Exam : 646-562

Title : Advanced Security for Account Managers (ASAM)□□

Ver : 11-08-07

QUESTION 1
You are meeting with an enterprise customer that has a multivendor network. Which Cisco Security product should you position with this customer?

A. CiscoWorks VPN/Security Management Solution Basic
B. Cisco Security MARS
C. Cisco Router and Security Device Manager
D. Cisco PIX Device Manager

Answer: B

QUESTION 2
Which security management offering helps customers to readily and accurately identify, manage, and mitigate network attacks and to maintain network security compliance?

A. Cisco Security Manager
B. Cisco Network Assistant
C. Cisco NAC
D. Cisco Security MARS
E. Cisco Security Agent
F. Cisco Trust Agent

Answer: D

QUESTION 3
In terms of the network life-cycle, what should you consider when evaluating the TCO of a security solution?

A. planning and design phases
B. implementation and operation phases
C. the entire network life-cycle
D. operation phase
E. planning phase

Answer: C

QUESTION 4
You are meeting with a customer who is concerned about ongoing network threats and vulnerabilities within the corporate network. How should you position the Cisco SDN with this customer?

A. The Cisco Self-Defending Network is the Cisco solution that protects the network of an organization. The SDN strategy offers security products that will defend your network before attacks occur. SDN products use industry-leading technologies, which will enable your company to stay up to date on network security.

B. Cisco NAC is a complete, end-to-end security solution that enables endpoints to be admitted to the network based on their adherence to security policy as enforced by network devices, such as routers and switches. NAC is a solution that will protect business processes and the network of your organization by identifying, preventing, and adapting to security threats.
C. Cisco SDN solutions are adaptive, allowing for innovative behavioral methods to be deployed in order to automatically recognize new types of threats as they arise. Mutual awareness can exist among and between security services and network intelligence, thus increasing security effectiveness and enabling a much more proactive response to new types of threats.
D. Most network threats and vulnerabilities arise from inefficient access control. Cisco VLAN solutions are a part of the Self-Defending Network strategy, and can segment users into different workgroups or virtual LANs based on whom they are, not where they are. In turn, VLAN solutions prohibit hackers from gaining network access, and will dramatically lessen the pains you are experiencing with network threats and vulnerabilities.

Answer: C

QUESTION 5
Which Cisco Security Solution helps organizations to effectively avoid disruptions that are caused by worms or viruses, while also helping to control the costs of deploying and maintaining a secure network?

A. CiscoWorks VPN/Security Management Solution
B. Cisco Security Monitoring, Analysis and Response System
C. Theft of Information Solution
D. Outbreak Prevention Solution

Answer: D

QUESTION 6
How does the Cisco Security Agent work in conjuction with third-party antivirus software?

A. Cisco Security Agent checks the status of third-party antivirus software and makes a decision about compliance.
B. Cisco Security Agent checks the status of third-party antivirus software and forwards it to the third-party antivirus policy server.
C. Cisco Security Agent checks the status of third-party antivirus software and forwards it to the policy server (ACS).
D. Cisco Security Agent enhances the security by sandboxing the applications and the system in addition to the antivirus protection offered by the antivirus software.
E. Cisco Security Agent makes the antivirus software superfluous.

Answer: D

QUESTION 7
Which security pain point can be resolved by each of these security products: Cisco ASA 5500 Series Adaptive Security Appliances, Cisco PIX Firewall 500 Series, Cisco Security Agent, and

the Cisco Guard DDoS Mitigation Appliances?

A. business disruption from an Internet attack, such as viruses, worms, and/or hackers
B. difficulty enforcing compliance to security policies that govern desktop antivirus software
C. extension of the investment in an existing Cisco router by making it a fully secure WAN device
D. remote employees that require access to the corporate network
E. firewall functionality that scales from the branch office to the network core

Answer: A

QUESTION 8
Which three technologies allow the Cisco SDN to adapt to new threats as they arise? (Choose three.)

A. antivirus
B. application awareness
C. behavior recognition
D. firewalling
E. network control
F. VPN

Answer: B, C, E

QUESTION 9
Why do end users need to be aware of the security policy?

A. Some security decisions are usually in their hands.
B. They should understand the probability of every risk.
C. They need to be aware of every threat.
D. They should avoid responsibility for their actions.

Answer: A

QUESTION 10
Which three elements should an enterprise security policy specify? (Choose three.)

A. risks and how to manage the risks
B. network inventory
C. user roles and responsibilities
D. software versions of the security products
E. contingency plan in case of compromise
F. funds allocated to security projects

Answer: A, C, E

QUESTION 11
Which business enabler provides a defense against damages and losses (such as financial, legal, commercial, image, branding, property, and people), which directly affect the ability of a company to do business?

A. government regulations
B. protection
C. ubiquitous access
D. contribution to profitability

Answer: B

QUESTION 12
Which two factors should be considered when calculating the cost of downtime? (Choose two.)

A. number of compromised servers
B. server downtime (in hours)
C. time (in hours) to rebuild servers
D. average revenue per hour

Answer: B, D

QUESTION 13
To successfully sell security products, you must identify customer pain points, and then map those pain points to Cisco Security Solutions that solve them through successful threat mitigation. What are three Cisco Security Solutions that directly relate to common security pain points that are identified in the annual CSI/FBI Computer Crime and Security Survey? (Choose three.)

A. Application Abuse Prevention Solution
B. DDoS Attack Solution
C. Anti-Spyware Solution
D. Internal Threat Prevention Solution
E. Outbreak Prevention Solution
F. Theft of Information Solution

Answer: B, E, F

QUESTION 14
Which three of these are key elements of the Adaptive Threat Defense? (Choose three.)

A. multilayer intelligence
B. a blend of IP and security technologies
C. active management and mitigation
D. dynamic adjustment of risk ratings
E. feature consistency
F. intrusion detection system

Answer: A, C, D

QUESTION 15
Which statement best describes the Cisco SDN strategy?

A. The SDN strategy is to protect standalone products at the physical perimeter of a network, where the LAN meets the WAN and corporate networks connect to the Internet.
B. The SDN strategy is to protect business processes and the network of an organization by identifying, preventing, and adapting to security threats and by including integrated, collaborative, and adaptive security elements throughout the network.
C. The SDN enables network elements to communicate with one another in a collaborative manner, for example, an IDS instructing an ACL to deny access to a connection.
D. The SDN is the most widely deployed network-admissions-control strategy, supporting organizations of all sizes as well as multiple access methods, including wireless, remote, LAN, WAN, and guest access.

Answer: B

QUESTION 16
In which two ways does application security protect against threats being introduced from within web-enabled applications? (Choose two.)

A. Application security examines message-level information to ascertain the "intent" of the applications.
B. Application security provides controls that limit the transmission of confidential data or policies.
C. Application security intelligently analyzes network payload.
D. Application security stops attacks as far as possible from their intended destination and the core of the network.
E. Application security provides sophisticated auditing, control, and correlation capabilities to control and protect any networked element.

Answer: A, C

QUESTION 17
Which two Cisco security technologies can help organizations that have difficulty enforcing compliance to security policies that govern desktop antivirus software? (Choose two.)

A. Cisco ASA 5500 Series Adaptive Security Appliances
B. Cisco Integrated Services Routers
C. Cisco PIX Firewall 500 Series
D. Cisco Security Agent
E. NAC Appliance (Cisco Clean Access)
F. Firewall Services Module

Answer: D, E

QUESTION 18
Which principal characteristic of the Cisco SDN incorporates technologies that are inherent in the secure operation of network devices, including control plane policing and CPU/memory thresholding?

A. collaboration
B. Cisco IOS software
C. integration
D. secure infrastructure

Answer: C

QUESTION 19
Which two factors should be considered when calculating the cost of recovery? (Choose two.)

A. number of compromised servers
B. server downtime (in hours)
C. time (in hours) to rebuild servers
D. average revenue per hour

Answer: A, C

QUESTION 20
How do you calculate risk quantitatively for SLE?

A. single loss expectancy divided by the annualized rate of occurrence
B. exposure factor multiplied by the asset value
C. cost of recovery multiplied by the number of compromised servers
D. average revenue per hour divided by the hourly server downtime

Answer: B

QUESTION 21
What are three benefits of the Cisco SDN that will be recognized by business decision makers? (Choose three.)

A. lowers TCO by using the existing infrastructure
B. helps to meet regulatory requirements
C. protects against insecure or contaminated devices
D. helps to manage IT and operational risk
E. effectively enforces security and confidentiality policies company-wide
F. provides network availability and reliability

Answer: A, B, D

QUESTION 22
When building a security policy for an organization, which of these steps should you take first?

A. risk assessment
B. risk management
C. threat avoidance
D. end-user training
E. threat identification

Answer: E

QUESTION 23
Which three features explain how the Cisco Self-Defending Network strategy helps control and contain security threats? (Choose three.)

A. reactive protection and containment of known and unknown threats
B. distributed mitigation of infections and outbreaks
C. tight security at higher operational costs
D. manageable patching and updating due to enforced endpoint compliance
E. defense in depth
F. single point of failure

Answer: B, D, E

QUESTION 24
Which Cisco IOS feature facilitates dynamic IPsec tunnels between spoke (branch) sites?

A. Cisco Easy VPN
B. V3PN
C. DMVPN
D. Cisco WebVPN

Answer: C

QUESTION 25
Which statement best describes the functionality of the Cisco Security Agent?

A. It enforces authorization policies and privileges.
B. It isolates noncompliant machines.
C. It prevents malicious behavior before damage can occur.
D. It performs vulnerability testing and threat remediation.

Answer: C

QUESTION 26
Network containment and control provides the ability to layer sophisticated auditing, control, and correlation capabilities to protect any networked element across any firewall, VPN, intrusion detection mechanism, or other technology. How does this enable proactive response to threats?

A. It distributes mitigation points throughout key security-enforcement points in the network.
B. It examines message-level information to ascertain the "intent" of the applications.
C. It provides controls that limit the transmission of confidential data or policies.
D. It aggregates and correlates security information.

Answer: D

QUESTION 27
What is a benefit of Cisco IOS IPS?

A. ensures security compliance before allowing network access
B. protects investments by using the existing network infrastructure
C. contains a network-based tool for vulnerability and threat remediation
D. protects against spyware and adware

Answer: B

QUESTION 28
In which two ways does a Cisco solution directly reduce the cost of operation? (Choose two.)

A. by minimizing the number of vendors that supply security
B. by reducing overall management complexity
C. by improving competitive advantage
D. by avoiding information theft
E. by addressing security pain points

Answer: A, B

QUESTION 29
In which two ways does a Cisco SDN provide outbreak prevention? (Choose two.)

A. efficiently mitigates DDoS attack damage
B. enforces security compliance for all devices that access network resources
C. identifies, quarantines, and remediates improperly protected devices
D. grants and enforces access rights and privileges to trusted, authenticated users

Answer: B, C

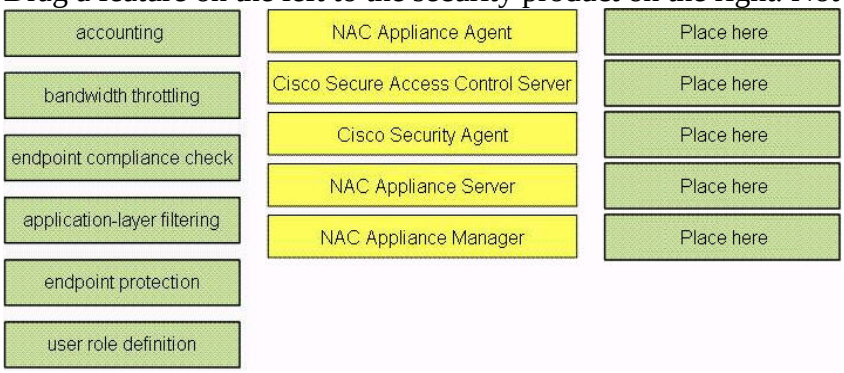
QUESTION 30
Which government regulation was implemented to promote world financial stability by

coordinating definitions of capital and risk assessment across countries?

A. BS 7799/ISO 17799
B. SOX
C. HIPAA
D. Basel II
E. USA PATRIOT Act

Answer: D

QUESTION 31
Drag a feature on the left to the security product on the right. Not all features are used.



Answer:

QUESTION 32
Which principal characteristic of the Cisco SDN allows endpoints to be admitted to the network based on their adherence to security policy as enforced by routers and switches?

A. endpoint security
B. integration
C. collaboration
D. adaptation

Answer: C

QUESTION 33
Which two threat-defense features allow a network to correlate events, mitigate events, and audit

policies? (Choose two.)

A. proactive threat response
B. control of data transmission
C. application security
D. network containment and control
E. Anti-X defenses

Answer: A, D

QUESTION 34
Which government regulation specifies which patient information must be kept private, how companies must secure the information, and the standards for electronic communication between medical providers and insurance companies?

A. Basel II
B. GLB Act
C. HIPAA
D. USA PATRIOT Act

Answer: C

QUESTION 35
Which statement accurately describes the difference between a quantitative and a qualitative risk analysis?

A. Quantitative risk analysis attempts to determine numeric values for risk that is based on a number of factors, such as impact, duration, and asset value. A qualitative approach assigns a subjective rating to each risk that typically is based on past experience or consultant opinion.
B. Qualitative risk analysis attempts to determine numeric values for risk that is based on a number of factors, such as impact, duration, and asset value. A quantitative approach assigns a subjective rating to each risk that typically is based on past experience or consultant opinion.
C. Both quantitative and qualitative risk analyses determine numeric values for risk. However, a quantitative risk analysis focuses on objective information, whereas a qualitative approach focuses on subjective information.
D. Both quantitative and qualitative risk analyses determine numeric values for risk. However, a quantitative risk analysis focuses on subjective information, whereas a qualitative approach focuses on objective information.

Answer: A

QUESTION 36
Which Cisco solution provides host protection against security violations by focusing on the behavior of the device?

A. Cisco PIX Firewall
B. Cisco Adaptive Security Appliance
C. Cisco Security Agent
D. NAC Appliance
E. host Analyzer

Answer: C

QUESTION 37
Which security management product combines network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification, and automated mitigation capabilities?

A. CiscoWorks VPN/Security Management Solution Basic
B. CiscoWorks SIMS
C. Cisco VPN 3000 Concentrator
D. Cisco Security MARS

Answer: D

QUESTION 38
Which government regulation opens up an opportunity to sell a Cisco Security Solution to companies that collect financial information?

A. AS/NZS 4360
B. BS 7799/ISO 17799
C. SOX
D. GLB Act
E. HIPAA

Answer: D

QUESTION 39
Which security product supports up to three Cisco Security devices and an unlimited number of CSAs?

A. CiscoWorks VPN/Security Management Solution Basic
B. CiscoWorks SIMS
C. Cisco Security MARS
D. Cisco Network Assistant

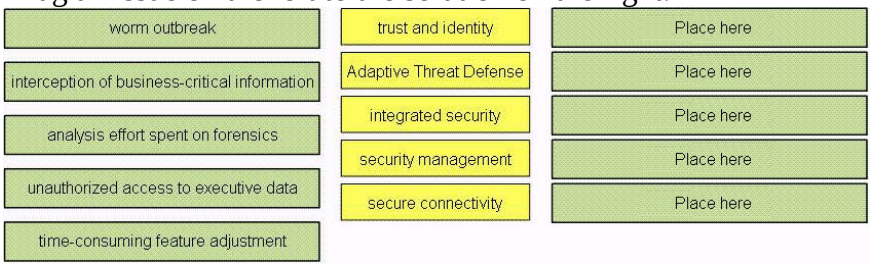
Answer: A

QUESTION 40
How is the Cisco ASA 5500 Series "adaptive" in terms of the principal characteristics of the Cisco SDN strategy?

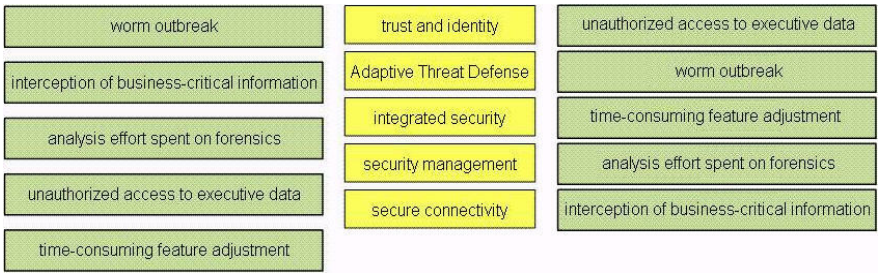
A. The Cisco ASA 5500 Series is alerted by the Cisco Traffic Anomaly Detector XT or other standards-based detection solutions. It then diverts traffic that is destined for a targeted device (and only that traffic), and subjects it to the unique MVP architecture from Cisco. This blocks malicious activity that is responsible for the attack while allowing legitimate transactions to pass.
B. The Cisco ASA 5500 Series incorporates converged security functionalities, such as delivering converged firewall, IDS, network antivirus, and VPN services. This enables the Cisco ASA 5500 Series to become part of a solution that allows every network element to act as a point of defense, working together to provide a secure and adaptive system.
C. The Adaptive Identification and Mitigation services architecture of the Cisco ASA 5500 Series allows businesses to adapt and extend the security services profile through highly customizable flow-specific security policies. These policies tailor security needs to application requirements while providing performance and security services when and where they are needed.
D. The Cisco ASA 5500 Series includes easily deployed products that can automatically detect, isolate, and clean infected or vulnerable devices that attempt to access the network. They identify whether networked devices are compliant with your network security policies and repair any vulnerabilities before permitting access to the network.

Answer: C

QUESTION 41
Drag an issue on the left to the solution on the right.



Answer:



QUESTION 42
The Cisco SDN is a strategy to protect the business processes and the network of an organization by identifying, preventing, and adapting to security threats. What are three principal characteristics of the SDN? (Choose three.)

A. application security

B. adaptation
C. intelligence
D. collaboration
E. protection
F. integration

Answer: B, D, F

QUESTION 43
A company suffered from a critical security breach and experienced considerable downtime. They decided to reassess the security policy and rebuild the network infrastructure. Which three business problems does the Self-Defending Network initiative address? (Choose three.)

A. asset exposure
B. legal liability
C. suboptimal product positioning
D. damage to customer confidence
E. inadequate time-to-market
F. lack of robustness

Answer: A, B, D

QUESTION 44
The Cisco SDN allows organizations to manage the IT network security risk that is associated with the deployment of online business processes, ensuring that organizations achieve their objectives efficiently while managing associated risks. What are three key SDN components of the Cisco Application Abuse Prevention Solution that work together to offer this type of protection? (Choose three.)

A. access control solutions
B. content security solutions
C. detector and guard solutions
D. endpoint protection solutions
E. transaction security solutions
F. VPN solutions

Answer: B, D, E

QUESTION 45
Because the initial product cost of a solution is often a fraction of the TCO over the life span of the solution, which two other factors should be considered when talking about the TCO of security? (Choose two.)

A. costs that are collected from a qualitative risk assessment
B. costs that are acquired from end-user training
C. costs that are associated with other similar competitive product offerings

D. costs that are associated with solution deployment

Answer: B, D

QUESTION 46
Your customer wants to ensure business continuity by allowing legitimate transactions to the website while redirecting illegitimate transactions. Which Cisco SDN solution offering would satisfy this requirement?

A. Cisco NAC framework
B. Cisco Secure ACS
C. Cisco Guard DDoS Mitigation Appliances
D. Cisco Security MARS

Answer: C

QUESTION 47
A Cisco Outbreak Prevention Solution provides customers with many benefits. Within this solution, which type of Cisco network security offering acts as the first line of defense to proactively isolate infections by preventing worms or viruses from infiltrating endpoints?

A. NIPS
B. HIPS
C. Cisco IOS infrastructure security
D. Cisco antivirus software

Answer: B

QUESTION 48
Which government regulation is designed to create a common information security structure that is based on recognized best practices, and is an internationally recognized generic standard?

A. Basel II
B. BS 7799/ISO 17799
C. AS/NZS 4360
D. SOX

Answer: B

QUESTION 49
You are meeting with a financial customer who is concerned about Internet worms, viruses, and other threats. A worm or virus would cost millions of dollars in lost productivity, and malware or spyware could result in information theft. How should you position Anti-X defenses with this customer?

A. Anti-X defenses intelligently analyze network payload so that application security tools can

control port 80 misuse by rogue applications.
B. Anti-X defenses provide broad attack-mitigation capabilities and distribute defenses throughout the network, including to critical system endpoints.
C. Anti-X defenses enable proactive response to threats by aggregating and correlating security information.
D. Anti-X defenses render malware and spyware harmless by managing patches more proactively.

Answer: B

QUESTION 50
Risk analysis is a critical part of assessing the security needs of a customer. What are three parts of the risk analysis process? (Choose three.)

A. assessing the current state of network infrastructure
B. identifying potential threats
C. prioritizing security needs
D. identifying regulatory compliancy issues (for example, Basel II)
E. determining the impact on business
F. analyzing competitive vendors

Answer: B, C, E

QUESTION 51
How does the Cisco SDN protect organizations from worm and virus outbreaks?

A. by controlling access control through different technologies, securing remote access by using VPN technology, and monitoring and enforcing which applications can run on the desktop
B. by protecting network endpoints, preventing infections from spreading through the network infrastructure, and monitoring the network in order to respond rapidly to outbreaks
C. by providing perimeter protection against unauthorized ingress and egress, providing network performance data to detect attacks, and securing desktops and laptops from malicious code
D. by checking for recognizable patterns, or by using heuristic scanning that inspects executable files using operations that might denote an unknown virus

Answer: B

QUESTION 52
Once you have concluded the discovery process, you will set up a meeting with the final decision maker and present the value proposition. Which two items would you include in your value proposition? (Choose two.)

A. qualitative information about how Cisco can help to increase revenue and reduce costs
B. a high-level review of the Cisco Security portfolio and how it differs from competitive offerings
C. a detailed review of the proposed technological enhancements that are provided in the security solution design

D. an analysis of the security-market business trends and related Cisco solution offerings
E. a review of customer security pain points and business needs that you learned about during the discovery process

Answer: A, E

QUESTION 53
What is one way that Cisco Security can decrease customer implementation costs?

A. through better security management products
B. through dedicated security appliances
C. by using the existing infrastructure
D. by reducing the number of people to train

Answer: C

QUESTION 54
Which two of these arguments can you use to convince a business decision-maker of the need for network security? (Choose two.)

A. A high-performance firewall is the only device that is needed to protect businesses.
B. Network security provides a method to balance threats with countermeasures.
C. The network should be secured at any expense.
D. Network security products are complex to manage, which makes them difficult to penetrate.
E. Organizations that operate vulnerable networks face increasing liability.

Answer: B, E

QUESTION 55
Continuance and protection fall under which layer of the business resilience model?

A. business resilience
B. applications resilience
C. communications resilience
D. network resilience

Answer: B

QUESTION 56
Which three ultimately lead to a higher TCO in terms of network security? (Choose three.)

A. best-of-breed point products
B. nonstandard configurations
C. centralized network management
D. ongoing support services
E. multiple vendors that supply security

F. security technology that is distributed into the network infrastructure

Answer: A, B, E

QUESTION 57
Which feature of Cisco Security MARS uses NetFlow data?

A. hotspot identification
B. anomaly detection
C. automated mitigation capabilities
D. context correlation

Answer: B

QUESTION 58
You are meeting with a customer who is concerned about remote employees connecting to the network with infected systems and spreading infection across the corporate network. How should you position the Cisco SDN with this customer?

A. The Cisco Self-Defending Network includes NAC, which evaluates devices that may not have the latest antivirus software or operating system patch, and either denies access to those devices or quarantines them.
B. The Cisco Self-Defending Network includes integration, which enables a more proactive response to threats with greater operational efficiency through the consolidation of multiple security services on the devices.
C. The Cisco Self-Defending Network is adaptive, distributing security technologies throughout every segment of the network to enable every network element as a point of defense.
D. The Cisco Self-Defending Network provides technologies that have intelligent insight into what is running on computers, so there is no possible way for remote employees to connect to the network with infected systems.

Answer: A

QUESTION 59
NAC is an example of which principal characteristic of the Cisco SDN?

A. adaptation
B. collaboration
C. differentiation
D. integration

Answer: B

QUESTION 60
A hacker initiates an attack that floods the network, overwhelming the company server, router. firewall, or network. Legitimate traffic cannot be processed, and the company cannot function.

This causes which security pain point?

A. DDoS attack
B. application security
C. theft of information
D. Day Zero attack

Answer: A