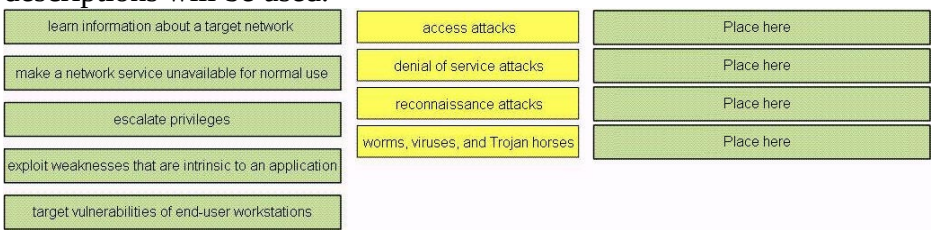
Exam : 642-565

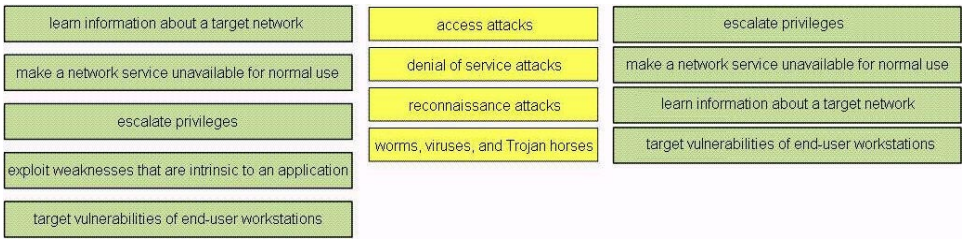
Title : Security Solutions for Systems Engineers(SSSE)□□

Ver : 11-08-07

QUESTION 1
Drag each description on the left to the corresponding attack methodology on the right. Not all descriptions will be used.



Answer:



QUESTION 2
SomeCompany, Ltd. wants to implement the the PCI Data Security Standard to protect sensitive cardholder information. They are planning to use RSA to ensure data privacy, integrity, and origin authentication. Which two of these statements describe features of the RSA keys? (Choose two.)

A. The public key only encrypts.
B. The public key only decrypts.
C. The public key both encrypts and decrypts.
D. The private key only encrypts.
E. The private key only decrypts.
F. The private key both encrypts and decrypts.

Answer: C, F

QUESTION 3
What are two functions of Cisco Security Agent? (Choose two.)

A. authentication
B. control of executable content
C. resource protection
D. spam filtering
E. user tracking

Answer: B, C

QUESTION 4
Which three policy types can be assigned to a network user role in the Cisco NAC Appliance architecture? (Choose three.)

A. allowed IP address ranges
B. session duration
C. minimum password length
D. VPN and roaming policies
E. inactivity period
F. network port scanning plug-ins

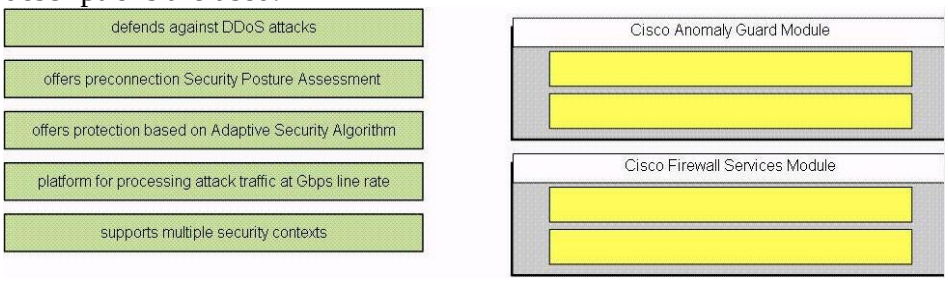
Answer: B, D, F

QUESTION 5
Which of these items is a valid method to verify a network security design?

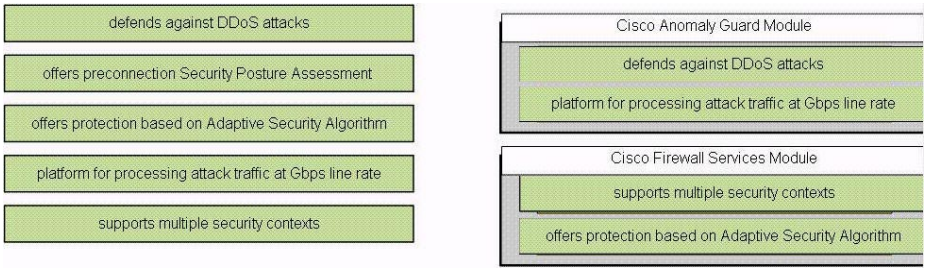
A. network audit
B. sign-off by the operations team
C. computer simulation
D. analysis of earlier attacks
E. pilot or prototype network

Answer: E

QUESTION 6
Drag the descriptions from the left to the corresponding Cisco security module on the right. Not all descriptions are used.



Answer:



QUESTION 7
Which two components should be included in a detailed design document for a security solution? (Choose two.)

A. data source
B. existing network infrastructure

C. organizational chart
D. proof of concept
E. traffic growth forecast
F. weak-link description

Answer: B, D

QUESTION 8
What are three functions of CSA in helping to secure customer environments? (Choose three.)

A. application control
B. control of executable content
C. identification of vulnerabilities
D. probing of systems for compliance
E. real-time analysis of network traffic
F. system hardening

Answer: A, B, F

QUESTION 9
Which two of these features are key elements of the collaborative security approach? (Choose two.)

A. integration of security features in network equipment
B. Network Admission Control
C. coordinated defense of potential entry points
D. automated event and action filters
E. network behavioral analysis
F. device chaining

Answer: B, C

QUESTION 10
Which two of these statements describe features of the NAC Appliance architecture. (Choose two.)

A. NAC Appliance Server evaluates the endpoint security information.
B. NAC Appliance Manager determines the appropriate access policy.
C. NAC Appliance Client acts as an authentication proxy for internal user authentication.
D. NAC Appliance Manager acts as an authentication proxy for external authentication servers.

Answer: B, D

QUESTION 11
Which three technologies address ISO 17799 requirements for unauthorized access prevention? (Choose three.)

A. Cisco Secure Access Control Server
B. SSLVPN
C. 802.1X
D. Network Admission Control
E. Cisco Security MARS
F. intrusion prevention system

Answer: A, C, D

QUESTION 12
Which certificates are needed for a device to join a certificate-authenticated network?

A. the certificates of the certificate authority and the device
B. the certificates of the device and its peer
C. the certificates of the certificate authority and the peer
D. the certificates of the certificate authority, the device, and the peer

Answer: A

QUESTION 13
What allows Cisco Security Agent to block malicious behavior before damage can occur?

A. correlation of network traffic with signatures
B. interception of operating system calls
C. scan of downloaded files for malicious code
D. user query and response

Answer: B

QUESTION 14
What are three advantages of Cisco Security MARS? (Choose three.)

A. performs automatic mitigation on Layer 2 devices
B. ensures that the user device is not vulnerable
C. fixes vulnerable and infected devices automatically
D. provides rapid profile-based provisioning capabilities
E. is network topology aware
F. contains scalable, distributed event analysis architecture

Answer: A, E, F

QUESTION 15
Which encryption protocol is suitable for an enterprise with standard security requirements?

A. MD5

B. 768-bit RSA encryption
C. AES-128
D. DES
E. SHA-256

Answer: C

QUESTION 16
In which two ways do Cisco ASA 5500 Series Adaptive Security Appliances achieve containment and control? (Choose two.)

A. by enabling businesses to create secure connections
B. by preventing unauthorized network access
C. by probing end systems for compliance
D. by tracking the state of all network communications
E. by performing traffic anomaly detection

Answer: B, D

QUESTION 17
Which three of these security products complement each other to achieve a secure e-banking solution? (Choose three.)

A. Cisco IOS DMVPN
B. Cisco Intrusion Prevention System
C. CCA Agent
D. Cisco Adaptive Security Appliance
E. Cisco Security Agent
F. Cisco Trust Agent

Answer: B, D, E

QUESTION 18
Which IPS feature models worm behavior and correlates the specific time between events, network behavior, and multiple exploit behavior to more accurately identify and stop worms?

A. Risk Rating
B. Meta Event Generator
C. Security Device Event Exchange support
D. traffic normalization

Answer: B

QUESTION 19
Which three elements does the NAC Appliance Agent check on the client machine? (Choose three.)

A. IP address
B. registry keys
C. presence of Cisco Trust Agent
D. presence of Cisco Security Agent
E. Microsoft hotfixes

Answer: B, D, E

QUESTION 20
Which of these items is a feature of a system-level approach to security management?

A. single-element management
B. responsibility sharing
C. multiple cross-vendor management platforms
D. high availability
E. complex operations

Answer: D

QUESTION 21
In which way do components of the NAC Appliance architecture communicate?

A. NAC Appliance Manager sends check-up instructions to the NAC Appliance Server.
B. NAC Appliance Manager sends remediation instructions to the NAC Appliance Agent.
C. NAC Appliance Server sends block instructions to the NAC Appliance Agent.
D. NAC Appliance Agent sends procedure instructions to the NAC Appliance Server.
E. NAC Appliance Agent sends check-up instructions to the NAC Appliance Manager.
F. NAC Appliance Server sends block instructions to the NAC Appliance Manager.

Answer: B

QUESTION 22
Which two technologies address ISO 17799 requirements in detecting, preventing, and responding to attacks and intrusions? (Choose two.)

A. Cisco Security MARS
B. 802.1X
C. DMVPN
D. Cisco NAC Appliance
E. Cisco Security Agent
F. Cisco Trust Agent

Answer: A, E

QUESTION 23
Which two are true about Cisco AutoSecure? (Choose two.)

A. blocks all IANA-reserved IP address blocks
B. enables identification service
C. enables log messages to include sequence numbers and time stamps
D. disables tcp-keepalives-in and tcp-keepalives-out
E. removes the exec-timeout

Answer: A, C

QUESTION 24
Which two components should be included in a network design document? (Choose two.)

A. complete network blueprint
B. configuration for each device
C. detailed part list
D. operating expense
E. risk analysis

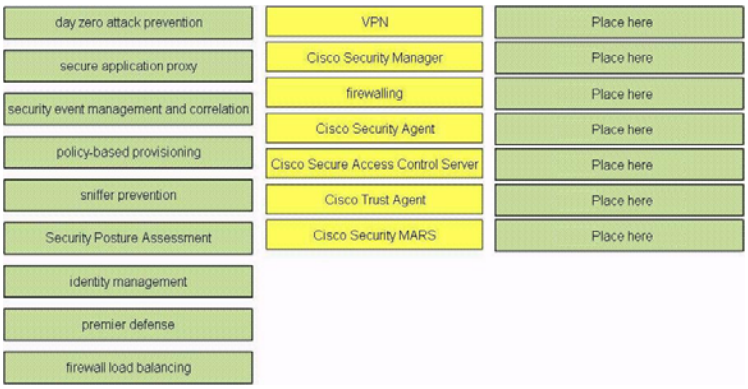
Answer: A, C

QUESTION 25
Which three components should be included in a security policy? (Choose three.)

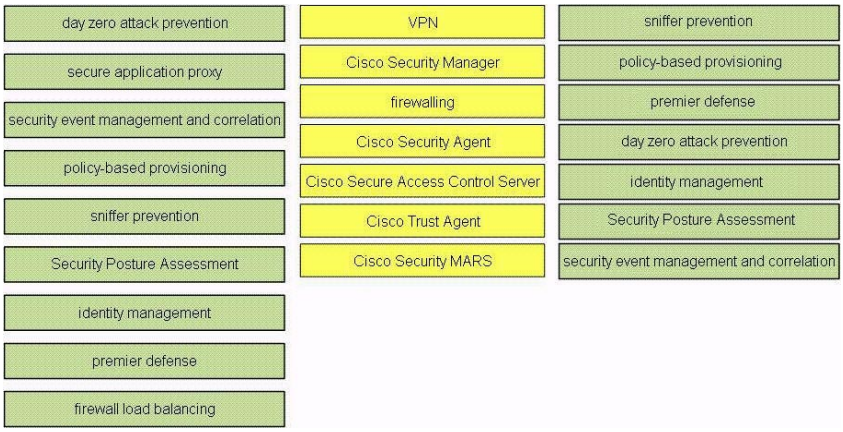
A. identification and authentication policy
B. incident handling procedure
C. security best practice
D. security product recommendation
E. software specifications
F. statement of authority and scope

Answer: A, B, F

QUESTION 26
Drag the security feature on the left to the appropriate Cisco technology on the right. Not all features are used.



Answer:



QUESTION 27
Which statement is true regarding Cisco IOS IPS performance and capabilities?

A. Cisco IOS IPS signatures have a minimal impact on router memory.
B. Cisco IOS IPS uses a parallel signature-scanning engine to scan for multiple patterns within a signature micro-engine at any given time.
C. Cisco IOS IPS offers a wider signature coverage than the IDSM-2 module.
D. All Cisco IOS IPS signatures should be enabled to maximize the coverage, except for falsepositives reduction.

Answer: B

QUESTION 28
Which IPS platform can operate in inline mode only?

A. Cisco IPS 4200 Series Sensor
B. IDSM-2
C. Cisco IOS IPS
D. Cisco ASA AIP SSM

Answer: C

QUESTION 29
Which of these items describes a benefit of deploying the NAC appliance in in-band mode rather than out-of-band mode?

A. bandwidth enforcement policy
B. Nessus scanning
C. NAC Appliance Agent deployment
D. higher number of users per NAC Appliance
E. support for Layer 2 or Layer 3 deployments

Answer: A

QUESTION 30
Which protocol should be used to provide secure communications when performing shunning on a network device?

A. Telnet
B. SNMPv2
C. SSL
D. SNMPv3
E. SSH

Answer: E

QUESTION 31
What are the advantages of IPsec-based site-to-site VPNs over traditional WAN networks?

A. bandwidth guarantees, support for non-IP protocols, scalability, and modular design guidelines
B. bandwidth guarantees, flexibility, security, and low cost
C. span, flexibility, security, and low cost
D. delay guarantees, span, performance, security, and low cost

Answer: C

QUESTION 32
SomeCompany, Ltd. wishes to adopt the Adaptive Threat Defense architecture in their security policy. Identify three components of the anti-X defense pillar. (Choose three.)

A. anomaly detection
B. application-level role-based access control
C. distributed denial-of-service mitigation
D. transaction privacy
E. URL filtering
F. network auditing

Answer: A, C, E

QUESTION 33
Which three of these security products complement each other to achieve a secure remoteaccess solution? (Choose three.)

A. Adaptive Security Appliance
B. Cisco Security MARS
C. NAC Appliance
D. Cisco GET VPN
E. Cisco Secure Access Control Server
F. URL filtering server

Answer: A, C, E

QUESTION 34
How is an incident defined in MARS?

A. a raw message sent to the MARS via syslog, SNMP, or NetFlow by the reporting devices
B. a series of events that is correlated to represent a single occurrence using related information within a given timeframe
C. a series of events that triggered a defined rule in the system
D. a series of behaviors in a session that describe an anomaly, worm or virus

Answer: C

QUESTION 35
What are three functions of Cisco Security Agent? (Choose three.)

A. spyware and adware protection
B. device-based registry scans
C. malicious mobile code protection
D. local shunning
E. protection against buffer overflows
F. flexibility against new attacks through customizable signatures "on the fly"

Answer: A, C, E

QUESTION 36
Which three factors can affect the risk rating of an IPS alert? (Choose three.)

A. event severity
B. asset integrity
C. signature priority
D. attacker location

E. signature fidelity
F. relevance

Answer: A, E, F

QUESTION 37
Which two of these features are the most appropriate test parameters for the acceptance test plan of a secure connectivity solution? (Choose two.)

A. resistance against brute-force attacks
B. privacy of key exchange
C. high availability
D. duration of the key refresh operation
E. certificate enrollment and revocation

Answer: C, E

QUESTION 38
What is the objective of the Cisco IOS resilient configuration?

A. speed up the Cisco IOS image or configuration recovery process
B. prevent a compromise of the router
C. enable redundant Cisco IOS images for fault tolerance router operations
D. activate primary and backup operations of two Cisco IOS routers

Answer: A

QUESTION 39
Which three of these items are features of the Cisco Secure Access Control Server? (Choose three.)

A. local OTP
B. NDS
C. Kerberos
D. LDAP
E. CA database
F. RSA certificates

Answer: B, D, F

QUESTION 40
Which two requirements call for the deployment of 802.1X? (Choose two.)

A. authenticate users on switch or wireless ports
B. validate security posture using TACACS+
C. grant or deny network access, at the port level, based on configured authorization policies

D. permit network access during the quiet period
E. deploy Cisco Secure ACS as the policy server

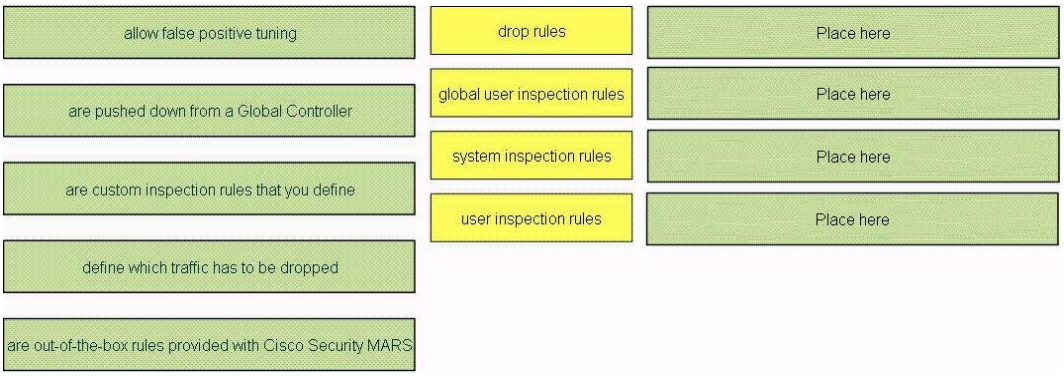
Answer: A, C

QUESTION 41
Which two of these features are integrated security components of the Cisco Adaptive Security Appliance? (Choose two.)

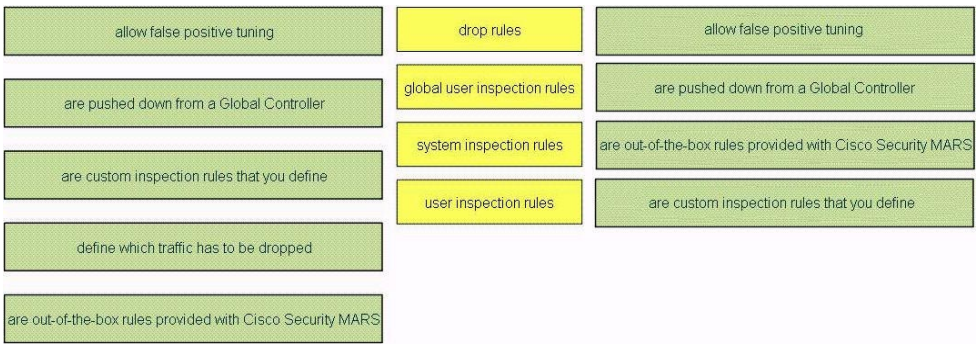
A. VTI
B. VRF-aware firewall
C. Cisco ASA AIP SSM
D. Anti-X
E. DMVPN
F. Control Plane Policing

Answer: C, D

QUESTION 42
Drag the descriptions on the left to their corresponding rule type on the right. Not all descriptions are used.



Answer:



QUESTION 43
Which two of these features are software components of the Cisco Security Manager bundle? (Choose two.)

A. Management Center for Firewalls and IPS
B. Resource Manager Essentials
C. Management Center for Cisco Security Agent
D. Auto Update Server
E. Backup Server

Answer: B, D

QUESTION 44
Which three of these features are elements of an acceptance test plan? (Choose three.)

A. system tuning
B. system integration in a production environment
C. timely rollout
D. pilot system demonstration
E. network impact analysis
F. user satisfaction analysis

Answer: A, B, E

QUESTION 45
What are the major characteristics for designing a VPN for existing networks?

A. vendors and the functionality of the installed equipment
B. performance, topology, and price
C. topology, high availability, security, scalability, manageability, and performance
D. intended use, existing installation, and desired functionality

Answer: C

QUESTION 46
Which two should be included in an analysis of a Security Posture Assessment? (Choose two.)

A. detailed action plan
B. identification of bottlenecks inside the network
C. identification of critical deficiencies
D. recommendations based on security best practice
E. service offer

Answer: C, D

QUESTION 47
Which two of these features are supported by Cisco Security MARS running software version 4.2.x? (Choose two.)

A. hierarchical design using global and local controllers

B. user login authentication using external AAA server
C. role-based access and dashboards
D. inline or promiscuous mode operation
E. NetFlow for network profiling and anomaly detection
F. attack capture and playback

Answer: A, E

QUESTION 48
Which Cisco security product is used to perform a Security Posture Assessment of client workstations?

A. Cisco ACS
B. Adaptive Security Appliance
C. Cisco Security Agent
D. Cisco NAC Appliance
E. Cisco Security Posture Assessment tool

Answer: D

QUESTION 49
Which two features work together to provide anti-X defense? (Choose two.)

A. enhanced application inspection engines
B. enhanced security state assessment
C. Cisco IPS sensors
D. network security event correlation
E. Cisco AutoSecure

Answer: A, C

QUESTION 50
Which two technologies mitigate the threat of a SYN flood attack? (Choose two.)

A. Cisco IOS IPS
B. MARS flood automitigation
C. ASA TCP Intercept
D. ASA enhanced application inspection
E. NAC Appliance security posture validation
F. Cisco IOS FPM

Answer: A, C

QUESTION 51
Which statement is true about the Cisco Security MARS Global Controller?

A. The Global Controller receives detailed incidents information from the Local Controllers, and correlates the incidents between multiple Local Controllers.
B. The Global Controller centrally manages a group of Local Controllers.
C. Rules that are created on a Local Controller can be pushed to the Global Controller.
D. Most data archiving is done by the Global Controller.

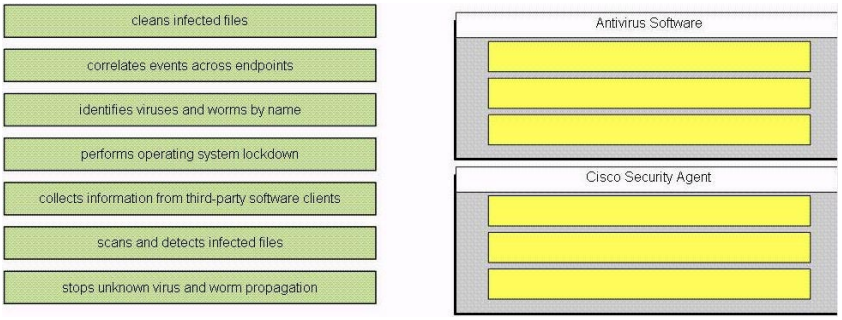
Answer: B

QUESTION 52
Which two technologies can prevent the Slammer worm from compromising a host? (Choose two.)

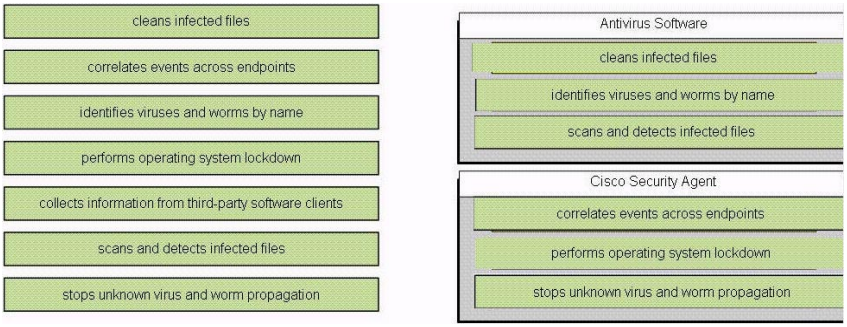
A. Cisco IOS IPS
B. ASA stateful firewall
C. ASA enhanced application inspection
D. NAC Appliance security posture validation
E. Cisco IOS FPM
F. Cisco Trust Agent

Answer: A, E

QUESTION 53
Drag each function on the left to the corresponding security product on the right. Not all items are used.



Answer:



QUESTION 54
Which two statements are true about symmetric key encryption? (Choose two.)

A. It uses secret-key cryptography.
B. Encryption and decryption use different keys.
C. It is typically used to encrypt the content of a message.
D. RSA is an example of symmetric key encryption
E. The key exchange can take place via a nonsecure channel.

Answer: A, C

QUESTION 55
Which of these protections is a benefit of HMAC?

A. protection against DoS attacks
B. protection against brute-force attacks
C. protection against man-in-the-middle attacks
D. protection from the avalanche effect

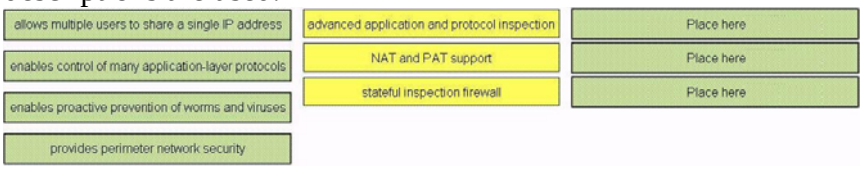
Answer: C

QUESTION 56
Which two are main security drivers? (Choose two.)

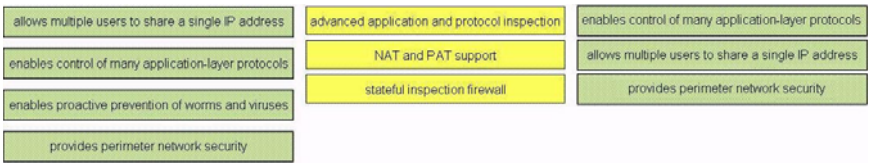
A. business needs
B. compliance with company policy
C. increased productivity
D. optimal network operation
E. security legislation

Answer: B, E

QUESTION 57
Drag the descriptions on the left to the corresponding firewall feature on the right. Not all descriptions are used.



Answer:



QUESTION 58
Which two of these statements describe features of the NAC Appliance architecture? (Choose two.)

A. The standard NAC Appliance Manager can manage up to 40 NAC Appliance Servers failover pairs.
B. NAC Appliance Servers managed by the same NAC Appliance Manager can run in mixed mode (inline or out-of-band).
C. The NAC Appliance Agent is bundled with the NAC Appliance Server software.
D. NAC Appliance high availability uses VRRP.
E. NAC Appliance Agent has the auto-upgrade feature.

Answer: B, E

QUESTION 59
What are the two main reasons for customers to implement Cisco Clean Access? (Choose two.)

A. enforcement of security policies by making compliance a condition of access
B. focus on validated incidents, not investigating isolated events
C. integrated network intelligence for superior event aggregation, reduction, and correlation
D. provision of secure remote access
E. significant cost savings by automating the process of repairing and updating user machines
F. implementation of NAC phase 1

Answer: A, E

QUESTION 60
What is the purpose of SNMP community strings when adding reporting devices into a newly installed Cisco Security MARS appliance?

A. to discover and display the full topology
B. to import the device configuration
C. to pull the log information from devices
D. to reconfigure managed devices

Answer: A

QUESTION 61
Which two of these characteristics apply to promiscuous IPS operation? (Choose two.)

A. typically used with SPAN on the switches
B. impacts connectivity in case of failure or overload
C. invisible to the attacker
D. increases latency
E. can use stream normalization techniques
F. less vulnerable to evasion techniques than inline mode

Answer: A, C

QUESTION 62
What is the security issue in classic packet filtering of active FTP sessions?

A. The control session cannot be adequately filtered.
B. Allowing control sessions to the client opens up all the high ports on the client.
C. The established keyword cannot be used for control or data sessions.
D. Allowing data sessions to the client opens up all the high ports on the client.

Answer: D

QUESTION 63
Which three of these features are key elements of the Adaptive Threat Defense? (Choose three.)

A. multilayer intelligence
B. blend of IP and security technologies
C. ability of a network to identify, prevent, and adapt to security threats
D. active management and mitigation
E. dynamic adjustment of risk ratings
F. feature consistency

Answer: A, D, E

QUESTION 64
How does CSA protect endpoints?

A. uses signatures to detect and stop attacks
B. uses deep-packet application inspections to control application misuse and abuse
C. uses file system, network, registry, and execution space interceptors to stop malicious activity
D. works in conjunction with antivirus software to lock down the OS
E. works at the application layer to provide buffer overflow protection

Answer: C

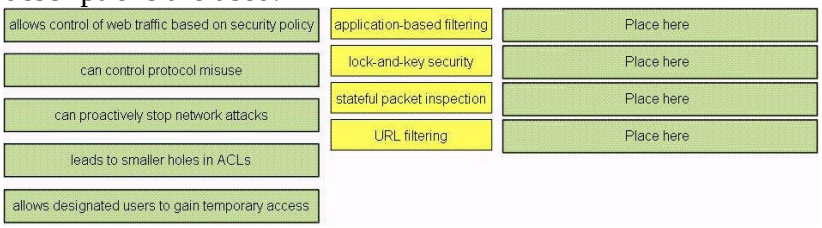
QUESTION 65
How is Cisco IOS Control Plane Policing achieved?

A. by adding a service-policy to virtual terminal lines and the console port
B. by applying a QoS policy in control plane configuration mode
C. by disabling unused services
D. by rate-limiting the exchange of routing protocol updates
E. by using AutoQoS to rate-limit the control plane traffic

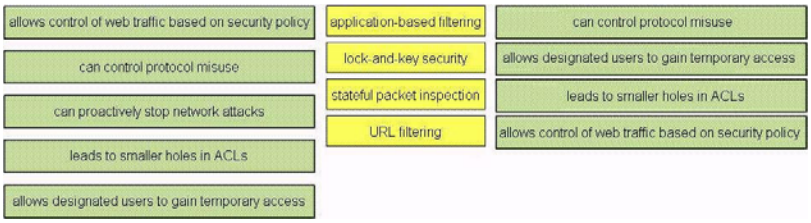
Answer: B

QUESTION 66
Drag the descriptions on the left to the corresponding security feature on the right. Not all

descriptions are used.



Answer:



QUESTION 67
When a FWSM is operating in transparent mode, what is true?

A. Each interface must be on the same VLAN.
B. The FWSM does not support multiple security contexts.
C. Each directly connected network must be on the same subnet.
D. The FWSM supports up to 256 VLANs.

Answer: C

QUESTION 68
Which of these characteristics is a feature of AES?

A. It has a variable key length.
B. It provides strong encryption and authentication.
C. It should be used with key lengths greater than 1024 bits.
D. It is not supported by hardware accelerators but runs very fast in software.

Answer: A

QUESTION 69
Which three Cisco security products help to prevent application misuse and abuse? (Choose three.)

A. Cisco ASA 5500 Series Adaptive Security Appliances
B. NAC Appliance (Cisco Clean Access)
C. Cisco Traffic Anomaly Detector
D. Cisco Security Agent
E. Cisco Trust Agent
F. Cisco IOS FW and IPS

Answer: A, D, F

QUESTION 70
Identify two ways to create a long-duration query on the Cisco Security MARS appliance.
(Choose two.)

A. by modifying an existing report
B. by saving a query as a report
C. by submitting a query in line
D. by submitting a batch query
E. by saving a query as a rule

Answer: A, D