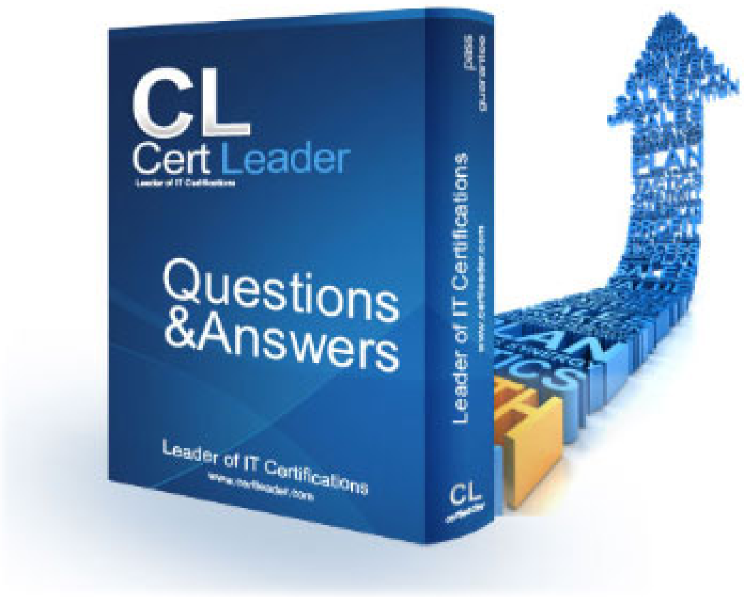
# 350-701 Dumps

# Implementing and Operating Cisco Security Core Technologies

https://www.certleader.com/350-701-dumps.html



**NEW QUESTION 1**
- (Exam Topic 3)
Which two capabilities does an MDM provide? (Choose two.)

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

**Answer:** BC

**NEW QUESTION 2**
- (Exam Topic 3)
What is a benefit of using GET VPN over FlexVPN within a VPN deployment?

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

**Answer:** B

**NEW QUESTION 3**
- (Exam Topic 3)
How does a cloud access security broker function?

A. It is an authentication broker to enable single sign-on and multi-factor authentication for a cloud solution
B. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution
C. It acts as a security information and event management solution and receives syslog from other cloud solutions.
D. It scans other cloud solutions being used within the network and identifies vulnerabilities

**Answer:** B

**NEW QUESTION 4**
- (Exam Topic 3)
What are two facts about WSA HTTP proxy configuration with a PAC file? (Choose two.)

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

**Answer:** CD

**NEW QUESTION 5**
- (Exam Topic 3)
Which two parameters are used for device compliance checks? (Choose two.)

A. endpoint protection software version
B. Windows registry values
C. DHCP snooping checks
D. DNS integrity checks
E. device operating system version

**Answer:** CE

**NEW QUESTION 6**
- (Exam Topic 3)
Which command is used to log all events to a destination colector 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 7**
- (Exam Topic 3)
An email administrator is setting up a new Cisco ESA. The administrator wants to enable the blocking of greymail for the end user. Which feature must the administrator enable first?

A. File Analysis

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

**Answer:** C

**NEW QUESTION 8**
- (Exam Topic 3)
An engineer musí set up 200 new laptops on a network and wants to prevent the users from moving their laptops around to simplify administration Which switch port MAC address security setting must be used?

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

**Answer:** A

**NEW QUESTION 9**
- (Exam Topic 3)
An administrator configures new authorization policies within Cisco ISE and has difficulty profiling the devices. Attributes for the new Cisco IP phones that are profiled based on the RADIUS authentication are seen however the attributes for CDP or DHCP are not. What should the administrator do to address this issue?

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

**Answer:** D

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

**NEW QUESTION 10**
- (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 10**
- (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 15**
- (Exam Topic 3)
Which MDM configuration provides scalability?

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

**Answer:** C

**NEW QUESTION 19**
- (Exam Topic 3)
An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation. What must be un solution?

A. L2TP is an IP packet encapsulation protocol, and GRE over IPsec is a tunneling protocol.
B. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701.
C. GRE over IPsec adds its own header, and L2TP does not.
D. GRE over IPsec cannot be used as a standalone protocol, and L2TP can.

**Answer:** D

**NEW QUESTION 23**
- (Exam Topic 3)
Which two authentication protocols are supported by the Cisco WSA? (Choose two.)

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

**Answer:** BE

**NEW QUESTION 25**
- (Exam Topic 3)
An administrator is establishing a new site-to-site VPN connection on a Cisco IOS router. The organization needs to ensure that the ISAKMP key on the hub is used only for terminating traffic from the IP address of 172.19.20.24. Which command on the hub will allow the administrator to accomplish this?

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

**Answer:** B

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

**NEW QUESTION 27**
- (Exam Topic 3)
Which posture assessment requirement provides options to the client for remediation and requires the remediation within a certain timeframe?

A. Audit
B. Mandatory
C. Optional
D. Visibility

**Answer:** B

**Explanation:**
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_client_posture_ Mandatory Requirements During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings

**NEW QUESTION 29**
- (Exam Topic 3)
Which solution allows an administrator to provision, monitor, and secure mobile devices on Windows and Mac computers from a centralized dashboard?

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

**Answer:** C

**NEW QUESTION 31**
- (Exam Topic 3)
Which Cisco Firewall solution requires zone definition?

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

**Answer:** C

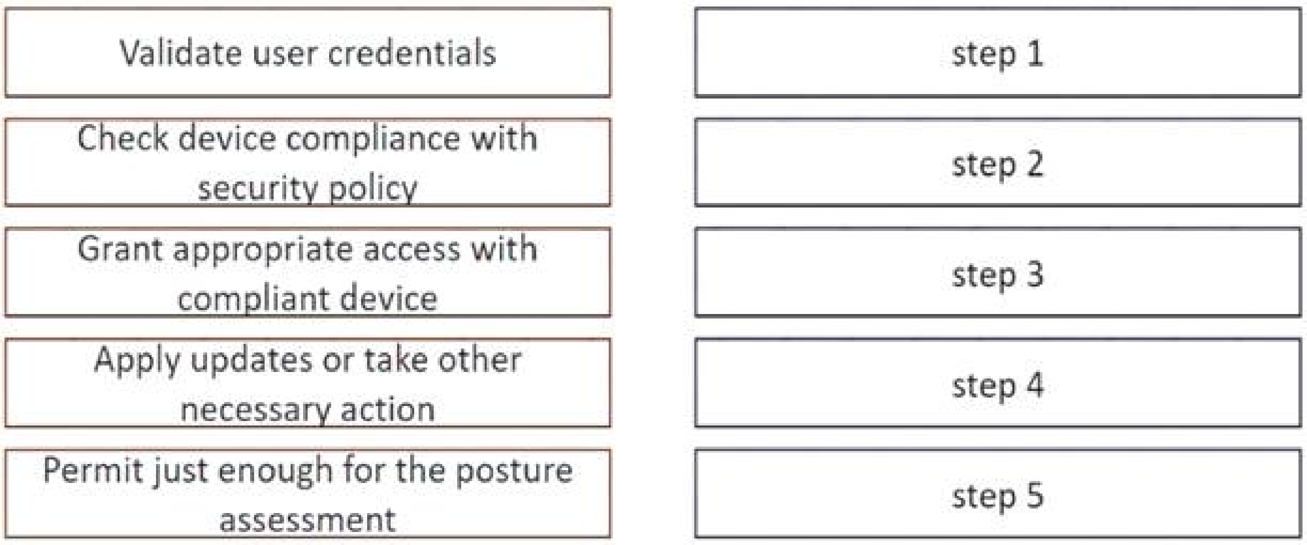
**NEW QUESTION 35**
- (Exam Topic 3)
What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?

A. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not
B. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA.

C. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA
D. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA

**Answer:** A

**NEW QUESTION 36**
- (Exam Topic 3)
Drag and drop the posture assessment flow actions from the left into a sequence on the right.

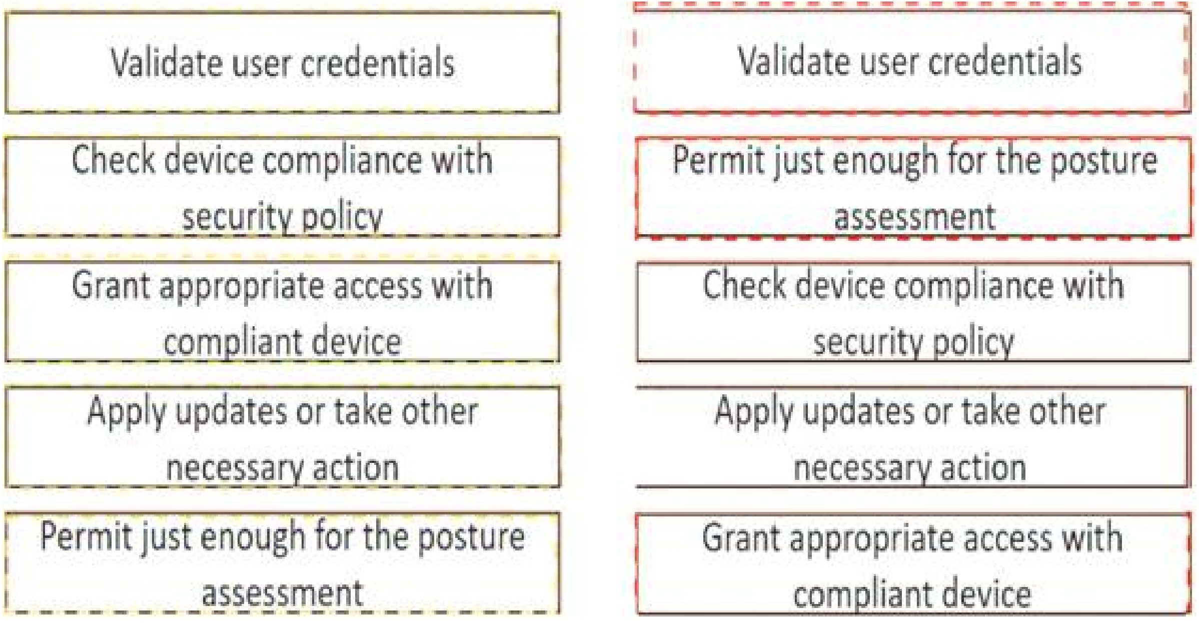


| | |
|---|---|
| Validate user credentials | step 1 |
| Check device compliance with security policy | step 2 |
| Grant appropriate access with compliant device | step 3 |
| Apply updates or take other necessary action | step 4 |
| Permit just enough for the posture assessment | step 5 |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**



| | |
|---|---|
| Validate user credentials | Validate user credentials |
| Check device compliance with security policy | Permit just enough for the posture assessment |
| Grant appropriate access with compliant device | Check device compliance with security policy |
| Apply updates or take other necessary action | Apply updates or take other necessary action |
| Permit just enough for the posture assessment | Grant appropriate access with compliant device |

**NEW QUESTION 37**
- (Exam Topic 3)
What are two functions of IKEv1 but not IKEv2? (Choose two)

A. NAT-T is supported in IKEv1 but rot in IKEv2.
B. With IKEv1, when using aggressive mode, the initiator and responder identities are passed cleartext
C. With IKEv1, mode negotiates faster than main mode
D. IKEv1 uses EAP authentication
E. IKEv1 conversations are initiated by the IKE_SA_INIT message

**Answer:** CE

**NEW QUESTION 42**
- (Exam Topic 3)
Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks? (Choose two.)

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

**Answer:** CE

**NEW QUESTION 44**
- (Exam Topic 3)
What are two security benefits of an MDM deployment? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 46**
- (Exam Topic 3)
An organization wants to provide visibility and to identify active threats in its network using a VM. The organization wants to extract metadata from network packet flow while ensuring that payloads are not retained or transferred outside the network. Which solution meets these requirements?

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

**Answer:** B

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

**NEW QUESTION 50**
- (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 53**
- (Exam Topic 3)
Which kind of API that is used with Cisco DNA Center provisions SSIDs, QoS policies, and update software versions on switches?

A. Integration
B. Intent
C. Event
D. Multivendor

**Answer:** B

**NEW QUESTION 55**
- (Exam Topic 3)
Email security has become a high priority task for a security engineer at a large multi-national organization due to ongoing phishing campaigns. To help control this, the engineer has deployed an Incoming Content Filter with a URL reputation of (-10 00 to -6 00) on the Cisco ESA Which action will the system perform to disable any links in messages that match the filter?

A. Defang
B. Quarantine
C. FilterAction
D. ScreenAction

**Answer:** B

**Explanation:**
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/esa-content-filters.pdf

**NEW QUESTION 58**
- (Exam Topic 3)
Refer to the exhibit. When creating an access rule for URL filtering, a network engineer adds certain categories and individual URLs to block. What is the result of the configuration?

A. Only URLs for botnets with reputation scores of 1-3 will be blocked.
B. Only URLs for botnets with a reputation score of 3 will be blocked.
C. Only URLs for botnets with reputation scores of 3-5 will be blocked.
D. Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked.

**Answer:** A

**NEW QUESTION 63**
- (Exam Topic 3)
How does the Cisco WSA enforce bandwidth restrictions for web applications?

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

**Answer:** C

**NEW QUESTION 65**
- (Exam Topic 3)
A customer has various external HTTP resources available including Intranet Extranet and Internet, with a proxy configuration running in explicit mode. Which method allows the client desktop browsers to be
configured
to select when to connect direct or when to use the proxy?

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

**Answer:** C

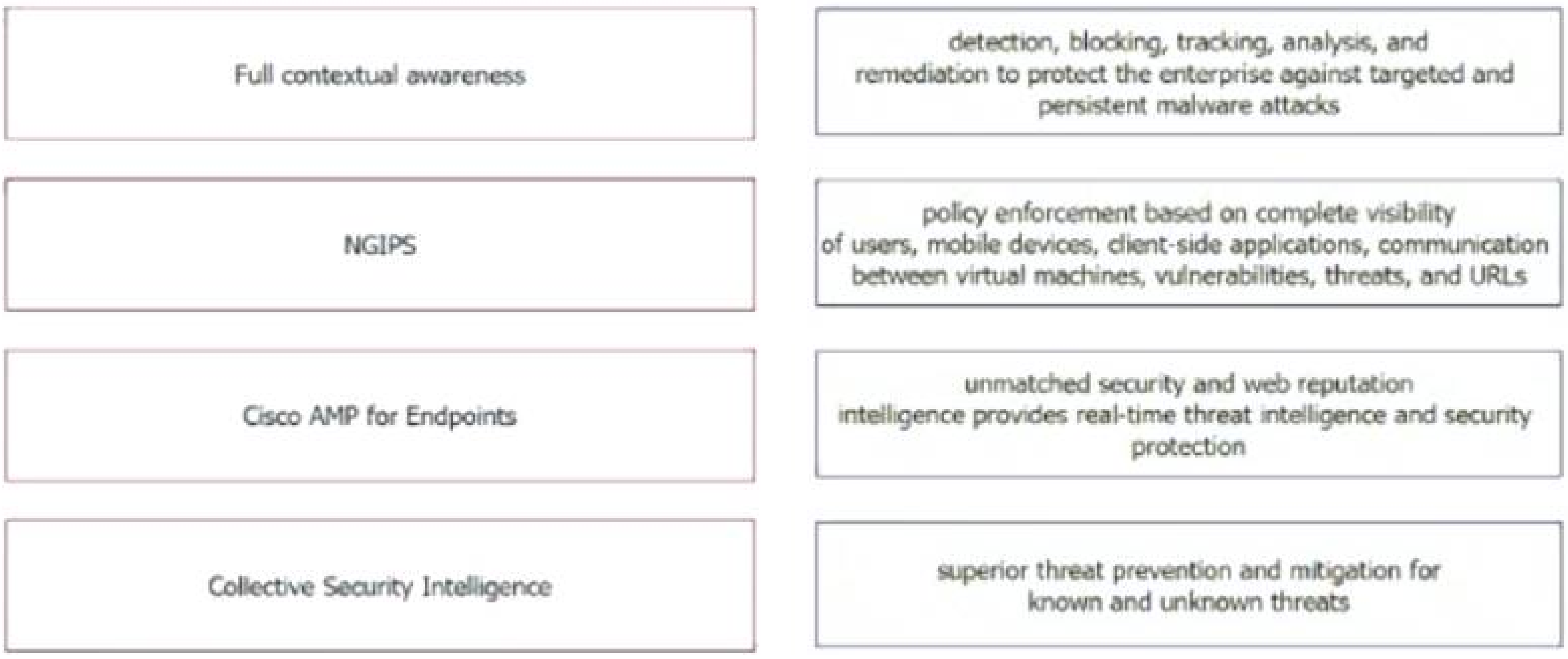
**Explanation:**
A Proxy Auto-Configuration (PAC) file is a JavaScript function definition that determines whether web browserrequests (HTTP, HTTPS, and FTP) go direct to the destination or are forwarded to a web proxy server.PAC files are used to support explicit proxy deployments in which client browsers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

**NEW QUESTION 66**
- (Exam Topic 3)
An engineer is configuring Cisco WSA and needs to deploy it in transparent mode. Which configuration component must be used to accomplish this goal?

A. MDA on the router
B. PBR on Cisco WSA
C. WCCP on switch
D. DNS resolution on Cisco WSA

**Answer:** C

**NEW QUESTION 71**
- (Exam Topic 3)
Drag and drop the security solutions from the left onto the benefits they provide on the right.



Full contextual awareness

NGIPS

Cisco AMP for Endpoints

Collective Security Intelligence

detection, blocking, tracking, analysis, and remediation to protect the enterprise against targeted and persistent malware attacks

policy enforcement based on complete visibility of users, mobile devices, client-side applications, communication between virtual machines, vulnerabilities, threats, and URLs

unmatched security and web reputation intelligence provides real-time threat intelligence and security protection

superior threat prevention and mitigation for known and unknown threats

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Diagram Description automatically generated

**NEW QUESTION 73**
- (Exam Topic 3)
A small organization needs to reduce the VPN bandwidth load on their headend Cisco ASA in order to
ensure that bandwidth is available for VPN users needing access to corporate resources on the10.0.0.0/24 local HQ network. How is this accomplished without adding additional devices to the
network?

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

**Answer:** A

**NEW QUESTION 75**
- (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 79**
- (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 82**
- (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

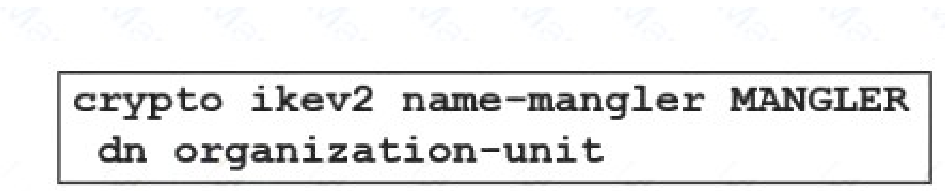
**Answer:** C

**NEW QUESTION 83**
- (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 86**
- (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 88**
- (Exam Topic 3)
Which two Cisco ISE components must be configured for BYOD? (Choose two.)

A. local WebAuth
B. central WebAuth
C. null WebAuth
D. guest
E. dual

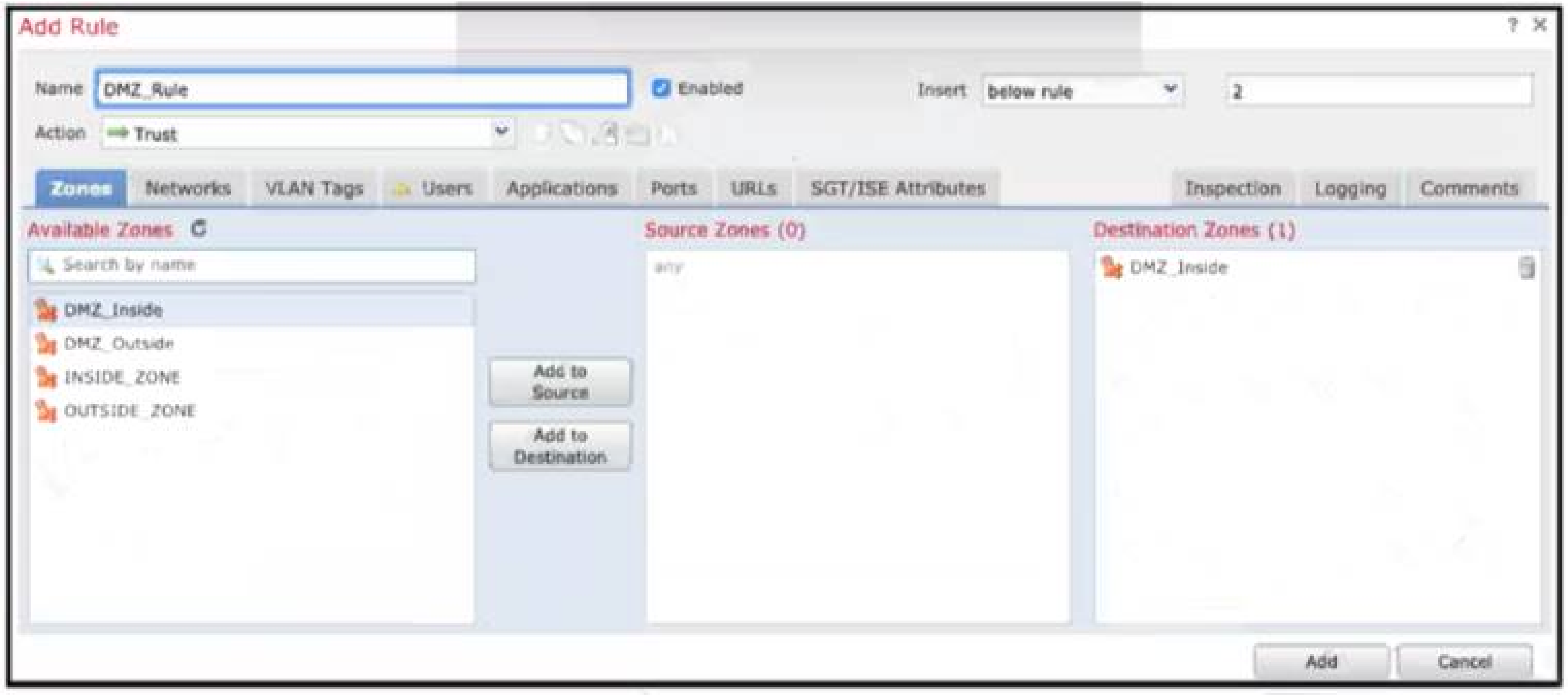
**Answer:** BD

**NEW QUESTION 92**
- (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 96**
- (Exam Topic 3)



Add Rule

Name: DMZ_Rule ☑ Enabled Insert: below rule 2

Action: Trust

Available Zones: DMZ_Inside, DMZ_Outside, INSIDE_ZONE, OUTSIDE_ZONE

Source Zones (0): any

Destination Zones (1): DMZ_Inside

Refer to the exhibit When configuring this access control rule in Cisco FMC, what happens with the traffic destined to the DMZjnside zone once the configuration is deployed?

A. All traffic from any zone to the DMZ_inside zone will be permitted with no further inspection
B. No traffic will be allowed through to the DMZ_inside zone regardless of if it's trusted or not
C. All traffic from any zone will be allowed to the DMZ_inside zone only after inspection
D. No traffic will be allowed through to the DMZ_inside zone unless it's already trusted

**Answer:** A

**NEW QUESTION 101**
- (Exam Topic 3)
What is the most common type of data exfiltration that organizations currently experience?

A. HTTPS file upload site
B. Microsoft Windows network shares
C. SQL database injections
D. encrypted SMTP

**Answer:** B

**Explanation:**
Reference: https://blogs.cisco.com/security/sensitive-data-exfiltration-and-the-insider

**NEW QUESTION 106**
- (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 111**
- (Exam Topic 2)
An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?

A. Cisco Umbrella
B. Cisco Cloud Email Security
C. Cisco NGFW
D. Cisco Cloudlock

**Answer:** D

**Explanation:**
Reference:
https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/at-a-glance-c45- 738565.pdf

**NEW QUESTION 116**
- (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 119**
- (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 123**
- (Exam Topic 2)
An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?

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

**Answer:** B

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

**NEW QUESTION 128**
- (Exam Topic 2)
A switch with Dynamic ARP Inspection enabled has received a spoofed ARP response on a trusted interface. How does the switch behave in this situation?

A. It forwards the packet after validation by using the MAC Binding Table.
B. It drops the packet after validation by using the IP & MAC Binding Table.
C. It forwards the packet without validation.
D. It drops the packet without validation.

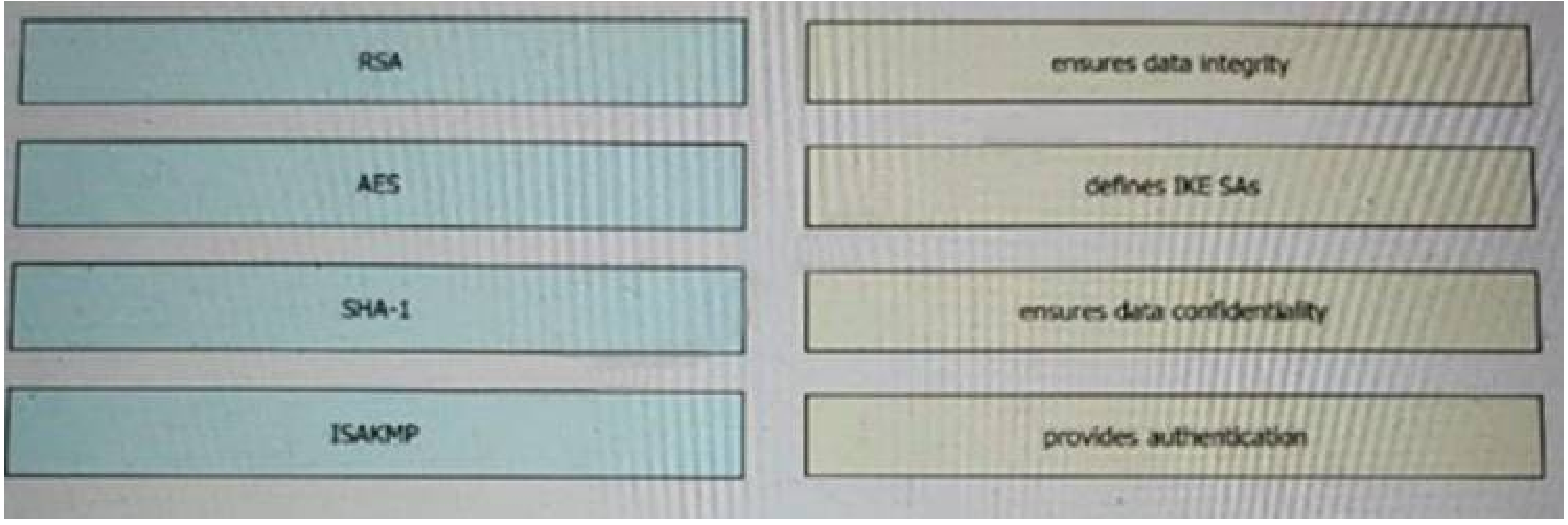
**Answer:** B

**NEW QUESTION 132**
- (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 135**
- (Exam Topic 2)
Drag and drop the VPN functions from the left onto the description on the right.

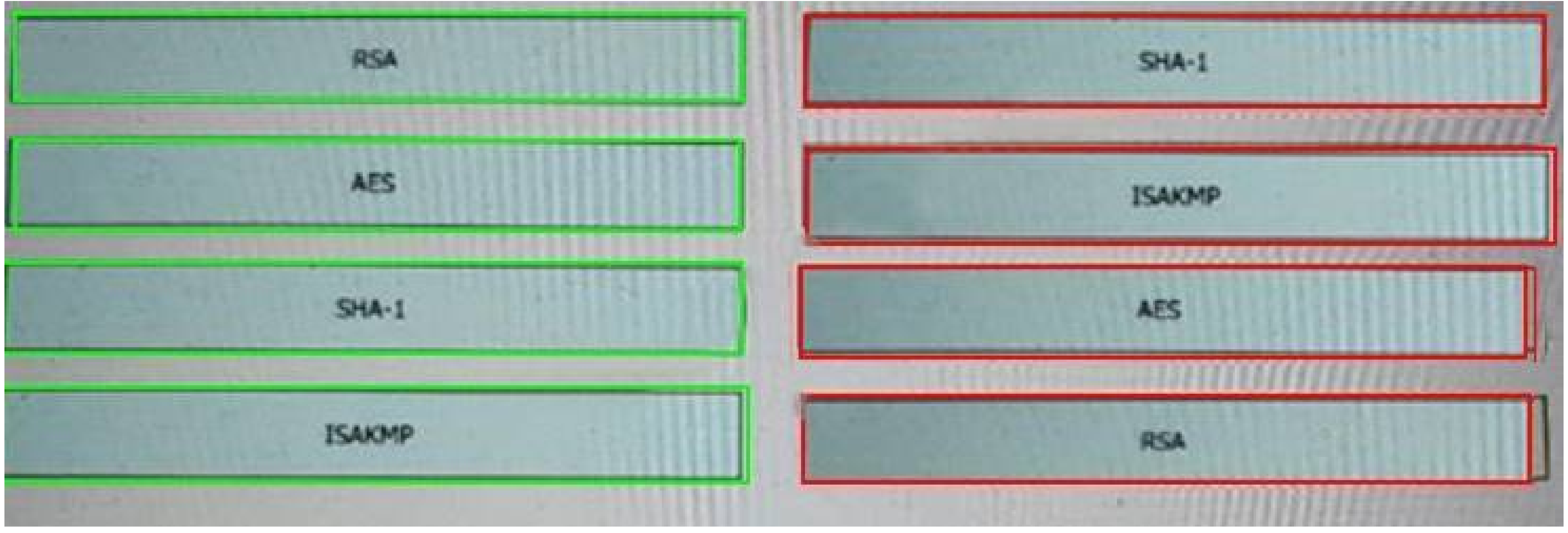


| | |
|---|---|
| RSA | ensures data integrity |
| AES | defines IKE SAs |
| SHA-1 | ensures data confidentiality |
| ISAKMP | provides authentication |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**



| | |
|---|---|
| RSA | SHA-1 |
| AES | ISAKMP |
| SHA-1 | AES |
| ISAKMP | RSA |

**NEW QUESTION 137**
- (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 140**
- (Exam Topic 2)
An organization has a Cisco Stealthwatch Cloud deployment in their environment. Cloud logging is working as expected, but logs are not being received from the on-premise network, what action will resolve this issue?

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

C. Deploy a Cisco FTD sensor to send events to Cisco Stealthwatch Cloud
D. Deploy a Cisco Stealthwatch Cloud sensor on the network to send data to Cisco Stealthwatch Cloud

**Answer:** D

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

**NEW QUESTION 144**
- (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 145**
- (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

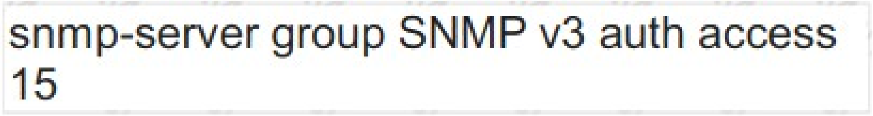
**NEW QUESTION 149**
- (Exam Topic 1)
What is the primary benefit of deploying an ESA in hybrid mode?

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

**Answer:** D

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

**NEW QUESTION 151**
- (Exam Topic 1)
Refer to the exhibit.



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

What does the number 15 represent in this configuration?

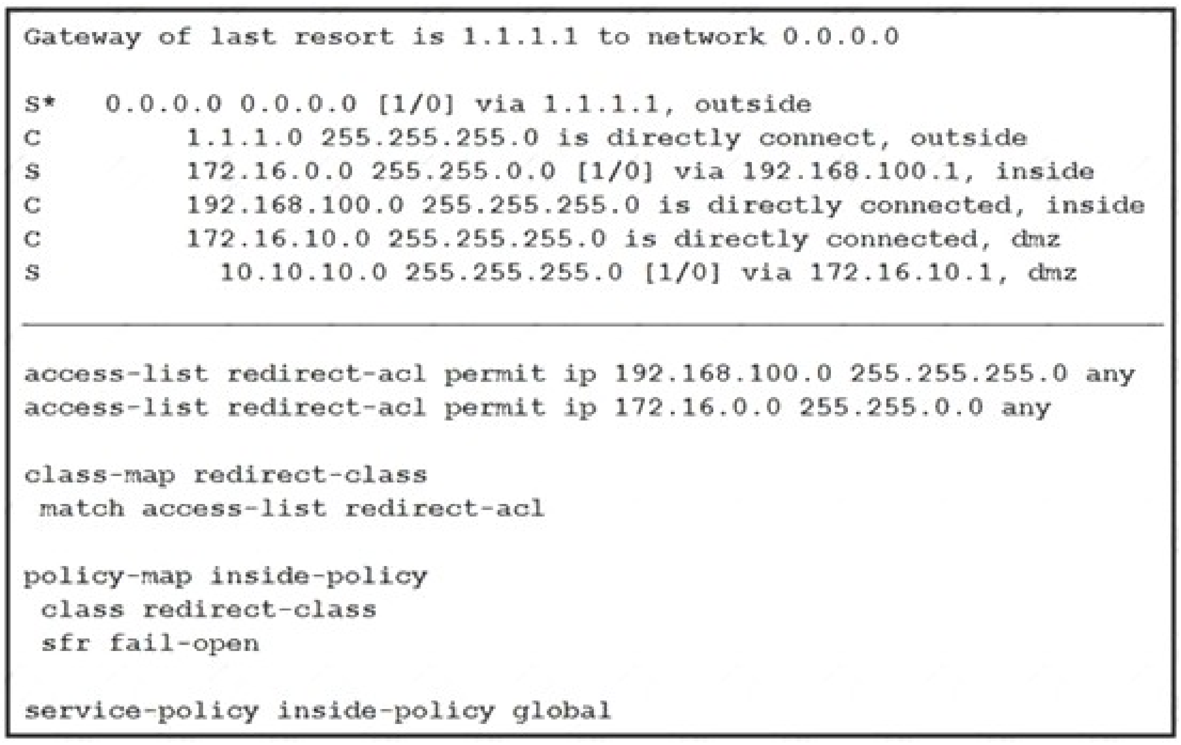
A. privilege level for an authorized user to this router
B. access list that identifies the SNMP devices that can access the router
C. interval in seconds between SNMPv3 authentication attempts
D. number of possible failed attempts until the SNMPv3 user is locked out

**Answer:** B

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

**NEW QUESTION 155**

- (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
```

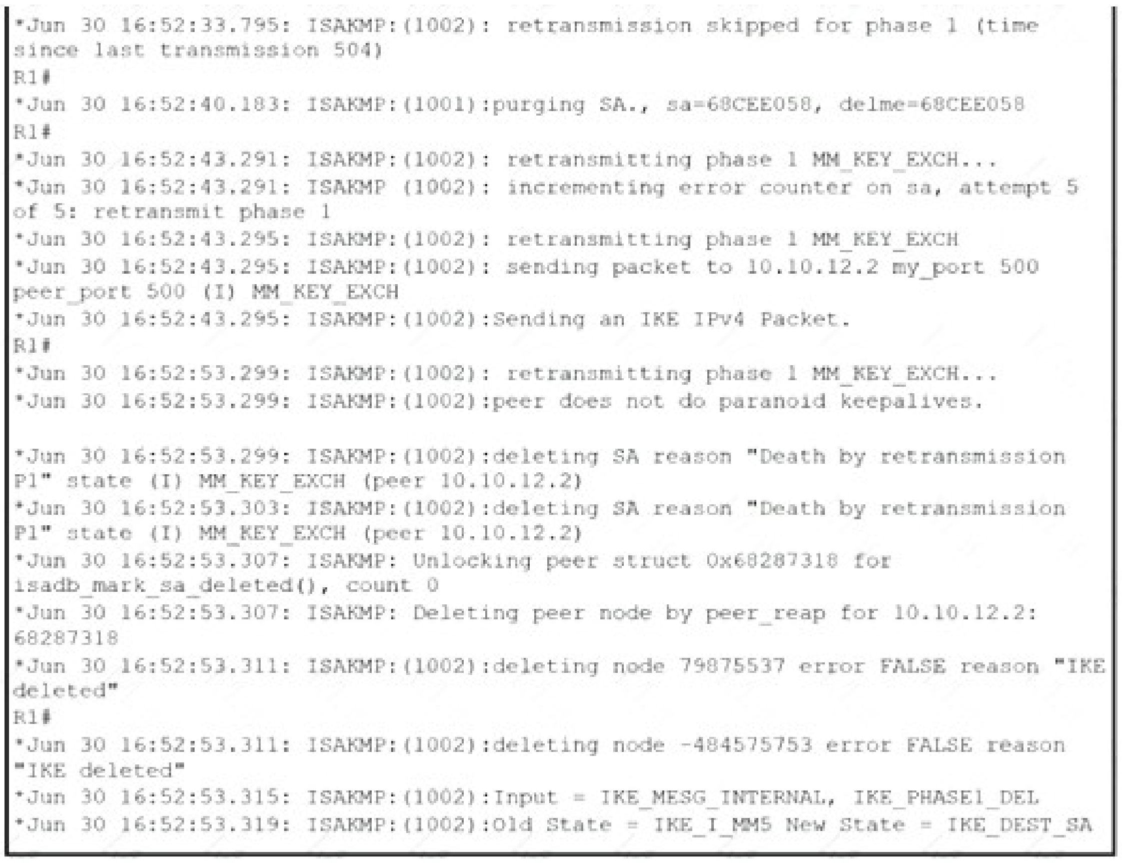
What is a result of the configuration?

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 157**
- (Exam Topic 1)
Refer to the exhibit.



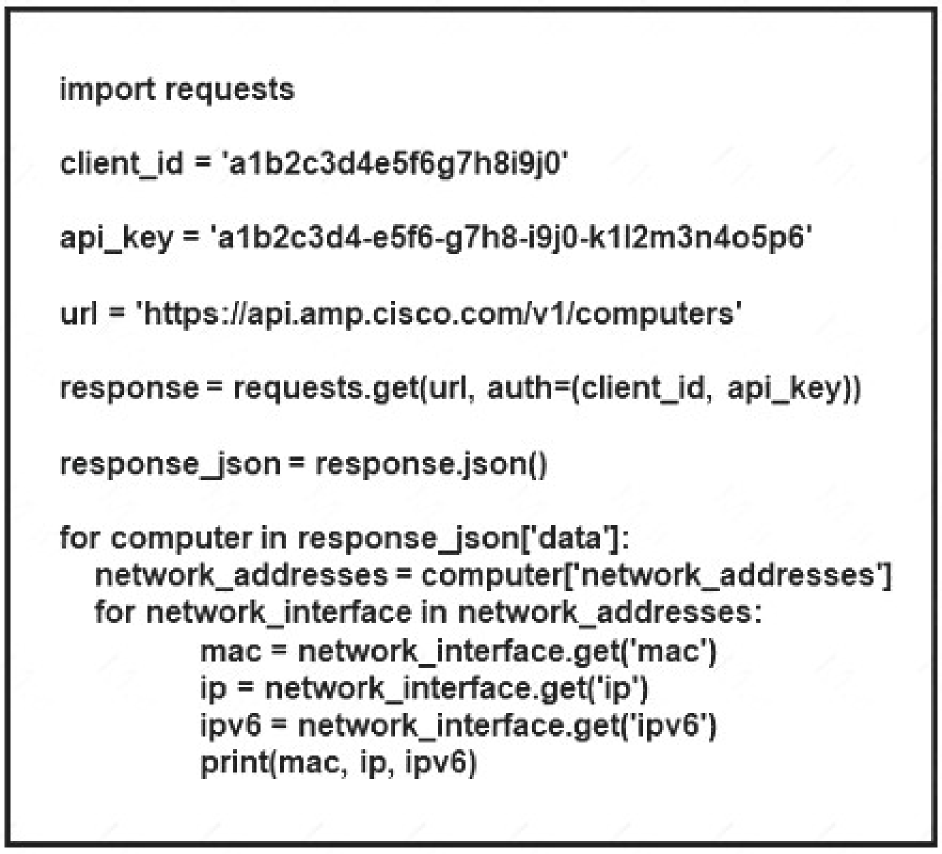
```
*Jun 30 16:52:33.795: ISAKMP:(1002): retransmission skipped for phase 1 (time
since last transmission 504)
R1#
*Jun 30 16:52:40.183: ISAKMP:(1001):purging SA., sa=68CEE058, delme=68CEE058
R1#
*Jun 30 16:52:43.291: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:43.291: ISAKMP (1002): incrementing error counter on sa, attempt 5
of 5: retransmit phase 1
*Jun 30 16:52:43.295: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002): sending packet to 10.10.12.2 my_port 500
peer_port 500 (I) MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP:(1002):Sending an IKE IPv4 Packet.
R1#
*Jun 30 16:52:53.299: ISAKMP:(1002): retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:53.299: ISAKMP:(1002):peer does not do paranoid keepalives.

*Jun 30 16:52:53.299: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.303: ISAKMP:(1002):deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.307: ISAKMP: Unlocking peer struct 0x68287318 for
isadb_mark_sa_deleted(), count 0
*Jun 30 16:52:53.307: ISAKMP: Deleting peer node by peer_reap for 10.10.12.2:
68287318
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node 79875537 error FALSE reason "IKE
deleted"
R1#
*Jun 30 16:52:53.311: ISAKMP:(1002):deleting node -484575753 error FALSE reason
"IKE deleted"
*Jun 30 16:52:53.315: ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL
*Jun 30 16:52:53.319: ISAKMP:(1002):Old State = IKE_I_MM5 New State = IKE_DEST_SA
```

A network administrator configured a site-to-site VPN tunnel between two Cisco IOS routers, and hosts are unable to communicate between two sites of VPN. The network administrator runs the debug crypto isakmp sa command to track VPN status. What is the problem according to this command output?

A. hashing algorithm mismatch
B. encryption algorithm mismatch
C. authentication key mismatch
D. interesting traffic was not applied

**Answer:** C

**NEW QUESTION 158**
- (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 160**
- (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 DNSqueries and responses. DNS tunneling often includes data payloads that can be added to an attacked DNSserver and used to control a remote server and applications.

**NEW QUESTION 164**
- (Exam Topic 1)
Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?

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

**Answer:** D

**NEW QUESTION 165**
- (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 167**
- (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 169**
- (Exam Topic 1)
Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two)

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

**Answer:** BE

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

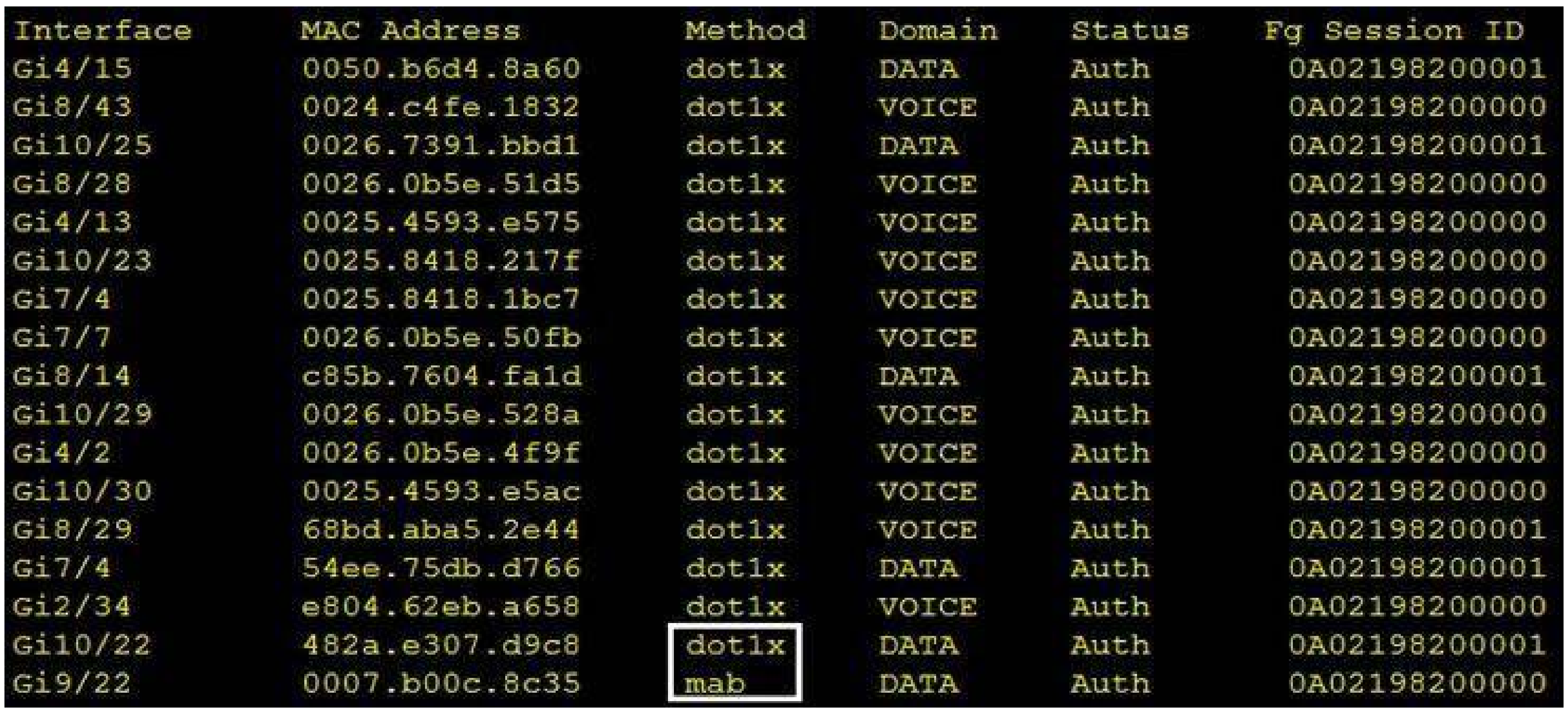
**NEW QUESTION 173**
- (Exam Topic 1)
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)

A. Patch for cross-site scripting.
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.
D. Install a spam and virus email filter.
E. Protect systems with an up-to-date antimalware program

**Answer:** DE

**Explanation:**
Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputablesource. It is usually done through email. The goal is to steal sensitive data like credit card and login information,or to install malware on the victim’s machine.

**NEW QUESTION 176**
- (Exam Topic 1)
Refer to the exhibit.



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

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

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

**Answer:** D

**Explanation:**
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-c Displaying the Summary of All Auth Manager Sessions on the Switch
Enter the following:
Switch# show authentication sessions
Interface MAC Address Method Domain Status Session ID

Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58
Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94

**NEW QUESTION 180**
- (Exam Topic 1)
Which two mechanisms are used to control phishing attacks? (Choose two)

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

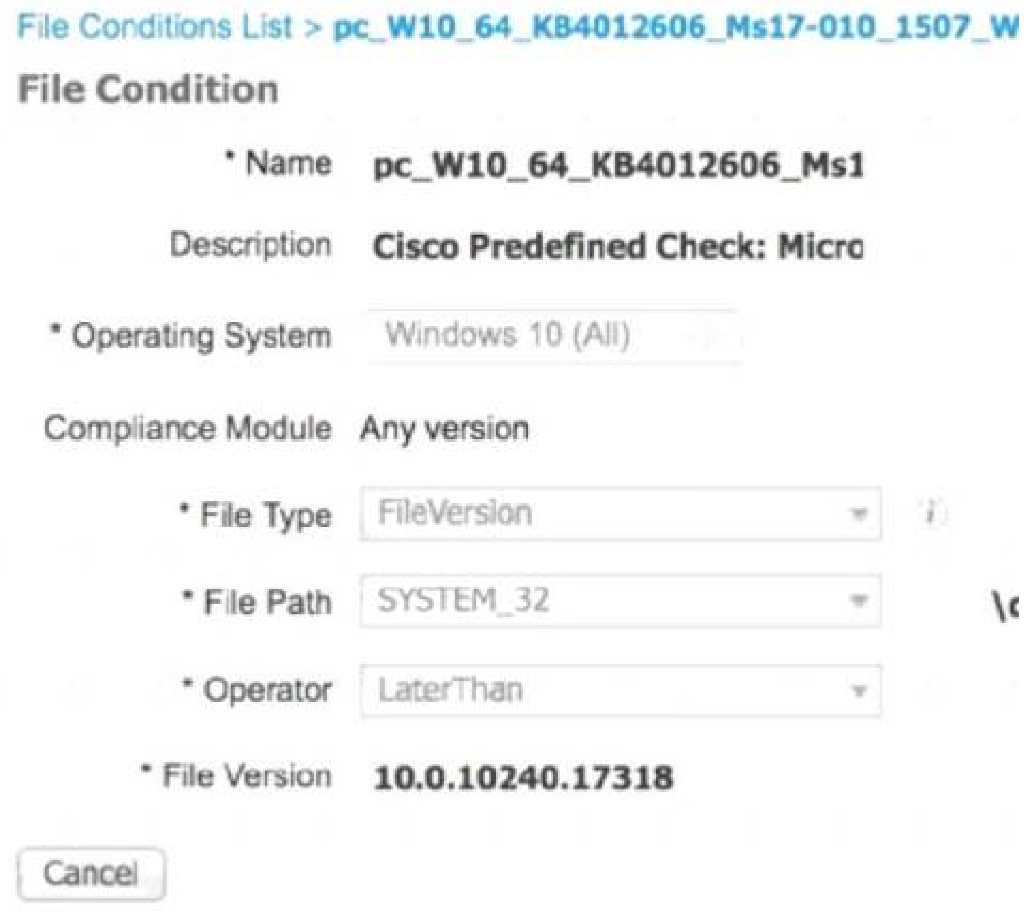
**Answer:** AE

**NEW QUESTION 184**
- (Exam Topic 1)
An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch was not installed, which left the endpoint vulnerable to WannaCry ransomware. Which two solutions mitigate the risk of this ransom ware infection? (Choose two)

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

**Answer:** AC

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


File Conditions List > pc_W10_64_KB4012606_Ms17-010_1507_W

File Condition

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

**NEW QUESTION 186**
- (Exam Topic 1)
When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?

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

**Answer:** B

**Explanation:**
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Refere Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload
thewhole file. Dynamic analysis sends files to AMP ThreatGrid.Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco ThreatGrid runs the file in a sandbox environment, analyzes the file’s behavior to determine whether the file ismalicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threatscore, you can view a dynamic analysis summary report with the reasons for the assigned threat score.

Youcan also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well asscrubbed reports with limited data for files that your organization did not submit.Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, andother types of files for the most common types of malware, using a detection rule set provided by the CiscoTalos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud,and does not run the file, local malware analysis saves time and system resources. -> Malware analysis doesnot upload files to anywhere, it only checks the files locally.There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in avirtual machine.

**NEW QUESTION 188**
- (Exam Topic 1)
Which Cisco AMP file disposition valid?

A. pristine
B. malware
C. dirty
D. non malicious

**Answer:** B

**NEW QUESTION 192**
- (Exam Topic 1)
Which benefit does endpoint security provide the overall security posture of an organization?

A. It streamlines the incident response process to automatically perform digital forensics on the endpoint.
B. It allows the organization to mitigate web-based attacks as long as the user is active in the domain.
C. It allows the organization to detect and respond to threats at the edge of the network.
D. It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.

**Answer:** D

**NEW QUESTION 194**
- (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 196**
- (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

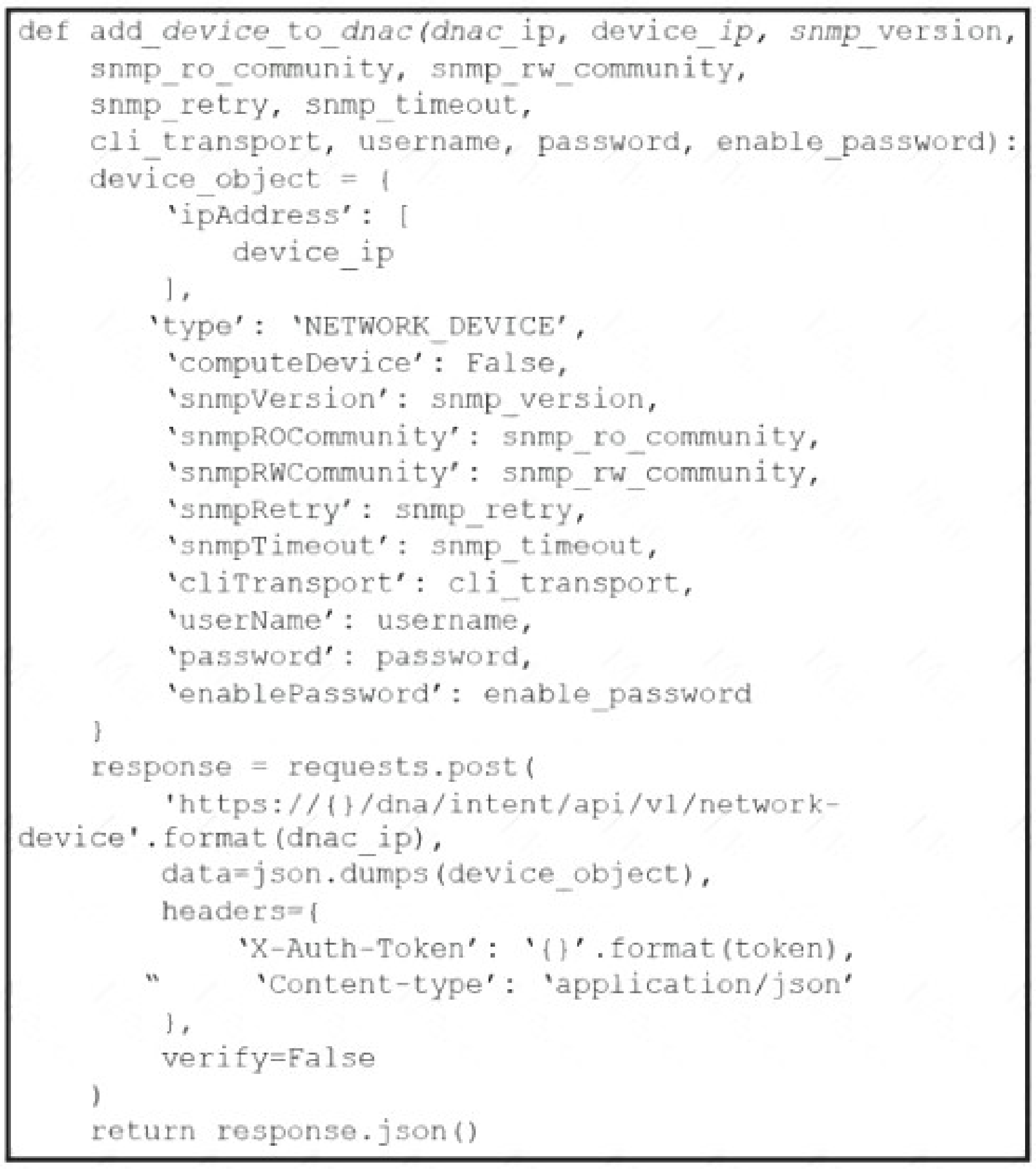
**Answer:** D

**NEW QUESTION 200**
- (Exam Topic 1)
A malicious user gained network access by spoofing printer connections that were authorized using MAB on four different switch ports at the same time. What two catalyst switch security features will prevent further violations? (Choose two)

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

**Answer:** AE

**NEW QUESTION 205**
- (Exam Topic 1)
Refer to the exhibit.



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

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

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

**Answer:** B

**NEW QUESTION 207**
- (Exam Topic 1)
Which two activities can be done using Cisco DNA Center? (Choose two)

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

**Answer:** BE

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

**NEW QUESTION 208**
- (Exam Topic 1)
Which two preventive measures are used to control cross-site scripting? (Choose two)

A. Enable client-side scripts on a per-domain basis.
B. Incorporate contextual output encoding/escaping.
C. Disable cookie inspection in the HTML inspection engine.
D. Run untrusted HTML input through an HTML sanitization engine.
E. Same Site cookie attribute should not be used.

**Answer:** AB

**NEW QUESTION 211**
- (Exam Topic 1)
How is ICMP used an exfiltration technique?

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

**Answer:** C

**NEW QUESTION 216**
- (Exam Topic 1)
What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?

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

**Answer:** A

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

**NEW QUESTION 221**
- (Exam Topic 1)
How is Cisco Umbrella configured to log only security events?

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

**Answer:** A

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

**NEW QUESTION 226**
- (Exam Topic 1)
Which two conditions are prerequisites for stateful failover for IPsec? (Choose two)

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

**Answer:** CE

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

**NEW QUESTION 229**
- (Exam Topic 1)
The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

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

**Answer:** D

**NEW QUESTION 233**
- (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 238**
- (Exam Topic 3)
Which feature enables a Cisco ISR to use the default bypass list automatically for web filtering?

A. filters
B. group key
C. company key
D. connector

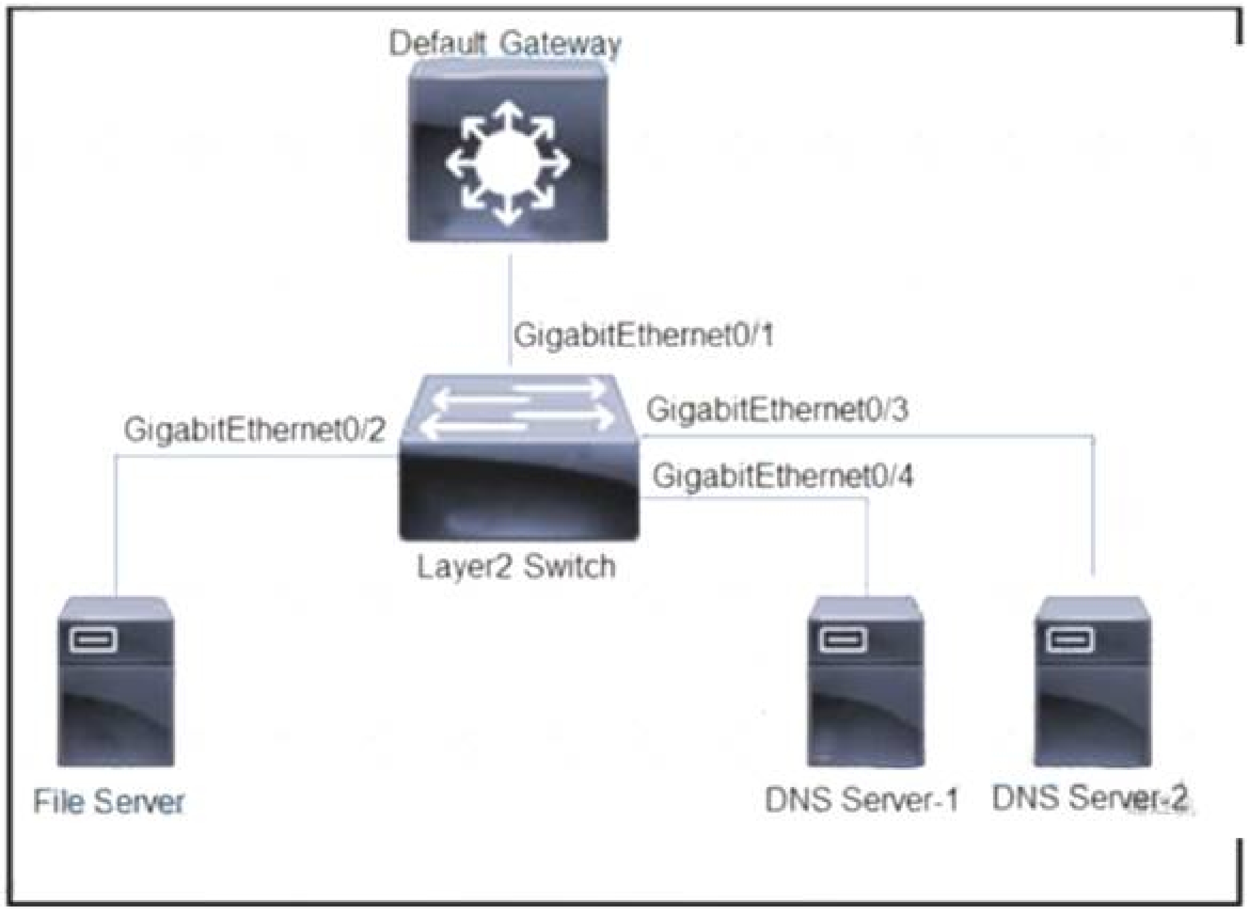
**Answer:** D

**NEW QUESTION 241**
- (Exam Topic 3)
An administrator enables Cisco Threat Intelligence Director on a Cisco FMC. Which process uses STIX and allows uploads and downloads of block lists?

A. consumption
B. sharing
C. editing
D. authoring

**Answer:** A

**NEW QUESTION 245**
- (Exam Topic 3)



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

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

**Answer:** C

**NEW QUESTION 246**
- (Exam Topic 3)
Which system performs compliance checks and remote wiping?

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

**Answer:** A

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

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

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

**Answer:** A

**NEW QUESTION 254**
- (Exam Topic 3)
What are two benefits of using Cisco Duo as an MFA solution? (Choose two.)

A. grants administrators a way to remotely wipe a lost or stolen device
B. provides simple and streamlined login experience for multiple applications and users
C. native integration that helps secure applications across multiple cloud platforms or on-premises environments
D. encrypts data that is stored on endpoints
E. allows for centralized management of endpoint device applications and configurations

**Answer:** BC

**NEW QUESTION 257**
- (Exam Topic 3)
What are two characteristics of the RESTful architecture used within Cisco DNA Center? (Choose two.)

A. REST uses methods such as GET, PUT, POST, and DELETE.
B. REST codes can be compiled with any programming language.
C. REST is a Linux platform-based architecture.
D. The POST action replaces existing data at the URL path.
E. REST uses HTTP to send a request to a web service.

**Answer:** AE

**NEW QUESTION 260**
- (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 263**
- (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 266**
- (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 269**
- (Exam Topic 3)
Which type of data does the Cisco Stealthwatch system collect and analyze from routers, switches, and firewalls?

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

**Answer:** D

**NEW QUESTION 271**

- (Exam Topic 3)
What are two functions of TAXII in threat intelligence sharing? (Choose two.)

A. determines the "what" of threat intelligence
B. Supports STIX information
C. allows users to describe threat motivations and abilities
D. exchanges trusted anomaly intelligence information
E. determines how threat intelligence information is relayed

**Answer:** BE

**NEW QUESTION 274**
- (Exam Topic 3)
Which solution stops unauthorized access to the system if a user's password is compromised?

A. VPN
B. MFA
C. AMP
D. SSL

**Answer:** B

**NEW QUESTION 278**
- (Exam Topic 3)
What is the result of the ACME-Router(config)#login block-for 100 attempts 4 within 60 command on a Cisco IOS router?

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

**Answer:** D

**NEW QUESTION 279**
- (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. userSudiSerlalNos and deviceInfo
C. POST and name
D. lastSyncTime and pid

**Answer:** A

**NEW QUESTION 281**
- (Exam Topic 3)
What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?

A. trusted automated exchange
B. Indicators of Compromise
C. The Exploit Database
D. threat intelligence

**Answer:** D

**NEW QUESTION 285**
- (Exam Topic 3)
A network administrator is configuring a role in an access control policy to block certain URLs and selects the "Chat and instant Messaging" category. which reputation score should be selected to accomplish
this goal?

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

**Answer:** C

**NEW QUESTION 288**
- (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

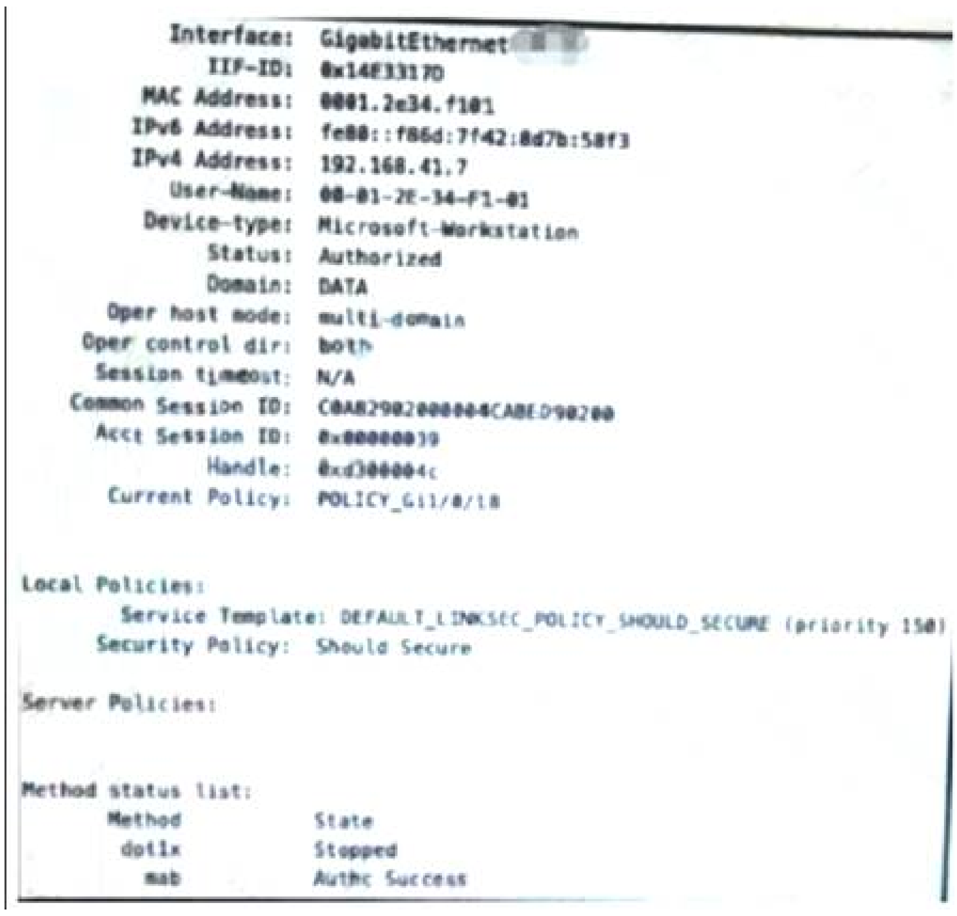
**Answer:** D

**NEW QUESTION 292**
- (Exam Topic 3)
Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using higher-level protocols without readdressing the network?

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

**Answer:** B

**NEW QUESTION 297**
- (Exam Topic 3)
Refer to the exhibit.



```
           Interface:  GigabitEthernet[redacted]
              IIF-ID:  0x14F3317D
         MAC Address:  0001.2e34.f101
        IPv6 Address:  fe80::f86d:7f42:8d7b:58f3
        IPv4 Address:  192.168.41.7
           User-Name:  00-01-2E-34-F1-01
         Device-type:  Microsoft-Workstation
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  C0A82902000004CABED90200
     Acct Session ID:  0x00000039
              Handle:  0xd300004c
      Current Policy:  POLICY_Gi1/0/18


Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure

Server Policies:


Method status list:
       Method           State
        dot1x           Stopped
          mab           Authc Success
```

Which configuration item makes it possible to have the AAA session on the network?

A. aaa authentication login console ise
B. aaa authentication enable default enable
C. aaa authorization network default group ise
D. aaa authorization exec default ise

**Answer:** C

**NEW QUESTION 300**
- (Exam Topic 3)
Which DoS attack uses fragmented packets in an attempt to crash a target machine?

A. teardrop
B. smurf
C. LAND
D. SYN flood

**Answer:** A

**Explanation:**
Reference: https://www.radware.com/security/ddos-knowledge-center/ddospedia/teardrop-attack/

**NEW QUESTION 303**
- (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 305**
- (Exam Topic 3)

A network engineer has configured a NTP server on a Cisco ASA. The Cisco ASA has IP reachability to the NTP server and is not filtering any traffic. The show ntp association detail command indicates that the configured NTP server is unsynchronized and has a stratum of 16. What is the cause of this issue?

A. Resynchronization of NTP is not forced
B. NTP is not configured to use a working server.
C. An access list entry for UDP port 123 on the inside interface is missing.
D. An access list entry for UDP port 123 on the outside interface is missing.

**Answer:** B

**NEW QUESTION 310**
- (Exam Topic 3)
What is a description of microsegmentation?

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

**Answer:** A

**NEW QUESTION 313**
- (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 315**
- (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 320**
- (Exam Topic 3)
An engineer is configuring Cisco Umbrella and has an identity that references two different policies. Which action ensures that the policy that the identity must use takes precedence over the second one?

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

**Answer:** D

**NEW QUESTION 324**
- (Exam Topic 3)
Which two actions does the Cisco identity Services Engine posture module provide that ensures endpoint security?(Choose two.)

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

**Answer:** AD

**NEW QUESTION 328**
- (Exam Topic 3)
What are two benefits of using an MDM solution? (Choose two.)

A. grants administrators a way to remotely wipe a lost or stolen device
B. provides simple and streamlined login experience for multiple applications and users
C. native integration that helps secure applications across multiple cloud platforms or on-premises environments
D. encrypts data that is stored on endpoints
E. allows for centralized management of endpoint device applications and configurations

**Answer:** AE

**NEW QUESTION 329**
- (Exam Topic 3)
Which endpoint protection and detection feature performs correlation of telemetry, files, and intrusion events that are flagged as possible active breaches?

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

**Answer:** B

**NEW QUESTION 334**
- (Exam Topic 3)
Which VMware platform does Cisco ACI integrate with to provide enhanced visibility, provide policy integration and deployment, and implement security policies with access lists?

A. VMware APIC
B. VMwarevRealize
C. VMware fusion
D. VMware horizons

**Answer:** B

**NEW QUESTION 336**
- (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 339**
- (Exam Topic 3)
Which category includes DoS Attacks?

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

**Answer:** C

**NEW QUESTION 343**
- (Exam Topic 3)
What is the difference between a vulnerability and an exploit?

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

**Answer:** B

**NEW QUESTION 348**
- (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

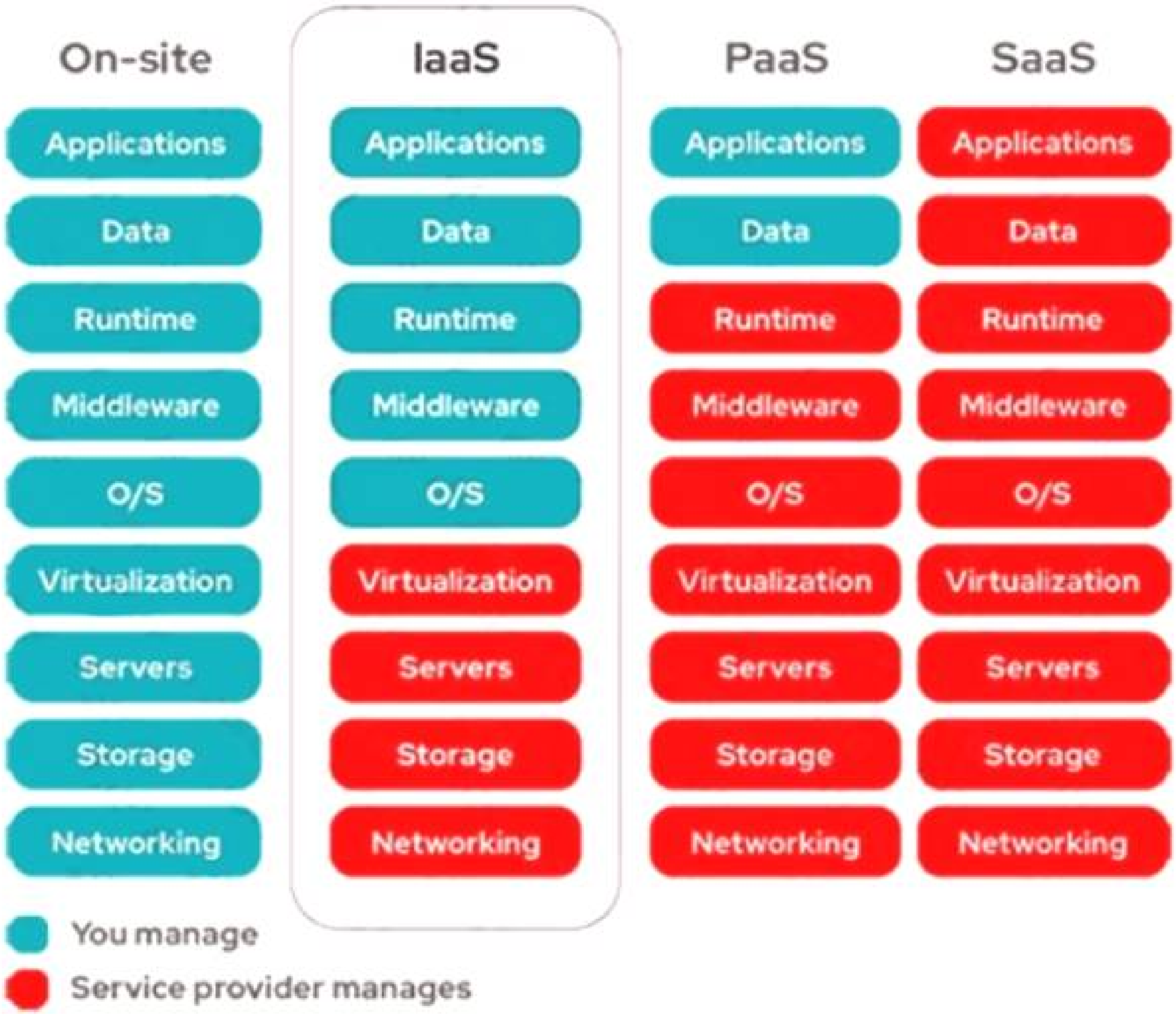
**NEW QUESTION 351**
- (Exam Topic 2)
Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two)

A. virtualization
B. middleware

C. operating systems
D. applications
E. data

**Answer:** DE

**Explanation:**
Customers must manage applications and data in PaaS.



| On-site | IaaS | PaaS | SaaS |
|---|---|---|---|
| 🟦 Applications | 🟦 Applications | 🟦 Applications | 🟥 Applications |
| 🟦 Data | 🟦 Data | 🟦 Data | 🟥 Data |
| 🟦 Runtime | 🟦 Runtime | 🟥 Runtime | 🟥 Runtime |
| 🟦 Middleware | 🟦 Middleware | 🟥 Middleware | 🟥 Middleware |
| 🟦 O/S | 🟦 O/S | 🟥 O/S | 🟥 O/S |
| 🟦 Virtualization | 🟥 Virtualization | 🟥 Virtualization | 🟥 Virtualization |
| 🟦 Servers | 🟥 Servers | 🟥 Servers | 🟥 Servers |
| 🟦 Storage | 🟥 Storage | 🟥 Storage | 🟥 Storage |
| 🟦 Networking | 🟥 Networking | 🟥 Networking | 🟥 Networking |

🟦 You manage
🟥 Service provider manages

**NEW QUESTION 353**
- (Exam Topic 2)
What are two differences between a Cisco WSA that is running in transparent mode and one running in explicit mode? (Choose two)

A. The Cisco WSA responds with its own IP address only if it is running in explicit mode.
B. The Cisco WSA is configured in a web browser only if it is running in transparent mode.
C. The Cisco WSA responds with its own IP address only if it is running in transparent mode.
D. The Cisco WSA uses a Layer 3 device to redirect traffic only if it is running in transparent mode.
E. When the Cisco WSA is running in transparent mode, it uses the WSA's own IP address as the HTTP request destination.

**Answer:** AD

**Explanation:**
In explicit proxy mode, users are configured to use a web proxy and the web traffic is sent directly to the Cisco WSA. In contrast, in transparent proxy mode the Cisco WSA intercepts user's web traffic redirected from other network devices, such as switches, routers, or firewalls.

**NEW QUESTION 356**
- (Exam Topic 2)
When planning a VPN deployment, for which reason does an engineer opt for an active/active FlexVPN configuration as opposed to DMVPN?

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

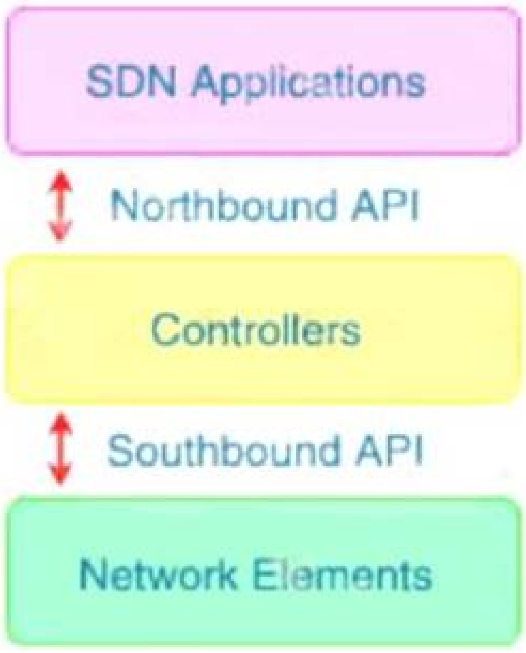
**Answer:** B

**NEW QUESTION 361**
- (Exam Topic 2)
Which type of API is being used when a controller within a software-defined network architecture dynamically makes configuration changes on switches within the network?

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

**Answer:** B

**Explanation:**
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands andscalability needs.



**NEW QUESTION 365**
- (Exam Topic 2)
Which attack type attempts to shut down a machine or network so that users are not able to access it?

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

**Answer:** A

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

**NEW QUESTION 368**
- (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

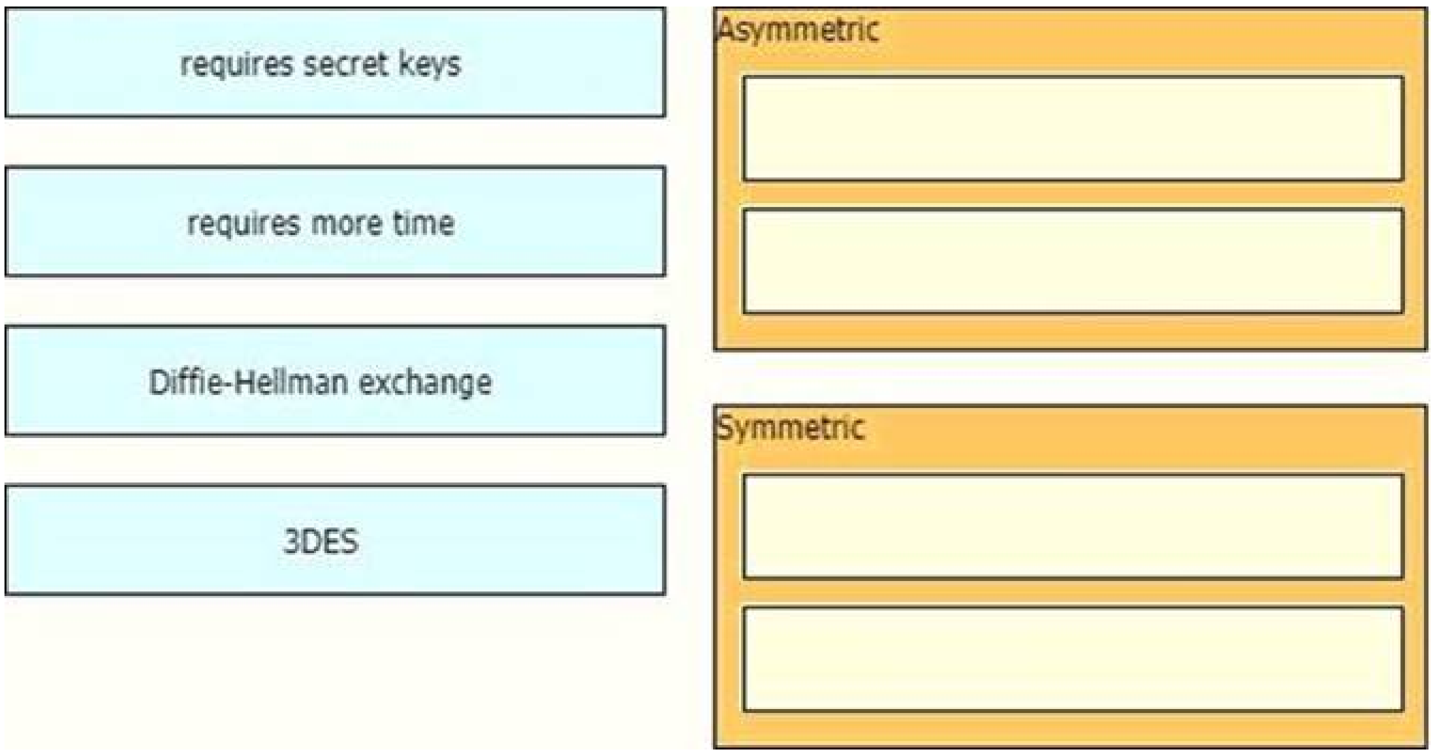
**NEW QUESTION 370**
- (Exam Topic 2)
What is a capability of Cisco ASA Netflow?

A. It filters NSEL events based on traffic
B. It generates NSEL events even if the MPF is not configured
C. It logs all event types only to the same collector
D. It sends NetFlow data records from active and standby ASAs in an active standby failover pair

**Answer:** A

**Explanation:**
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGui Policy Order The order in which policies are listed in a policy table determines the priority with which they are applied to Web requests. Web requests are checked against policies beginning at the top of the table and ending at the first policy matched. Any policies below that point in the table are not processed. If no user-defined policy is matched against a Web request, then the global policy for that policy type is applied. Global policies are always positioned last in Policy tables and cannot be re-ordered.

**NEW QUESTION 373**
- (Exam Topic 2)
Drag and drop the descriptions from the left onto the encryption algorithms on the right.



requires secret keys

requires more time

Diffie-Hellman exchange

3DES

Asymmetric

Symmetric

A. Mastered
B. Not Mastered

**Answer:** A

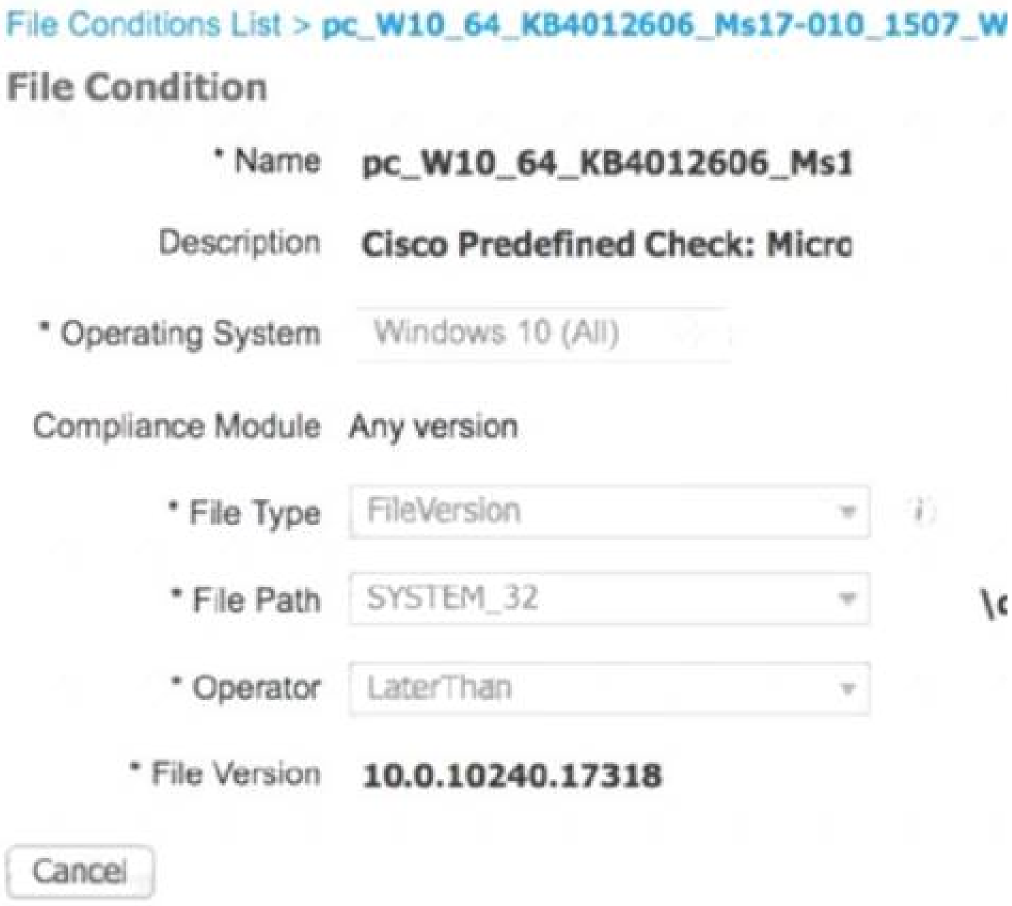
**Explanation:**
Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetric encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.Asymmetric encryption takes relatively more time than the symmetric encryption.Diffie Hellman algorithm is an asymmetric algorithm used to establish a shared secret for a symmetric keyalgorithm. Nowadays most of the people uses hybrid crypto system i.e, combination of symmetric andasymmetric encryption. Asymmetric Encryption is used as a technique in key exchange mechanism to share secret key and after the key is shared between sender and receiver, the communication will take place using symmetric encryption. The shared secret key will be used to encrypt the communication.Triple DES (3DES), a symmetric-key algorithm for the encryption of electronic data, is the successor of DES (Data Encryption Standard) and provides more secure encryption then DES.Note: Although “requires secret keys” option in this question is a bit unclear but it can only be assigned toSymmetric algorithm.

**NEW QUESTION 374**
- (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 | Windows 10 (All) |
| Compliance Module | Any version |
| * File Type | FileVersion |
| * File Path | SYSTEM_32 \c |
| * Operator | LaterThan |
| * File Version | 10.0.10240.17318 |

**NEW QUESTION 379**
- (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 381**
- (Exam Topic 2)
What is the purpose of the certificate signing request when adding a new certificate for a server?

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

**Answer:** B

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

**NEW QUESTION 382**
- (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 387**
- (Exam Topic 2)
What is the benefit of installing Cisco AMP for Endpoints on a network?

A. It provides operating system patches on the endpoints for security.
B. It provides flow-based visibility for the endpoints network connections.
C. It enables behavioral analysis to be used for the endpoints.
D. It protects endpoint systems through application control and real-time scanning

**Answer:** D

**NEW QUESTION 388**
- (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 targetmachine. Since the machine receiving such packets cannot reassemble them due
to a bug in TCP/IPfragmentation 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 392**
- (Exam Topic 2)
What are two benefits of Flexible NetFlow records? (Choose two)

A. They allow the user to configure flow information to perform customized traffic identification
B. They provide attack prevention by dropping the traffic
C. They provide accounting and billing enhancements
D. They converge multiple accounting technologies into one accounting mechanism
E. They provide monitoring of a wider range of IP packet information from Layer 2 to 4

**Answer:**

AD

**Explanation:**
Reference: https://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon_external_docbase_0 d9.html#wp1057997Note: Traditional NetFlow allows us to monitor from Layer 2 to 4 but Flexible NetFlow goes beyond theselayers.

**NEW QUESTION 393**
- (Exam Topic 2)
A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an undetermined verdict. What is causing this issue?

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

**Answer:** D

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

**NEW QUESTION 394**
......