Configure a Cisco FMC to send syslogs to Cisco Stealthwatch Cloud
- B. Deploy the Cisco Stealthwatch Cloud PNM sensor that sends data to Cisco Stealthwatch Cloud
- C. Deploy a Cisco FTD sensor to send network events to Cisco Stealthwatch Cloud
- D. Configure a Cisco FMC to send NetFlow to Cisco Stealthwatch Cloud

Answer: B

Explanation:

Reference:

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

NEW QUESTION 32

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 36

- (Exam Topic 3)

What is a function of Cisco AMP for Endpoints?

- A. It detects DNS attacks
- B. It protects against web-based attacks
- C. It blocks email-based attacks
- D. It automates threat responses of an infected host

Answer: D

NEW QUESTION 41

- (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 43

- (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 48

- (Exam Topic 3)

What is a description of microsegmentation?

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

Answer: B

NEW QUESTION 49

- (Exam Topic 3)

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

- A. Add the specified addresses to the identities list and create a block action.
- B. Create a destination list for addresses to be allowed or blocked.
- C. Use content categories to block or allow specific addresses.
- D. Modify the application settings to allow only applications to connect to required addresses.

Answer: B

NEW QUESTION 51

- (Exam Topic 3)

Which two configurations must be made on Cisco ISE and on Cisco TrustSec devices to force a session to be adjusted after a policy change is made? (Choose two)

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

Answer: DE

NEW QUESTION 54

- (Exam Topic 3)

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

- A. WSAv performance
- B. AVC performance
- C. OTCP performance
- D. RTP performance

Answer: D

NEW QUESTION 55

- (Exam Topic 3)

An engineer needs to add protection for data in transit and have headers in the email message Which configuration is needed to accomplish this goal?

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

Answer: D

NEW QUESTION 58

- (Exam Topic 3)

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 NGFW
- B. Cisco AnyConnect
- C. Cisco AMP for Endpoints
- D. Cisco Duo

Answer: D

NEW QUESTION 59

- (Exam Topic 3)

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

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

Answer: CD

NEW QUESTION 64

- (Exam Topic 3)

Refer to the exhibit.


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

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

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

Answer: B

NEW QUESTION 68

- (Exam Topic 3)

A company identified a phishing vulnerability during a pentest What are two ways the company can protect employees from the attack? (Choose two.)

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

Answer: AB

NEW QUESTION 71

- (Exam Topic 3)

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

- A. The hosts must run Cisco AsyncOS 10.0 or greater.
- B. The hosts must run different versions of Cisco AsyncOS.
- C. The hosts must have access to the same defined network.
- D. The hosts must use a different datastore than the virtual appliance.

Answer: C

NEW QUESTION 72

- (Exam Topic 3)

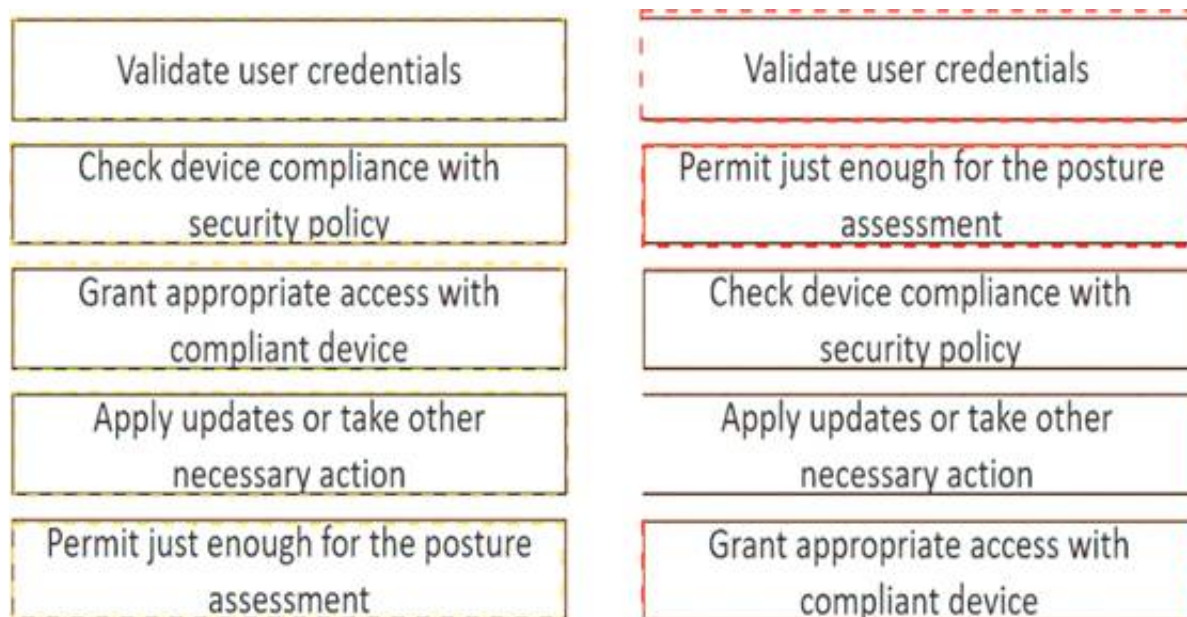
Drag and drop the posture assessment flow actions from the left into a sequence on the right.

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 77

- (Exam Topic 3)

What is a benefit of using Cisco Tetration?

- A. It collects telemetry data from servers and then uses software sensors to analyze flow information.
- B. It collects policy compliance data and process details.
- C. It collects enforcement data from servers and collects interpacket variation.
- D. It collects near-real time data from servers and inventories the software packages that exist on servers.

Answer: C

NEW QUESTION 82

- (Exam Topic 3)

What are two functions of IKEv1 but not IKEv2? (Choose two)

- A. NAT-T is supported in IKEv1 but not in IKEv2.
- B. With IKEv1, when using aggressive mode, the initiator and responder identities are passed cleartext
- C. With IKEv1, mode negotiates faster than main mode
- D. IKEv1 uses EAP authentication
- E. IKEv1 conversations are initiated by the IKE_SA_INIT message

Answer: CE

NEW QUESTION 84

- (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 85

- (Exam Topic 3)

Which feature does the IaaS model provide?

- A. granular control of data
- B. dedicated, restricted workstations
- C. automatic updates and patching of software
- D. software-defined network segmentation

Answer: C

NEW QUESTION 90

- (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 91

- (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 92

- (Exam Topic 3)

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

- A. as part of the UDP/53 packet payload
 B. as part of the domain name
 C. as part of the TCP/53 packet header
 D. as part of the DNS response packet

Answer: A

NEW QUESTION 96

- (Exam Topic 3)

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

Answer: A

NEW QUESTION 97

- (Exam Topic 3)

An engineer is configuring Dropbox integration with Cisco Cloudlock. Which action must be taken before granting API access in the Dropbox admin console?

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

Answer: A

NEW QUESTION 99

- (Exam Topic 3)

Refer to the exhibit.

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

A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced What is the cause of this issue?

- A. The key was configured in plain text.
- B. NTP authentication is not enabled.
- C. The hashing algorithm that was used was MD5. which is unsupported.
- D. The router was not rebooted after the NTP configuration updated.

Answer: B

NEW QUESTION 101

- (Exam Topic 3)

Refer to the exhibit.

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

A Cisco ISE administrator adds a new switch to an 802.1X deployment and has difficulty with some endpoints gaining access. Most PCs and IP phones can connect and authenticate using their machine certificate credentials. However printer and video cameras cannot base d on the interface configuration provided, what must be to get these devices on to the network using Cisco ISE for authentication and authorization while maintaining security controls?

- A. Change the default policy in Cisco ISE to allow all devices not using machine authentication .
- B. Enable insecure protocols within Cisco ISE in the allowed protocols configuration.
- C. Configure authentication event fail retry 2 action authorize vlan 41 on the interface
- D. Add mab to the interface configuration.

Answer: D

NEW QUESTION 103

- (Exam Topic 3)

What is a functional difference between Cisco AMP for Endpoints and Cisco Umbrella Roaming Client?

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

Answer: D

NEW QUESTION 108

- (Exam Topic 3)

Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or Microsoft vSwitch?

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

Answer: C

Explanation:

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

NEW QUESTION 111

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 114

- (Exam Topic 3)

An administrator is configuring NTP on Cisco ASA via ASDM and needs to ensure that rogue NTP servers cannot insert themselves as the authoritative time source. Which two steps must be taken to accomplish this task? (Choose two)

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

Answer: CD

NEW QUESTION 118

- (Exam Topic 3)

What is a feature of container orchestration?

- A. ability to deploy Amazon ECS clusters by using the Cisco Container Platform data plane
- B. ability to deploy Amazon EKS clusters by using the Cisco Container Platform data plane
- C. ability to deploy Kubernetes clusters in air-gapped sites
- D. automates daily updates

Answer: C

NEW QUESTION 120

- (Exam Topic 3)

What must be enabled to secure SaaS-based applications?

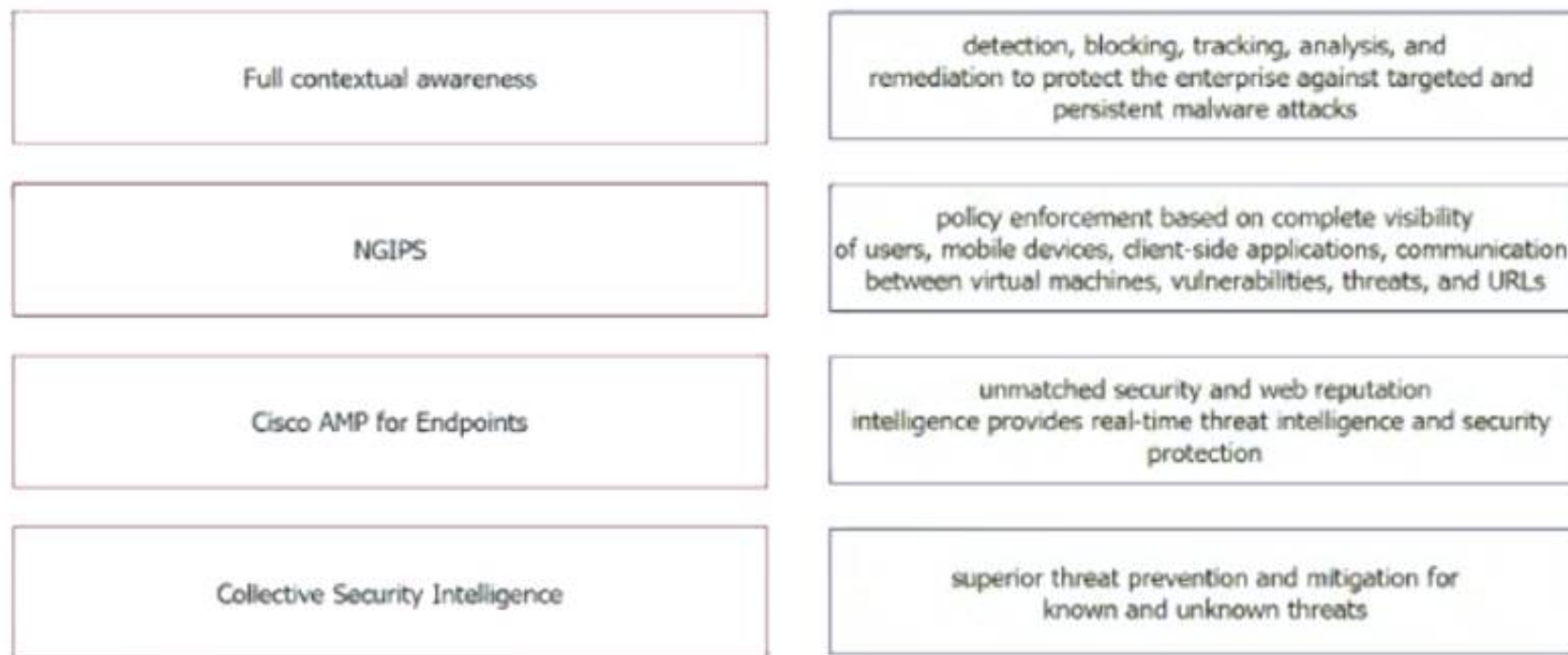
- A. modular policy framework
- B. two-factor authentication
- C. application security gateway
- D. end-to-end encryption

Answer: C

NEW QUESTION 122

- (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 125

- (Exam Topic 3)

For a given policy in Cisco Umbrella, how should a customer block website based on a custom list?

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

Answer: C

NEW QUESTION 126

- (Exam Topic 3)

Which endpoint solution protects a user from a phishing attack?

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

Answer: D

NEW QUESTION 131

- (Exam Topic 3)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 136

- (Exam Topic 3)

Why should organizations migrate to a multifactor authentication strategy?

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

Answer: D

NEW QUESTION 138

- (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 140

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 141

- (Exam Topic 3)

Which algorithm is an NGE hash function?

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

Answer: D

NEW QUESTION 144

- (Exam Topic 3)

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 victim's web browser executes the code?

- A. buffer overflow
- B. browser WGET
- C. SQL injection
- D. cross-site scripting

Answer: D

NEW QUESTION 145

- (Exam Topic 3)

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

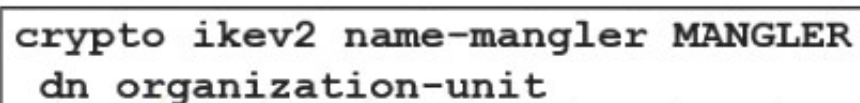
- A. pxGrid
- B. NetFlow
- C. SNMP
- D. Cisco Talos

Answer: A

NEW QUESTION 148

- (Exam Topic 3)

Refer to the exhibit.



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

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

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

Answer: A

NEW QUESTION 150

- (Exam Topic 3)

A Cisco AMP for Endpoints administrator configures a custom detection policy to add specific MD5 signatures. The configuration is created in the simple detection policy section, but it does not work. What is the reason for this failure?

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

Answer: D

NEW QUESTION 151

- (Exam Topic 3)

An engineer is configuring device-hardening on a router in order to prevent credentials from being seen if the router configuration was compromised. Which command should be used?

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

Answer: A

NEW QUESTION 155

- (Exam Topic 3)

Which capability is provided by application visibility and control?

- A. reputation filtering
- B. data obfuscation
- C. data encryption
- D. deep packet inspection

Answer: D

NEW QUESTION 158

- (Exam Topic 3)

Which ESA implementation method segregates inbound and outbound email?

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

Answer: D

NEW QUESTION 159

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 160

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 165

- (Exam Topic 3)

What are two workloaded security models? (Choose two)

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

Answer: CD

NEW QUESTION 166

- (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 170

- (Exam Topic 2)

An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?

- A. Cisco Defense Orchestrator
- B. Cisco Secureworks
- C. Cisco DNA Center
- D. Cisco Configuration Professional

Answer: A

Explanation:

Reference:

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

NEW QUESTION 171

- (Exam Topic 2)

Which cryptographic process provides origin confidentiality, integrity, and origin authentication for packets?

- A. IKEv1
- B. AH
- C. ESP
- D. IKEv2

Answer: C

NEW QUESTION 173

- (Exam Topic 2)

For Cisco IOS PKI, which two types of Servers are used as a distribution point for CRLs? (Choose two)

- A. SDP
- B. LDAP
- C. subordinate CA
- D. SCP
- E. HTTP

Answer: BE

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mtbook/sec-pk

NEW QUESTION 176

- (Exam Topic 2)

What is the function of SDN southbound API protocols?

- A. to allow for the dynamic configuration of control plane applications
- B. to enable the controller to make changes
- C. to enable the controller to use REST
- D. to allow for the static configuration of control plane applications

Answer: B

Explanation:

Reference: <https://www.ciscopress.com/articles/article.asp?p=3004581&seqNum=2>

Note: Southbound APIs helps us communicate with data plane (not control plane) applications

NEW QUESTION 181

- (Exam Topic 2)

Refer to the exhibit.

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

What will happen when this Python script is run?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 186

- (Exam Topic 2)

Which two cryptographic algorithms are used with IPsec? (Choose two)

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

Answer: CE

Explanation:

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

NEW QUESTION 190

- (Exam Topic 2)

A network administrator is configuring SNMPv3 on a new router. The users have already been created; however, an additional configuration is needed to facilitate access to the SNMP views. What must the administrator do to accomplish this?

- A. map SNMPv3 users to SNMP views
- B. set the password to be used for SNMPv3 authentication
- C. define the encryption algorithm to be used by SNMPv3
- D. specify the UDP port used by SNMP

Answer: B

NEW QUESTION 191

- (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 193

- (Exam Topic 2)

Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps.

Which two actions must be taken to ensure that interfaces are put back into service? (Choose two)

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

Answer: CE

Explanation:

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

NEW QUESTION 194

- (Exam Topic 2)

Which attack is preventable by Cisco ESA but not by the Cisco WSA?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 196

- (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 200

- (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.

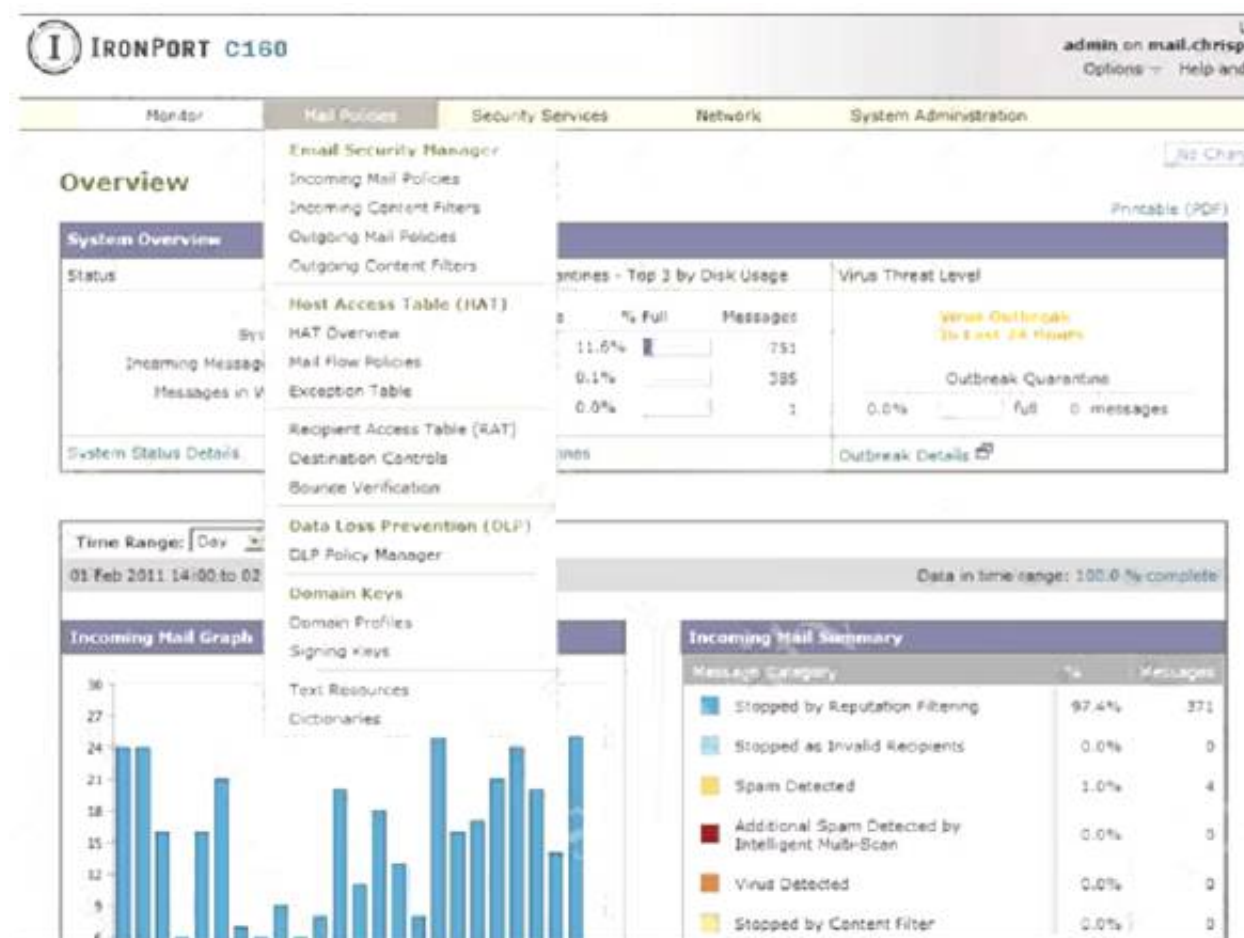
What must be configured to accomplish this?

- 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 201

- (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 204

- (Exam Topic 2)

Which public cloud provider supports the Cisco Next Generation Firewall Virtual?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 208

- (Exam Topic 2)

An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco Firepower. Which feature should be used to accomplish this?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 211

- (Exam Topic 2)

What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?

- A. Cisco Cloudlock
- B. Cisco Umbrella
- C. Cisco AMP
- D. Cisco App Dynamics

Answer: A

Explanation:

Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

NEW QUESTION 216

- (Exam Topic 2)

In which two ways does Easy Connect help control network access when used with Cisco TrustSec? (Choose two)

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

Answer: CE

Explanation:

Reference:

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

NEW QUESTION 217

- (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 219

- (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 224

- (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 228

- (Exam Topic 2)

What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

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

Answer: B

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nse1.pdf>

NEW QUESTION 231

- (Exam Topic 2)

What is an attribute of the DevSecOps process?

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

Answer: C

Explanation:

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

NEW QUESTION 233

- (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 234

- (Exam Topic 2)

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

- A. Cisco Umbrella
- B. Cisco AMP
- C. Cisco Stealthwatch
- D. Cisco Tetration

Answer: D

Explanation:

Reference:

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

NEW QUESTION 239

- (Exam Topic 2)

An engineer notices traffic interruption on the network. Upon further investigation, it is learned that broadcast packets have been flooding the network. What must be configured, based on a predefined threshold, to address this issue?

- A. Bridge Protocol Data Unit guard
- B. embedded event monitoring
- C. storm control
- D. access control lists

Answer: C

Explanation:

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm. By using the "storm-control broadcast level [falling-threshold]" we can limit the broadcast traffic on the switch.

NEW QUESTION 240

- (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 242

- (Exam Topic 2)

Refer to the exhibit.

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

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

Answer: D

Explanation:

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

NEW QUESTION 245

- (Exam Topic 1)

What is the primary role of the Cisco Email Security Appliance?

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

Answer: B

Explanation:

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

NEW QUESTION 249

- (Exam Topic 2)

An organization has two systems in their DMZ that have an unencrypted link between them for communication.

The organization does not have a defined password policy and uses several default accounts on the systems. The application used on those systems also have not gone through stringent code reviews. Which vulnerability would help an attacker brute force their way into the systems?

- A. weak passwords
- B. lack of input validation
- C. missing encryption
- D. lack of file permission

Answer: C

Explanation:

Reference: <https://tools.ietf.org/html/rfc3954>

NEW QUESTION 252

- (Exam Topic 2)

What is a benefit of using Cisco FMC over Cisco ASDM?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 255

- (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 256

- (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 257

- (Exam Topic 1)

What is a commonality between DMVPN and FlexVPN technologies?

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

Answer: D

Explanation:

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

NEW QUESTION 262

- (Exam Topic 1)

Which VPN technology can support a multivendor environment and secure traffic between sites?

- A. SSL VPN
- B. GET VPN

- C. FlexVPN
- D. DMVPN

Answer: C

Explanation:

FlexVPN is an IKEv2-based VPN technology that provides several benefits beyond traditional site-to-site VPN implementations. FlexVPN is a standards-based solution that can interoperate with non-Cisco IKEv2 implementations. Therefore FlexVPN can support a multivendor environment. All of the three VPN technologies support traffic between sites (site-to-site or spoke-to-spoke).

NEW QUESTION 264

- (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 267

- (Exam Topic 1)

Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?

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

Answer: D

NEW QUESTION 268

- (Exam Topic 1)

Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?

- A. Group Policy
- B. Access Control Policy
- C. Device Management Policy
- D. Platform Service Policy

Answer: D

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/platfo> the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the best answer here so we have to choose it.

NEW QUESTION 271

- (Exam Topic 1)

For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two)

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

Answer: AD

NEW QUESTION 274

- (Exam Topic 1)

Which ASA deployment mode can provide separation of management on a shared appliance?

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

Answer: C

NEW QUESTION 278

- (Exam Topic 1)

Refer to the exhibit.

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

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

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

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

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

service-policy inside-policy global
```

What is a result of the configuration?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 280

- (Exam Topic 1)

A company is experiencing exfiltration of credit card numbers that are not being stored on-premise. The company needs to be able to protect sensitive data throughout the full environment. Which tool should be used to accomplish this goal?

- A. Security Manager
- B. Cloudlock
- C. Web Security Appliance
- D. Cisco ISE

Answer: B

Explanation:

Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

NEW QUESTION 284

- (Exam Topic 1)

A mall provides security services to customers with a shared appliance. The mall wants separation of management on the shared appliance. Which ASA deployment mode meets these needs?

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

Answer: C

NEW QUESTION 288

- (Exam Topic 1)

An engineer configured a new network identity in Cisco Umbrella but must verify that traffic is being routed through the Cisco Umbrella network. Which action tests the routing?

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

Answer: B

NEW QUESTION 292

- (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 297

- (Exam Topic 1)

Refer to the exhibit.

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

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

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']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
        mac = network_interface.get('mac')
        ip = network_interface.get('ip')
        ipv6 = network_interface.get('ipv6')
        print(mac, ip, ipv6)
```

What does the API do when connected to a Cisco security appliance?

- A. get the process and PID information from the computers in the network
- B. create an SNMP pull mechanism for managing AMP
- C. gather network telemetry information from AMP for endpoints
- D. gather the network interface information about the computers AMP sees

Answer: D

Explanation:

Reference:

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

NEW QUESTION 302

- (Exam Topic 1)

Which technology must be used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 307

- (Exam Topic 1)

What provides visibility and awareness into what is currently occurring on the network?

- A. CMX
- B. WMI

- C. Prime Infrastructure
- D. Telemetry

Answer: D

Explanation:

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

NEW QUESTION 308

- (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 312

- (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 315

- (Exam Topic 1)

What is a feature of the open platform capabilities of Cisco DNA Center?

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

Answer: A

NEW QUESTION 318

- (Exam Topic 1)

Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

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

Answer: A

Explanation:

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

NEW QUESTION 323

- (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 327

- (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 329

- (Exam Topic 1)

In which two ways does a system administrator send web traffic transparently to the Web Security Appliance? (Choose two)

- A. configure Active Directory Group Policies to push proxy settings
- B. configure policy-based routing on the network infrastructure
- C. reference a Proxy Auto Config file
- D. configure the proxy IP address in the web-browser settings
- E. use Web Cache Communication Protocol

Answer: BE

NEW QUESTION 334

- (Exam Topic 1)

What must be used to share data between multiple security products?

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

Answer: B

NEW QUESTION 335

- (Exam Topic 1)

An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA. Which Cisco ASA command must be used?

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

Answer: A

Explanation:

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

NEW QUESTION 340

- (Exam Topic 1)

Refer to the exhibit.

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

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

- A. show authentication registrations
- B. show authentication method
- C. show dot1x all
- D. show authentication sessions

Answer: D

Explanation:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-c> Displaying the Summary of All Auth Manager Sessions on the Switch

Enter the following:

Switch# show authentication sessions

Interface MAC Address Method Domain Status Session ID

Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success

0A3462B10000000D24F80B58

Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

NEW QUESTION 341

- (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 342

- (Exam Topic 1)

Which two features of Cisco Email Security can protect your organization against email threats? (Choose two)

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

Answer: BD

Explanation:

Reference:

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

NEW QUESTION 346

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 350

- (Exam Topic 1)

Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?

- A. url
- B. terminal
- C. profile
- D. selfsigned

Answer: C

Explanation:

Reference:

<https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/211333-IOSPKI-Deploy>

NEW QUESTION 352

- (Exam Topic 1)

Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 357

- (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 358

- (Exam Topic 1)

Which statement describes a traffic profile on a Cisco Next Generation Intrusion Prevention System?

- A. It allows traffic if it does not meet the profile.
- B. It defines a traffic baseline for traffic anomaly deduction.
- C. It inspects hosts that meet the profile with more intrusion rules.
- D. It blocks traffic if it does not meet the profile.

Answer: B

NEW QUESTION 359

- (Exam Topic 1)

How is DNS tunneling used to exfiltrate data out of a corporate network?

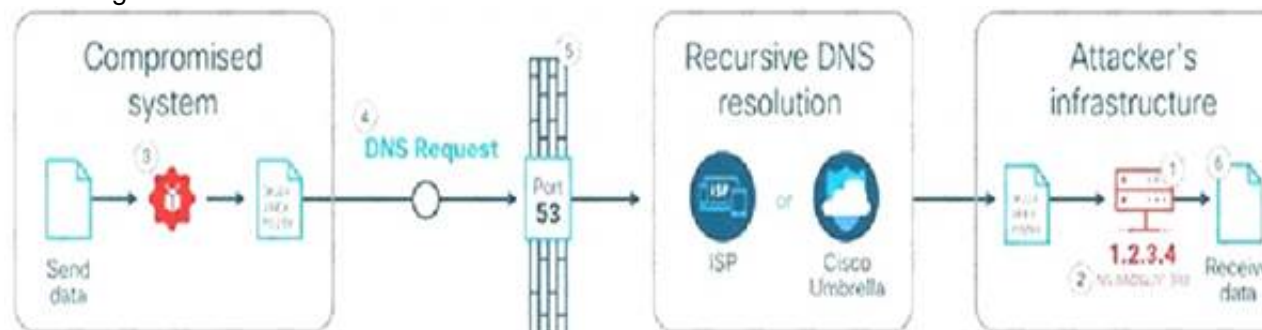
- A. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.
- B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.
- C. It redirects DNS requests to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

Answer:

B

Explanation:

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



➤ The attacker incorporates one of many open-source DNS tunneling kits into an authoritative DNSnameserver (NS) and malicious payload.2. An IP address (e.g. 1.2.3.4) is allocated from the attacker's infrastructure and a domain name (e.g. attackerdomain.com) is registered or reused. The registrar informs the top-level domain (.com) nameservers to refer requests for attackerdomain.com to ns.attackerdomain.com, which has a DNS record mapped to 1.2.3.43. The attacker compromises a system with the malicious payload. Once the desired data is obtained, the payload encodes the data as a series of 32 characters (0-9, A-Z) broken into short strings (3KJ242AIE9, P028X977W,...).4. The payload initiates thousands of unique DNS record requests to the attacker's domain with each string as Reference: <https://learn-umbrella.cisco.com/i/775902-dns-tunneling/0>

NEW QUESTION 362

- (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: `<ahref=javascript:alert('XSS')>Click Here` is equivalent to: `Click Here` Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form.

NEW QUESTION 363

- (Exam Topic 1)

What is a characteristic of Firepower NGIPS inline deployment mode?

- A. ASA with Firepower module cannot be deployed.
- B. It cannot take actions such as blocking traffic.
- C. It is out-of-band from traffic.
- D. It must have inline interface pairs configured.

Answer: D

NEW QUESTION 365

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 369

- (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 373

- (Exam Topic 1)

Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

- A. transparent
- B. redirection
- C. forward
- D. proxy gateway

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVDWebSecurityUsingCiscoWSADesign>

NEW QUESTION 378

- (Exam Topic 1)

Which technology reduces data loss by identifying sensitive information stored in public computing environments?

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

Answer: D

NEW QUESTION 383

- (Exam Topic 1)

Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?

- A. Advanced Malware Protection
- B. Platform Exchange Grid
- C. Multifactor Platform Integration
- D. Firepower Threat Defense

Answer: B

Explanation:

With Cisco pxGrid (Platform Exchange Grid), your multiple security products can now share data and work together. This open, scalable, and IETF standards-driven platform helps you automate security to get answers and contain threats faster.

NEW QUESTION 386

- (Exam Topic 1)

Which attack is commonly associated with C and C++ programming languages?

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

Answer: D

Explanation:

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's allotted memory space. This happens quite frequently in the case of arrays.

NEW QUESTION 389

- (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 394

- (Exam Topic 1)

Which statement about IOS zone-based firewalls is true?

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

Answer: D

NEW QUESTION 395

- (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 399

- (Exam Topic 1)

Which threat involves software being used to gain unauthorized access to a computer system?

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

Answer: A

NEW QUESTION 401

- (Exam Topic 1)

Which capability is exclusive to a Cisco AMP public cloud instance as compared to a private cloud instance?

- A. RBAC
- B. ETHOS detection engine
- C. SPERO detection engine
- D. TETRA detection engine

Answer: B

NEW QUESTION 404

- (Exam Topic 1)

Which action controls the amount of URI text that is stored in Cisco WSA logs files?

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

Answer: B

NEW QUESTION 407

- (Exam Topic 1)

What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?

- A. STIX
- B. XMPP
- C. pxGrid
- D. SMTP

Answer: A

Explanation:

TAXII (Trusted Automated Exchange of Indicator Information) is a standard that provides a transport

NEW QUESTION 412

- (Exam Topic 1)

Which two are valid suppression types on a Cisco Next Generation Intrusion Prevention System? (Choose two)

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

Answer: BC

NEW QUESTION 414

- (Exam Topic 1)

How is ICMP used as an exfiltration technique?

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

Answer: C

NEW QUESTION 419

- (Exam Topic 1)

What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two)

- A. data exfiltration
- B. command and control communication
- C. intelligent proxy
- D. snort
- E. URL categorization

Answer: AB

Explanation:

Reference:

<https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-73655>

NEW QUESTION 420

- (Exam Topic 1)

How does Cisco Stealthwatch Cloud provide security for cloud environments?

- A. It delivers visibility and threat detection.
- B. It prevents exfiltration of sensitive data.
- C. It assigns Internet-based DNS protection for clients and servers.
- D. It facilitates secure connectivity between public and private networks.

Answer: A

Explanation:

Cisco Stealthwatch Cloud: Available as an SaaS product offer to provide visibility and threat detection within public cloud infrastructures such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

NEW QUESTION 425

- (Exam Topic 1)

Which two conditions are prerequisites for stateful failover for IPsec? (Choose two)

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

Answer: CE

Explanation:

Stateful failover for IP Security (IPsec) enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This failover process is transparent to users and does not require adjustment or reconfiguration of any remote peer. Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators. Prerequisites for Stateful Failover for IPsec

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpn/configuration/15-mt/sec-vpn-availability-15-the-prerequisites-only-stated-that-Both-routers-should-be-the-same-type-of-device-but-in-the-Restrictions-for-Stateful-Failover-for-IPsec-section-of-the-link-above-it-requires-Both-the-active-and-standby-devices-must-run-the-identical-version-of-the-Cisco-IOS-software-so-answer-E-is-better-than-answer-B

NEW QUESTION 430

- (Exam Topic 1)

Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?

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

Answer: D

Explanation:

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

NEW QUESTION 435

- (Exam Topic 1)

An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?

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

Answer: D

NEW QUESTION 439

- (Exam Topic 1)

Where are individual sites specified to be blacklisted in Cisco Umbrella?

- A. application settings
- B. content categories
- C. security settings
- D. destination lists

Answer: D

Explanation:

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

NEW QUESTION 440

- (Exam Topic 3)

An organization wants to secure data in a cloud environment. Its security model requires that all users be authenticated and authorized. Security configuration and posture must be continuously validated before access is granted or maintained to applications and data. There is also a need to allow certain application traffic and deny all other traffic by default. Which technology must be used to implement these requirements?

- A. Virtual routing and forwarding
- B. Microsegmentation
- C. Access control policy
- D. Virtual LAN

Answer: C

Explanation:

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location. The Zero Trust model uses microsegmentation — a security technique that involves dividing perimeters into small zones to maintain separate access to every part of the network — to contain attacks.

NEW QUESTION 444

- (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 447

- (Exam Topic 3)

An engineer is trying to decide whether to use Cisco Umbrella, Cisco CloudLock, Cisco Stealthwatch, or Cisco AppDynamics Cloud Monitoring for visibility into data transfers as well as protection against data exfiltration. Which solution best meets these requirements?

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

Answer: D

NEW QUESTION 452

- (Exam Topic 3)

An engineer integrates Cisco FMC and Cisco ISE using pxGrid Which role is assigned for Cisco FMC?

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

Answer: D

NEW QUESTION 453

- (Exam Topic 3)

Cisco SensorBase gathers threat information from a variety of Cisco products and services and performs analytics to find patterns on threats Which term describes this process?

- A. deployment
- B. consumption
- C. authoring
- D. sharing

Answer: A

NEW QUESTION 458

- (Exam Topic 3)

What is a characteristic of an EDR solution and not of an EPP solution?

- A. stops all ransomware attacks
- B. retrospective analysis
- C. decrypts SSL traffic for better visibility
- D. performs signature-based detection

Answer: B

NEW QUESTION 461

- (Exam Topic 3)

When network telemetry is implemented, what is important to be enabled across all network infrastructure devices to correlate different sources?

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

Answer: B

NEW QUESTION 463

- (Exam Topic 3)

Which Cisco platform onboards the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing the endpoint to gain network access?

- A. Cisco ISE
- B. Cisco NAC
- C. Cisco TACACS+
- D. Cisco WSA

Answer: A

NEW QUESTION 468

- (Exam Topic 3)

Which system performs compliance checks and remote wiping?

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

Answer: A

NEW QUESTION 472

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 474

- (Exam Topic 3)

Which Cisco security solution stops exfiltration using HTTPS?

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

Answer: C

Explanation:

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

NEW QUESTION 479

- (Exam Topic 3)

An engineer needs to configure a Cisco Secure Email Gateway (SEG) to prompt users to enter multiple forms of identification before gaining access to the SEG. The SEG must also join a cluster using the preshared key of cisc421555367. What steps must be taken to support this?

- A. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG GUI.
- B. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG CLI.
- C. Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG CLI
- D. Enable two-factor authentication through a TACACS+ server, and then join the cluster via the SEG GUI.

Answer: C

Explanation:

Reference:

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

NEW QUESTION 481

- (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 482

- (Exam Topic 3)

Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?

- A. RADIUS-based REAP
- B. fingerprinting
- C. Dynamic ARP Inspection
- D. multifactor authentication

Answer: D

NEW QUESTION 484

- (Exam Topic 3)

Refer to the exhibit.



Consider that any feature of DNS requests, such as the length off the domain name and the number of subdomains, can be used to construct models of expected behavior to which observed values can be compared. Which type of malicious attack are these values associated with?

- A. Spectre Worm
- B. Eternal Blue Windows
- C. Heartbleed SSL Bug
- D. W32/AutoRun worm

Answer: D

NEW QUESTION 488

- (Exam Topic 3)

What is the target in a phishing attack?

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

Answer: D

NEW QUESTION 490

- (Exam Topic 3)

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 sampler
- D. flow monitor

Answer: D

NEW QUESTION 493

- (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 495

- (Exam Topic 3)

With Cisco AMP for Endpoints, which option shows a list of all files that have been executed in your environment?

- A. Prevalence
- B. File analysis
- C. Detections
- D. Vulnerable software
- E. Threat root cause

Answer: A

Explanation:

Reference: <https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf>

NEW QUESTION 499

- (Exam Topic 3)

What is a benefit of using a multifactor authentication strategy?

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

Answer: D

NEW QUESTION 500

- (Exam Topic 3)

Which Cisco DNA Center RESTful PNP API adds and claims a device into a workflow?

- A. api/v1/fie/config
- B. api/v1/onboarding/pnp-device/import
- C. api/v1/onboarding/pnp-device
- D. api/v1/onboarding/workflow

Answer:

B

NEW QUESTION 505

- (Exam Topic 3)

Which baseline form of telemetry is recommended for network infrastructure devices?

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

Answer: D

NEW QUESTION 506

- (Exam Topic 3)

What is the purpose of the Cisco Endpoint IoC feature?

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

Answer: A

Explanation:

Reference: <https://docs.amp.cisco.com/Cisco%20Endpoint%20IOC%20Attributes.pdf>

The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers.

NEW QUESTION 507

- (Exam Topic 3)

Which API method and required attribute are used to add a device into Cisco DNA Center with the native API?

- A. GET and serialNumber
- B. userSudiSerialNos and deviceInfo
- C. POST and name
- D. lastSyncTime and pid

Answer: A

NEW QUESTION 509

- (Exam Topic 3)

Which type of attack is MFA an effective deterrent for?

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

Answer: B

NEW QUESTION 511

- (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 512

- (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 513

- (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 515

- (Exam Topic 3)

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

Full Context Awareness	detection, blocking and remediation to protect the enterprise against targeted malware attacks
NGIPS	policy enforcement based on complete visibility of users and communication between virtual machines
AMP	real-time threat intelligence and security protection
Collective Security Intelligence	threat prevention and mitigation for known and unknown threats

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Full Context Awareness - policy enforcement NGIPS - threat prevention

AMP - real-time

Collective Sec Intel - Detection, blocking an remediation

NEW QUESTION 520

- (Exam Topic 3)

Which service allows a user export application usage and performance statistics with Cisco Application Visibility and control?

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

Answer: B

Explanation:

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

NEW QUESTION 523

- (Exam Topic 3)

Which two capabilities of Integration APIs are utilized with Cisco DNA center? (Choose two)

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

Answer: BC

Explanation:

Reference:

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

NEW QUESTION 528

- (Exam Topic 3)

Which IETF attribute is supported for the RADIUS CoA feature?

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

Answer: A

NEW QUESTION 532

- (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 534

- (Exam Topic 3)

Which industry standard is used to integrate Cisco ISE and pxGrid to each other and with other interoperable security platforms?

- A. IEEE
- B. IETF
- C. NIST
- D. ANSI

Answer: B

NEW QUESTION 536

- (Exam Topic 3)

When a transparent authentication fails on the Web Security Appliance, which type of access does the end user get?

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

Answer: C

NEW QUESTION 538

- (Exam Topic 3)

Why should organizations migrate to an MFA strategy for authentication?

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

Answer: A

NEW QUESTION 540

- (Exam Topic 3)

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

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

Answer: CE

NEW QUESTION 545

- (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 550

- (Exam Topic 3)

Which threat intelligence standard contains malware hashes?

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

Answer: A

NEW QUESTION 555

- (Exam Topic 3)

Which feature is used in a push model to allow for session identification, host reauthentication, and session termination?

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

Answer: C

NEW QUESTION 558

- (Exam Topic 3)

What provides total management for mobile and PC including managing inventory and device tracking, remote view, and live troubleshooting using the included native remote desktop support?

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

Answer: A

NEW QUESTION 562

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 566

- (Exam Topic 3)

Refer to the exhibit.

```
ASA# show service-policy sfr

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

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

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

Answer: AE

Explanation:

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

NEW QUESTION 570

- (Exam Topic 3)

A company has 5000 Windows users on its campus. Which two precautions should IT take to prevent WannaCry ransomware from spreading to all clients? (Choose two.)

- A. Segment different departments to different IP blocks and enable Dynamic ARP inspection on all VLANs
- B. Ensure that noncompliant endpoints are segmented off to contain any potential damage.
- C. Ensure that a user cannot enter the network of another department.
- D. Perform a posture check to allow only network access to those Windows devices that are already patched.
- E. Put all company users in the trusted segment of NGFW and put all servers to the DMZ segment of the Cisco NGF
- F. ni

Answer: BD

NEW QUESTION 573

- (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 574

- (Exam Topic 3)

What is the intent of a basic SYN flood attack?

- A. to solicit DNS responses
- B. to exceed the threshold limit of the connection queue
- C. to flush the register stack to re-initiate the buffers
- D. to cause the buffer to overflow

Answer: B

NEW QUESTION 575

- (Exam Topic 3)

```
aaa new-model
```

```
radius-server host 10.0.0.12 key secret12
```

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

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

Answer: D

NEW QUESTION 580

- (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 Stealthwatch Cloud
- C. Cisco Cloudlock
- D. Cisco Umbrella Investigate

Answer: C

NEW QUESTION 583

- (Exam Topic 3)

Which category includes DoS Attacks?

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

Answer: C

NEW QUESTION 588

- (Exam Topic 3)

Which Cisco solution extends network visibility, threat detection, and analytics to public cloud environments?

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

Answer: B

NEW QUESTION 592

- (Exam Topic 3)

Refer to the exhibit.



```

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

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

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

```

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

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

Answer: A

NEW QUESTION 596

- (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 599

- (Exam Topic 3)

An organization must add new firewalls to its infrastructure and wants to use Cisco ASA or Cisco FTD.

The chosen firewalls must provide methods of blocking traffic that include offering the user the option to bypass the block for certain sites after displaying a warning page and to reset the connection. Which solution should the organization choose?

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

Answer: C

NEW QUESTION 600

- (Exam Topic 3)

Which threat intelligence standard contains malware hashes?

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

Answer: C

NEW QUESTION 605

- (Exam Topic 2)

What is a prerequisite when integrating a Cisco ISE server and an AD domain?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 607

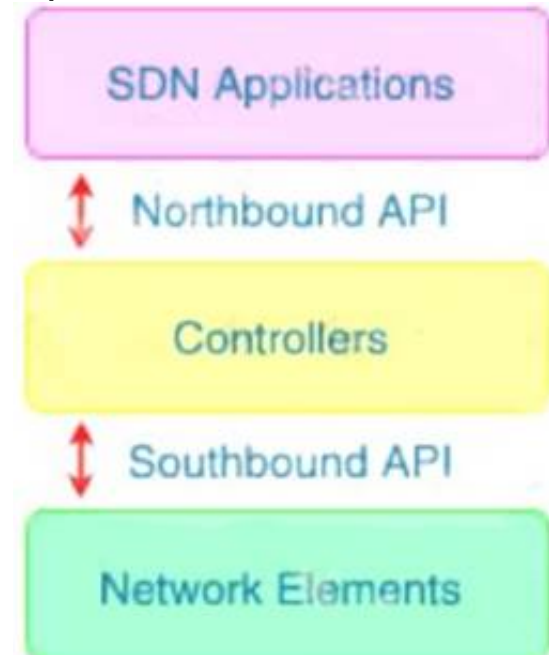
- (Exam Topic 2)

With which components does a southbound API within a software-defined network architecture communicate?

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

Answer: D

Explanation:



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

NEW QUESTION 608

- (Exam Topic 2)

A network administrator is configuring a rule in an access control policy to block certain URLs and selects the “Chat and Instant Messaging” category. Which reputation score should be selected to accomplish this goal?

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

Answer: D

Explanation:

We choose “Chat and Instant Messaging” category in “URL Category”:

Edit Action

Quarantine

Encrypt on Delivery

Strip Attachment by Content

Strip Attachment by File Info

URL Category

URL Reputation

Add Disclaimer Text

Bypass Outbreak Filter Scanning

Bypass DKIM Signing

Send Copy (Bcc:)

Notify

Change Recipient to

Send to Alternate Destination Host

Deliver from IP Interface

Strip Header

Add/Edit Header

Add Message Tag

Add Log Entry

S/MIME Sign/Encrypt on Delivery

Encrypt and Deliver Now (Final Action)

S/MIME Sign/Encrypt (Final Action)

Bounce (Final Action)

Skip Remaining Content Filters (Final Action)

Drop (Final Action)

URL Category

URL Category

Help

Does any URL in the message body or subject belong to one of the selected categories?

Available Categories:

Advertisements

Alcohol

Arts

Astrology

Auctions

Business and Industry

Chat and Instant Messagir

Cheating and Plagiarism

Computer Security

Computers and Internet

Add >

< Remove

Selected Categories:

Adult

Child Abuse Content

Illegal Activities

Illegal Downloads

Illegal Drugs

Use a URL whitelist: None : ?

Action on URL:

Defang URL ?

Redirect to Cisco Security Proxy ?

Replace URL with text message

Perform Action for:

All messages

Unsigned messages

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

Edit Condition

Message Body or Attachment

Message Body

URL Category

URL Reputation

Message Size

Attachment Content

Attachment File Info

Attachment Protection

Subject Header

Other Header

Envelope Sender

Envelope Recipient

Receiving Listener

Remote IP/Hostname

Reputation Score

URL Reputation

URL Reputation

What is the reputation of URL's in the message? This rule evaluates URL's using their Web Based Reputation Score (W

URL Reputation is:

Malicious (-10.0 to -6.0)

Suspect (-5.9 to 5.9)

Clean (6.0 to 10.0)

Custom Range (min to max)

No Score

Use a URL whitelist: None : ?

NEW QUESTION 610

- (Exam Topic 2)

Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats?

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

Answer: B

Explanation:

Reference: <https://talosintelligence.com/newsletters>

NEW QUESTION 614

- (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 617

- (Exam Topic 2)

Passing Certification Exams Made Easy

visit - <https://www.2PassEasy.com>

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

Install monitoring extension for AWS EC2	step 1
Restart the Machine Agent.	step 2
Update config.yaml.	step 3
Configure a Machine Agent or SIM Agent	step 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

NEW QUESTION 622

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 627

- (Exam Topic 2)

Which Cisco platform ensures that machines that connect to organizational networks have the recommended antivirus definitions and patches to help prevent an organizational malware outbreak?

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

Answer: C

Explanation:

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

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

Compliance Module **Any version**

* File Type ⓘ

* File Path ⓘ

* Operator

* File Version **10.0.10240.17318**

NEW QUESTION 628

- (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 632

- (Exam Topic 2)

Which risk is created when using an Internet browser to access cloud-based service?

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

Answer: D

NEW QUESTION 636

- (Exam Topic 2)

Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?

- A. Encrypted Traffic Analytics
- B. Threat Intelligence Director
- C. Cognitive Threat Analytics
- D. Cisco Talos Intelligence

Answer: B

NEW QUESTION 638

- (Exam Topic 2)

An organization has noticed an increase in malicious content downloads and wants to use Cisco Umbrella to prevent this activity for suspicious domains while allowing normal web traffic. Which action will accomplish this task?

- A. Set content settings to High
- B. Configure the intelligent proxy.
- C. Use destination block lists.
- D. Configure application block lists.

Answer: B

Explanation:

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

NEW QUESTION 639

- (Exam Topic 2)

Which Dos attack uses fragmented packets to crash a target machine?

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

Answer: C

Explanation:

A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due

to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

NEW QUESTION 641

- (Exam Topic 2)

What is the difference between Cross-site Scripting and SQL Injection, attacks?

- A. Cross-site Scripting is an attack where code is injected into a database, whereas SQL Injection is an attack where code is injected into a browser.
- B. Cross-site Scripting is a brute force attack targeting remote sites, whereas SQL Injection is a social engineering attack.
- C. Cross-site Scripting is when executives in a corporation are attacked, whereas SQL Injection is when a database is manipulated.
- D. Cross-site Scripting is an attack where code is executed from the server side, whereas SQL Injection is an attack where code is executed from the client side.

Answer: A

Explanation:

Answer B is not correct because Cross-site Scripting (XSS) is not a brute force attack. Answer C is not correct because the statement “Cross-site Scripting is when executives in a corporation are attacked” is not true. XSS is a client-side vulnerability that targets other application users. Answer D is not correct because the statement “Cross-site Scripting is an attack where code is executed from the server side”. In fact, XSS is a method that exploits website vulnerability by injecting scripts that will run at client’s side. Therefore only answer A is left. In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites where attackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POST parameters. Note: The main difference between a SQL and XSS injection attack is that SQL injection attacks are used to steal information from databases whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

NEW QUESTION 643

- (Exam Topic 2)

Drag and drop the NetFlow export formats from the left onto the descriptions on the right.

Version 1	appropriate only for the main cache
Version 5	introduced support for aggregation caches
Version 8	appropriate only for legacy systems
Version 9	introduced extensibility

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfgnflow-data-e>

NEW QUESTION 646

- (Exam Topic 2)

What is provided by the Secure Hash Algorithm in a VPN?

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

Answer: A

Explanation:

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

NEW QUESTION 647

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

350-701 Practice Exam Features:

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