- **Vendor:** Cisco
- **Exam Code:** 350-701
- **Exam Name:** Implementing and Operating Cisco Security Core Technologies (SCOR)
- **New Updated Questions from Braindump2go (Updated in Nov./2020)**

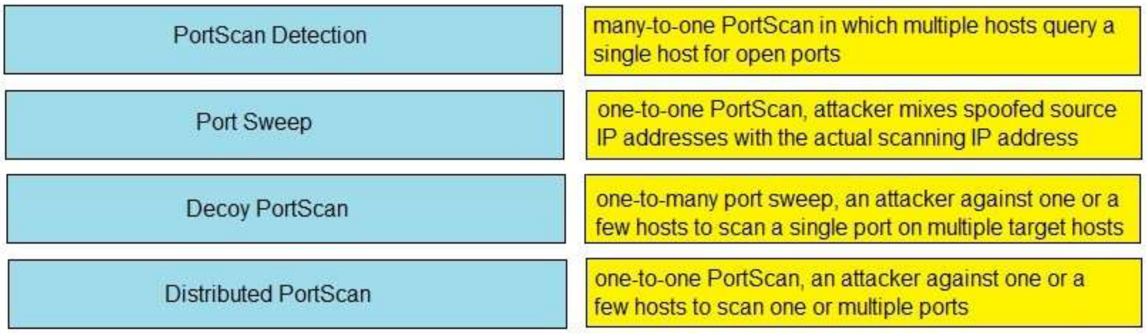
Visit Braindump2go and Download Full Version 350-701 Exam Dumps

QUESTION 88
Which two deployment modes does the Cisco ASA FirePOWER module support? (Choose two.)

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

Answer: CE

QUESTION 89
Drag and Drop Question
Drag and drop the Firepower Next Generation Intrustion Prevention System detectors from the left onto the correct definitions on the right.



PortScan Detection

Port Sweep

Decoy PortScan

Distributed PortScan

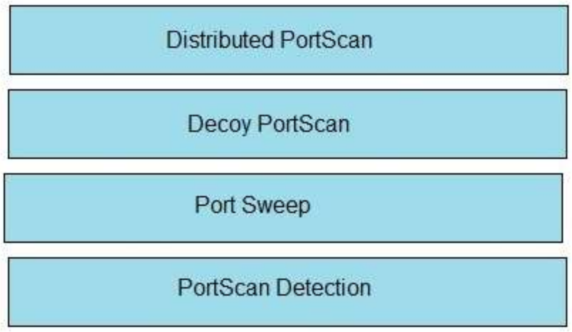
many-to-one PortScan in which multiple hosts query a single host for open ports

one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address

one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts

one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

Answer:



Distributed PortScan

Decoy PortScan

Port Sweep

PortScan Detection

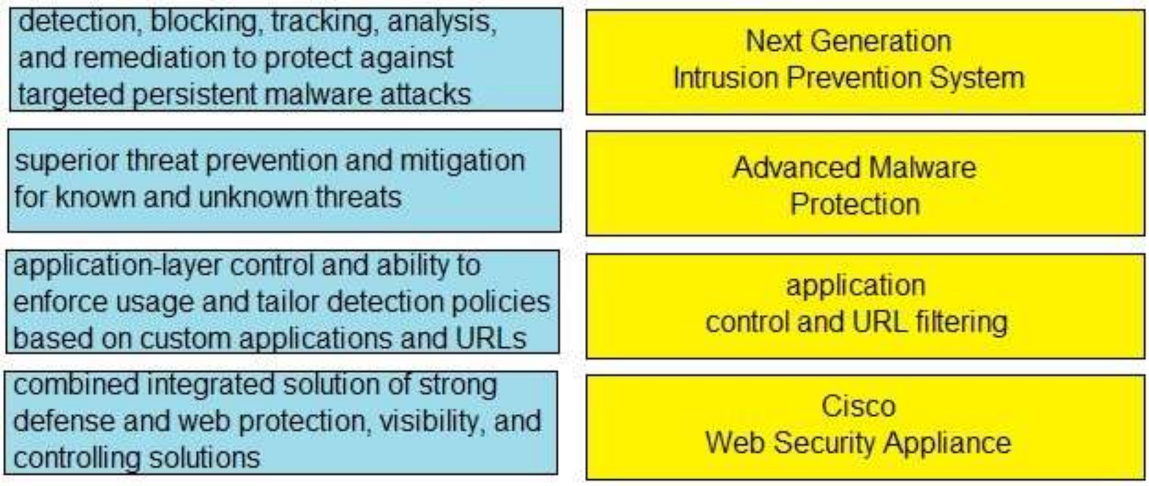
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-

v64/detecting_specific_threats.html

QUESTION 90

Drag and Drop Question

Drag and drop the capabilities from the left onto the correct technologies on the right.



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

superior threat prevention and mitigation for known and unknown threats

application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs

combined integrated solution of strong defense and web protection, visibility, and controlling solutions

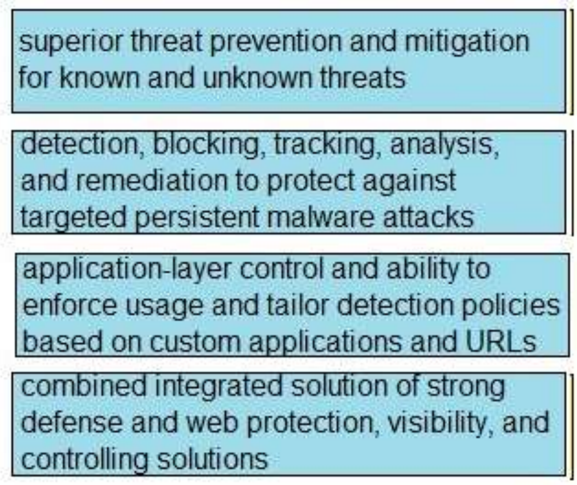
Next Generation Intrusion Prevention System

Advanced Malware Protection

application control and URL filtering

Cisco Web Security Appliance

Answer:



superior threat prevention and mitigation for known and unknown threats

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

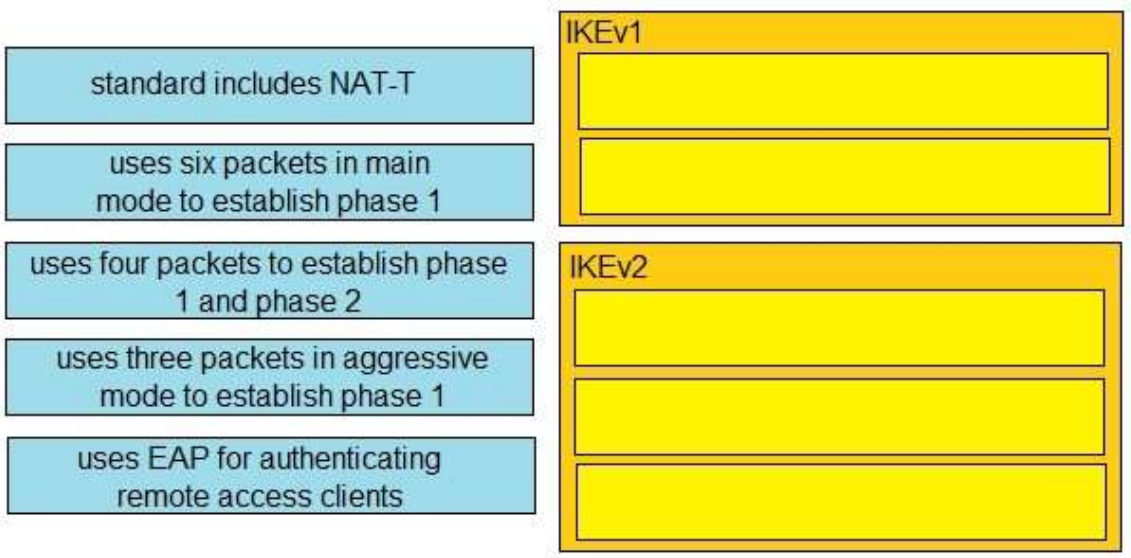
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs

combined integrated solution of strong defense and web protection, visibility, and controlling solutions

QUESTION 91

Drag and Drop Question

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



standard includes NAT-T

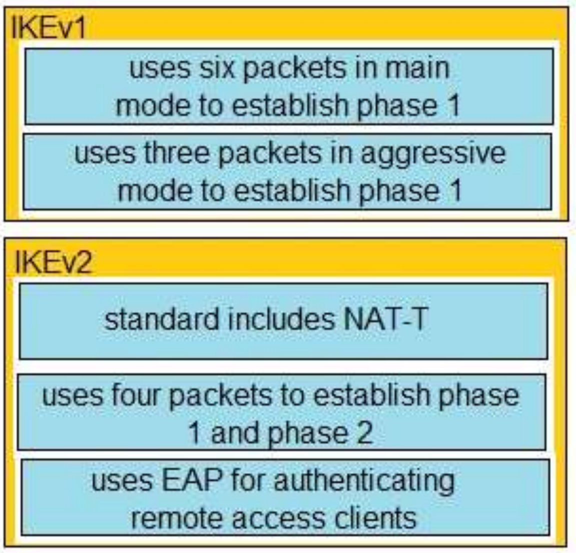
uses six packets in main mode to establish phase 1

uses four packets to establish phase 1 and phase 2

uses three packets in aggressive mode to establish phase 1

uses EAP for authenticating remote access clients

Answer:



IKEv1

uses six packets in main mode to establish phase 1

uses three packets in aggressive mode to establish phase 1

IKEv2

standard includes NAT-T

uses four packets to establish phase 1 and phase 2

uses EAP for authenticating remote access clients

QUESTION 92
Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

A. AMP
B. AnyConnect
C. DynDNS
D. Talos

Answer: D

QUESTION 93
What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?

A. It decrypts HTTPS application traffic for unauthenticated users.
B. It alerts users when the WSA decrypts their traffic.

C. It decrypts HTTPS application traffic for authenticated users.
D. It provides enhanced HTTPS application detection for AsyncOS.

Answer: D
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01011.html

QUESTION 94
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

QUESTION 95
Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two.)

A. accounting
B. assurance
C. automation
D. authentication
E. encryption

Answer: BC
Explanation:
https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html

QUESTION 96
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:
https://learn-umbrellA.cisco.com/cloud-security/dns-tunneling

QUESTION 97
Which algorithm provides encryption and authentication for data plane communication?

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

Answer: A

QUESTION 98
How does Cisco Umbrella archive logs to an enterprise-owned storage?

A. by using the Application Programming Interface to fetch the logs
B. by sending logs via syslog to an on-premises or cloud-based syslog server
C. by the system administrator downloading the logs from the Cisco Umbrella web portal
D. by being configured to send logs to a self-managed AWS S3 bucket

Answer: D
Explanation:
https://docs.umbrellA.com/deployment-umbrella/docs/log-management

QUESTION 99
In which cloud services model is the tenant responsible for virtual machine OS patching?

A. IaaS
B. UCaaS
C. PaaS
D. SaaS

Answer: A
Explanation:
https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paashow-microsoft-office-365-azure-fit-in-021672.php

QUESTION 100
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
Explanation:
https://gpdb.docs.pivotal.io/43190/admin_guide/topics/ipsec.html