350-701$^{\text{Q\&As}}$

Implementing and Operating Cisco Security Core Technologies (SCOR)

Pass Cisco 350-701 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/350-701.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

What are two differences between a Cisco WSA that is running in transparent mode and one running in explicit mode? (Choose two)

A. When the Cisco WSA is running in transparent mode, it uses the WSA\\'s own IP address as the HTTP request destination.

B. The Cisco WSA responds with its own IP address only if it is running in explicit mode.

C. The Cisco WSA is configured in a web browser 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. The Cisco WSA responds with its own IP address only if it is running in transparent mode.

Correct Answer: BD

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.

The Cisco WSA responds with its own IP address only if it is running in explicit mode.

This statement is true. In explicit mode, the client\\'s browser is configured to send web traffic to the proxy server\\'s IP address. Therefore, the WSA responds with its own IP address to the client\\'s requests.

The Cisco WSA uses a Layer 3 device to redirect traffic only if it is running in transparent mode.

Option D is correct because in transparent mode, the WSA uses a Layer 3 device (such as a router) to redirect traffic to the proxy server, whereas in explicit mode, the client\\'s browser is configured to send traffic directly to the WSA.

QUESTION 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

Correct Answer: CE

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.

QUESTION 3

A network engineer needs to select a VPN type that provides the most stringent security, multiple security associations for the connections, and efficient VPN establishment with the least bandwidth consumption. Why should the engineer select either FlexVPN or DMVPN for this environment?

A. DMVPN because it supports IKEv2 and FlexVPN does not

B. FlexVPN because it supports IKEv2 and DMVPN does not

C. FlexVPN because it uses multiple SAs and DMVPN does not

D. DMVPN because it uses multiple SAs and FlexVPN does not

Correct Answer: C

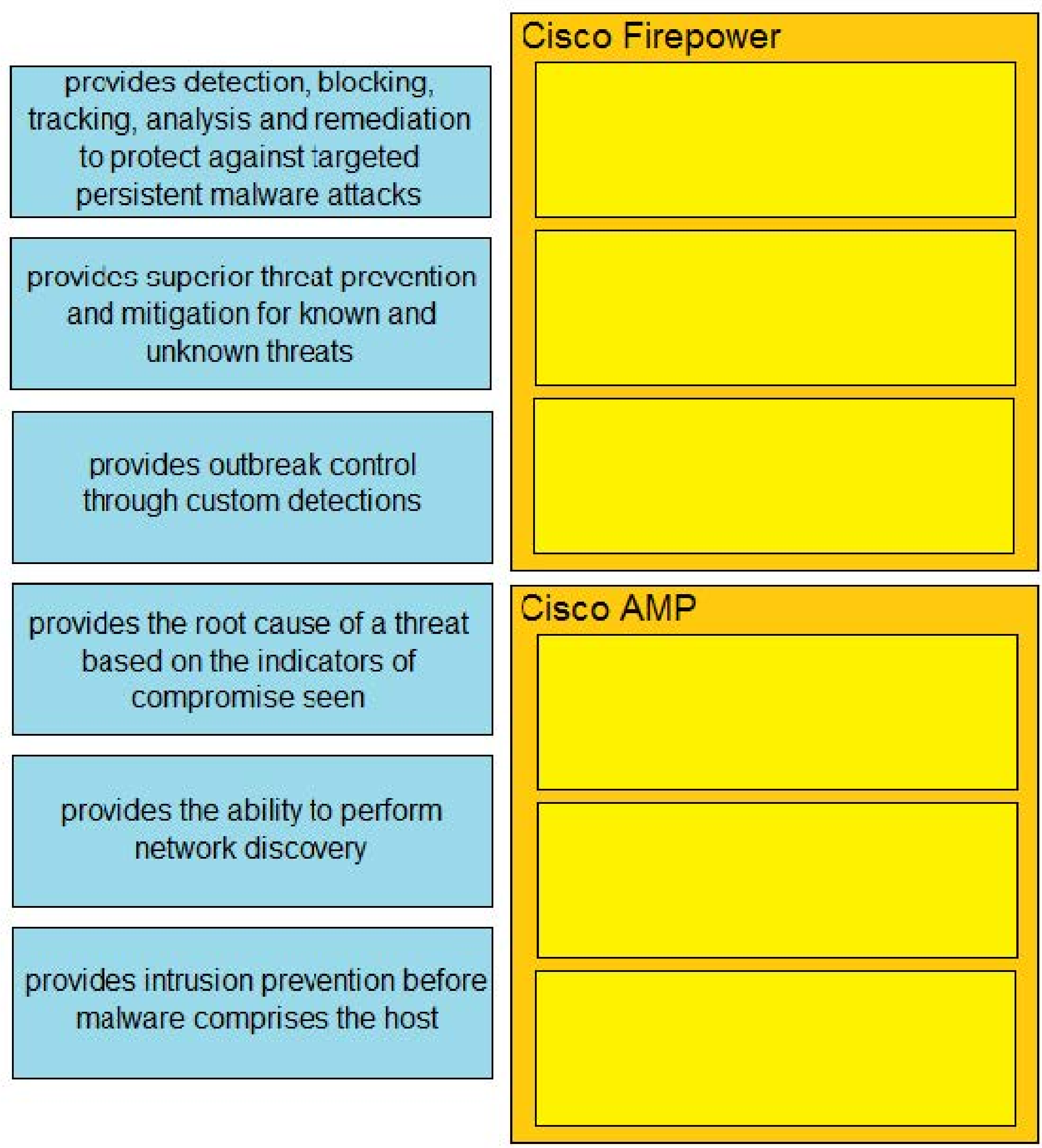
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-16-12/sec-flex-vpn-xe-16-12-book/sec-cfg-flex-serv.html

QUESTION 4

DRAG DROP

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

Select and Place:



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

provides superior threat prevention and mitigation for known and unknown threats

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

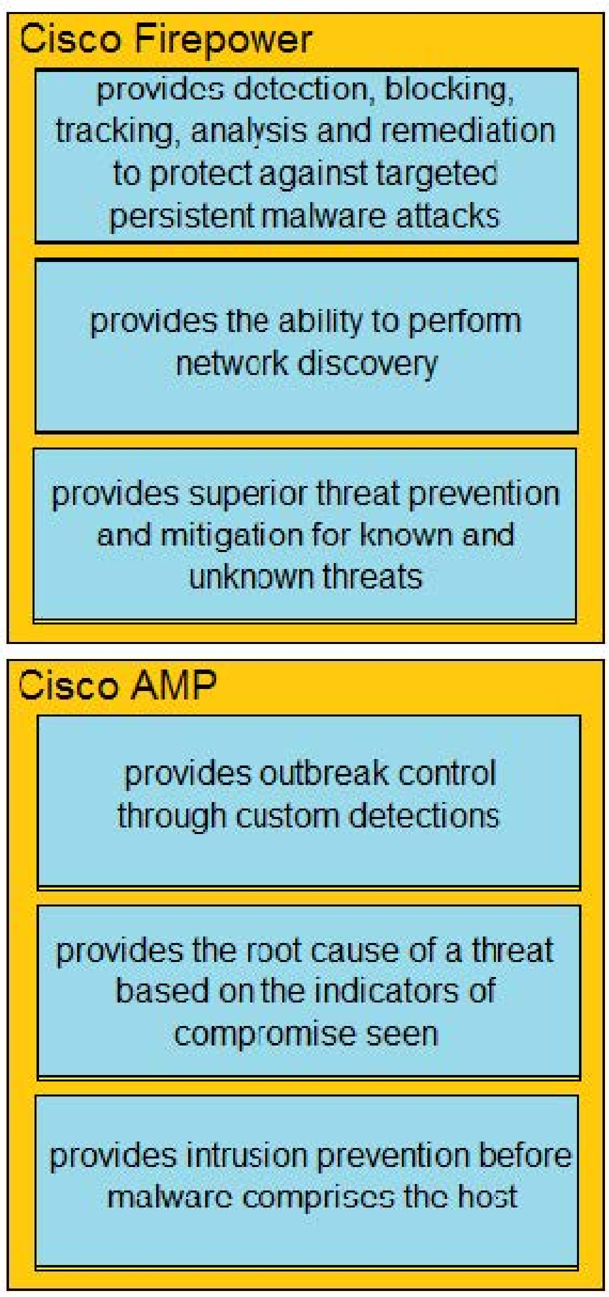
provides the ability to perform network discovery

provides intrusion prevention before malware comprises the host

Cisco Firepower

Cisco AMP

Correct Answer:



Cisco Firepower

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

provides the ability to perform network discovery

provides superior threat prevention and mitigation for known and unknown threats

Cisco AMP

provides outbreak control through custom detections

provides the root cause of a threat based on the indicators of compromise seen

provides intrusion prevention before malware comprises the host

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

QUESTION 5

What is a function of the Layer 4 Traffic Monitor on a Cisco WSA?

A. blocks traffic from URL categories that are known to contain malicious content

B. decrypts SSL traffic to monitor for malicious content

C. monitors suspicious traffic across all the TCP/UDP ports

D. prevents data exfiltration by searching all the network traffic for specified sensitive information

Correct Answer: C

350-701 PDF Dumps 350-701 VCE Dumps 350-701 Study Guide