إلى قارئ هذا الكتاب ، تحية طيبة وبعد ...

لقد أصبحنا نعيش في عالم يعج بالأبحاث والكتب والمعلومات، وأصبح العلم معياراً حقيقياً لتفاضل الأمم والدول والمؤسسات والأشخاص على حدٍّ سواء، وقد أمسى بدوره حلاً شبه وحيدٍ لأكثر مشاكل العالم حدة وخطورة، فالبيئة تبحث عن حلول، وصحة الإنسان تبحث عن حلول، والموارد التي تشكل حاجة أساسية للإنسان تبحث عن حلول كذلك، والطاقة والغذاء والماء جميعها تحديات يقف العلم في وجهها الآن ويحاول أن يجد الحلول لها. فأين نحن من هذا العلم ؟ وأين هو منا؟

نسعى في موقع عالم الإلكترون www.4electron.com لأن نوفر بين أيدي كل من حمل على عاتقه مسيرة درب تملؤه التحديات ما نستطيع من أدوات تساعده في هذا الدرب، من مواضيع علمية، ومراجع أجنبية بأحدث إصداراتها، وساحات لتبادل الآراء والأفكار العلمية والمرتبطة بحياتنا الهندسية، وشروحٍ لأهم برمجيات الحاسب التي تتداخل مع تطبيقات الحياة الأكاديمية والعملية، ولكننا نتوقع في نفس الوقت أن نجد بين الطلاب والمهندسين والباحثين من يسعى مثلنا لتحقيق النفع والفائدة للجميع، ويحلم أن يكون عضواً في مجتمعٍ يساهم بتحقيق بيئة خصبة للمواهب والإبداعات والتألق، فهل تحلم بذلك ؟

حاول أن تساهم بفكرة، بومضة من خواطر تفكيرك العلمي، بفائدة رأيتها في إحدى المواضيع العلمية، بجانب مضيء لمحته خلف ثنايا مفهوم هندسي ما. تأكد بأنك ستلتمس الفائدة في كل خطوة تخطوها، وترى غيرك يخطوها معك ...

أخي القارئ، نرجو أن يكون هذا الكتاب مقدمة لمشاركتك في عالمنا العلمي التعاوني، وسيكون موقعكم عالم الإلكترون ww.4electron.com بكل الإمكانيات المتوفرة لديه جاهزاً على الدوام لأن يحقق البيئة والواقع الذي يبحث عنه كل باحث أو طالب في علوم الهندسة، ويسعى فيه للإفادة كل ساعٍ ، فأهلاً وسهلاً بكم .

مع تحيات إدارة الموقع وفريق عمله

www.4electron.com

Cisco 642-564

Security Solutions for Systems Engineers

Q&A

Version 2.0

Important Note, Please Read Carefully

Other CertWays products
A) Offline Testing engine
Use the offline Testing engine product topractice the questions in an exam environment.
B) Study Guide (not available for all exams)
Build a foundation of knowledge which will be useful also after passing the exam.

Latest Version
We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at CertWays and update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1.Go towww.CertWays.com
2.Click on **Log in**
3.The latest versions of all purchased products are downloadable from here. Just click the links.
For mostupdates,itisenough just to print the new questions at the end of the new version, not the whole document.

Feedback
If you spot a possible improvement then please let us know. We always interested in improving product quality. Feedback should be send to feedback@CertWays.com. You should include the following: Exam number, version, page number, question number, and your login Email.

Our experts will answer your mail promptly.

Copyright
Each ePAD file is a green exe file. if we find out that a particular ePAD Viewer file is being distributed by you, CertWays reserves the right to take legal action against you according to the International Copyright Laws.

Explanations
This product does not include explanations at the moment. If you are interested in providing explanations for this exam, please contact feedback@CertWays.com.

CertWays Q: 1
Which protocol is used for transporting the event data from Cisco IPS 5.0 and later devices to the Cisco Security MARS appliance?

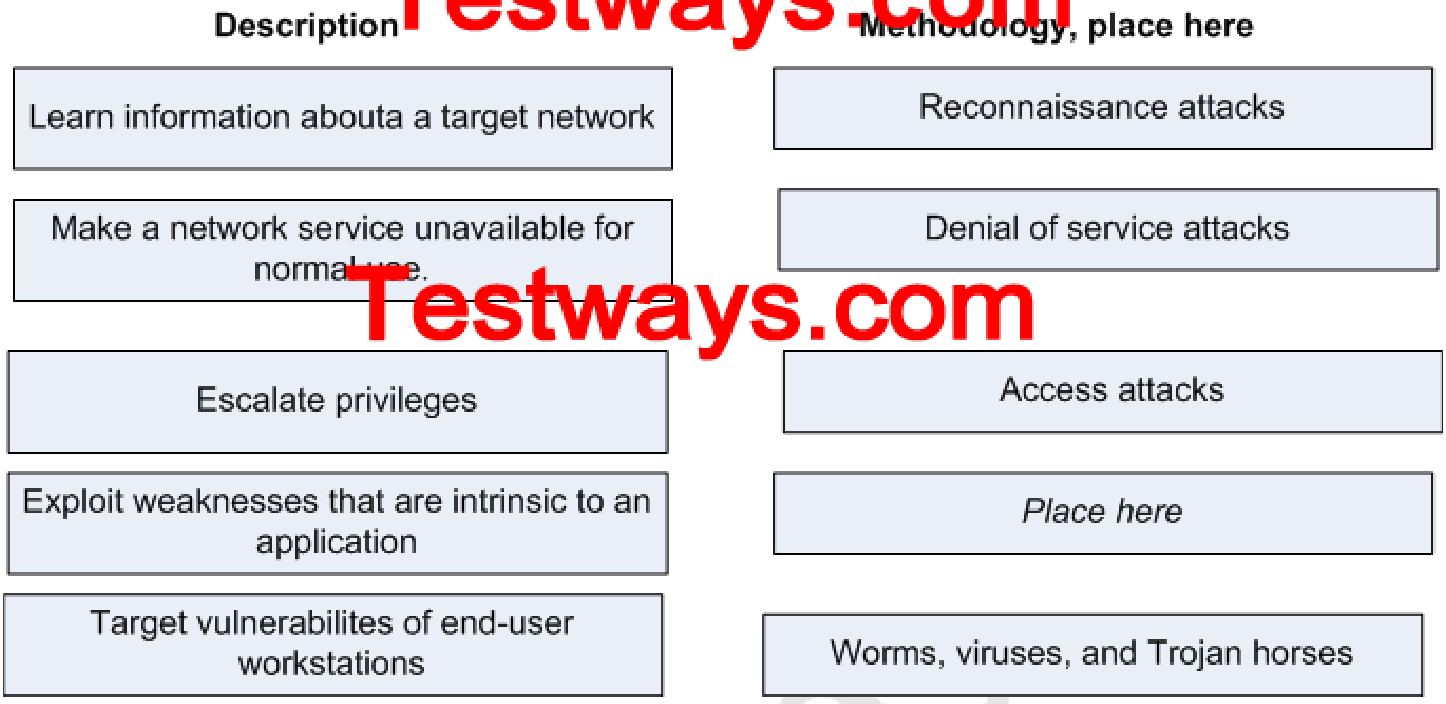
A. RDEP over SSL
B. SDEE over SSL
C. SSH
D. syslog

Answer: B

CertWays Q: 2 DRAG DROP
You work as a network technician at CertWays.com. Your boss, Mrs Tess King, is curious about attack methodologies. Match the technology with the appropriate description.

Use each technology once and only once.

Answer:
Explanation:



Reconnaissance Attacks

Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also called information gathering. In most cases, it precedes an actual access or DoS attack. The malicious intruder typically ping-sweeps the target network first to determine what IP addresses are alive. After this is accomplished, the intruder determines what services or ports are active on the live IP addresses. From this information, the intruder queries the ports to determine the application type and version as well as the type and version of the operating system running on the target host.

Reconnaissance is somewhat analogous to a thief scoping out a neighborhood for vulnerable homes he can break into, such as an unoccupied residence, an easy-to-open door or window, and so on. In many cases, an intruder goes as far as "rattling the door handle"-not to go in immediately if it is open, but to discover vulnerable services he can exploit later when there is less likelihood that anyone is looking.

Access Attacks

Access is an all-encompassing term that refers to unauthorized data manipulation, system access, or privilege escalation. Unauthorized data retrieval is simply reading, writing, copying, or moving files that are not intended to be accessible to the intruder. Sometimes this is as easy as finding shared folders in Windows 9x or NT, or NFS exported directories in UNIX systems with read or read-write access to everyone. The intruder has no problem getting to the files. More often than not, the easily accessible information is highly confidential and completely unprotected from prying eyes, especially if the attacker is already an internal user.

System access is an intruder's ability to gain access to a machine that he is not allowed access to (such as when the intruder does not have an account or password). Entering or accessing systems that you don't have access to usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

Another form of access attacks involves privilege escalation. This is done by legitimate users who have a lower level of access privileges or intruders who have gained lower-privileged access. The intent is to get information or execute procedures that are unauthorized at the user's current level of access. In many cases this involves gaining root access in a UNIX system to install a sniffer to record network traffic, such as usernames and passwords, that can be used to access another target.

In some cases, intruders only want to gain access, not steal information-especially when the motive is intellectual challenge, curiosity, or ignorance.

DoS Attacks
DoS is when an attacker disables or corrupts networks, systems, or services with the intent to deny the service to intended users. It usually involves either crashing the system or slowing it down to the point where it is unusable. But DoS can also be as simple as wiping out or corrupting information necessary for business. In most cases, performing the attack simply involves running a hack, script, or tool. The attacker does not need prior access to the target, because usually all that is required is a way to get to it. For these reasons and because of the great damaging potential, DoS attacks are the most feared-especially by e-commerce website operators.

CertWays Q: 3
Which Cisco management product provides a Security Audit wizard?

A. Cisco Security Auditor
B. CiscoWorks VPN/Security Management Solution
C. Cisco Adaptive Security Device Manager
D. Cisco Router and Security Device Manager

Answer: D

CertWays Q: 4
Which three features of Cisco Security MARS provide for identity and mitigation of threats? (Choose three.)

A. determines security incidents based on device messages, events, and sessions

B. provides incident analysis that is topologically aware for visualization and replay
C. integrates with Trend Micro to clean infected hosts
D. performs mitigation on Layer 2 ports and at Layer 3 choke points
E. provides a security solution for preventing DDoS attacks
F. pushes signatures to Cisco IPS to keep viruses from entering the network

Answer: A,B,D

CertWays Q: 5
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

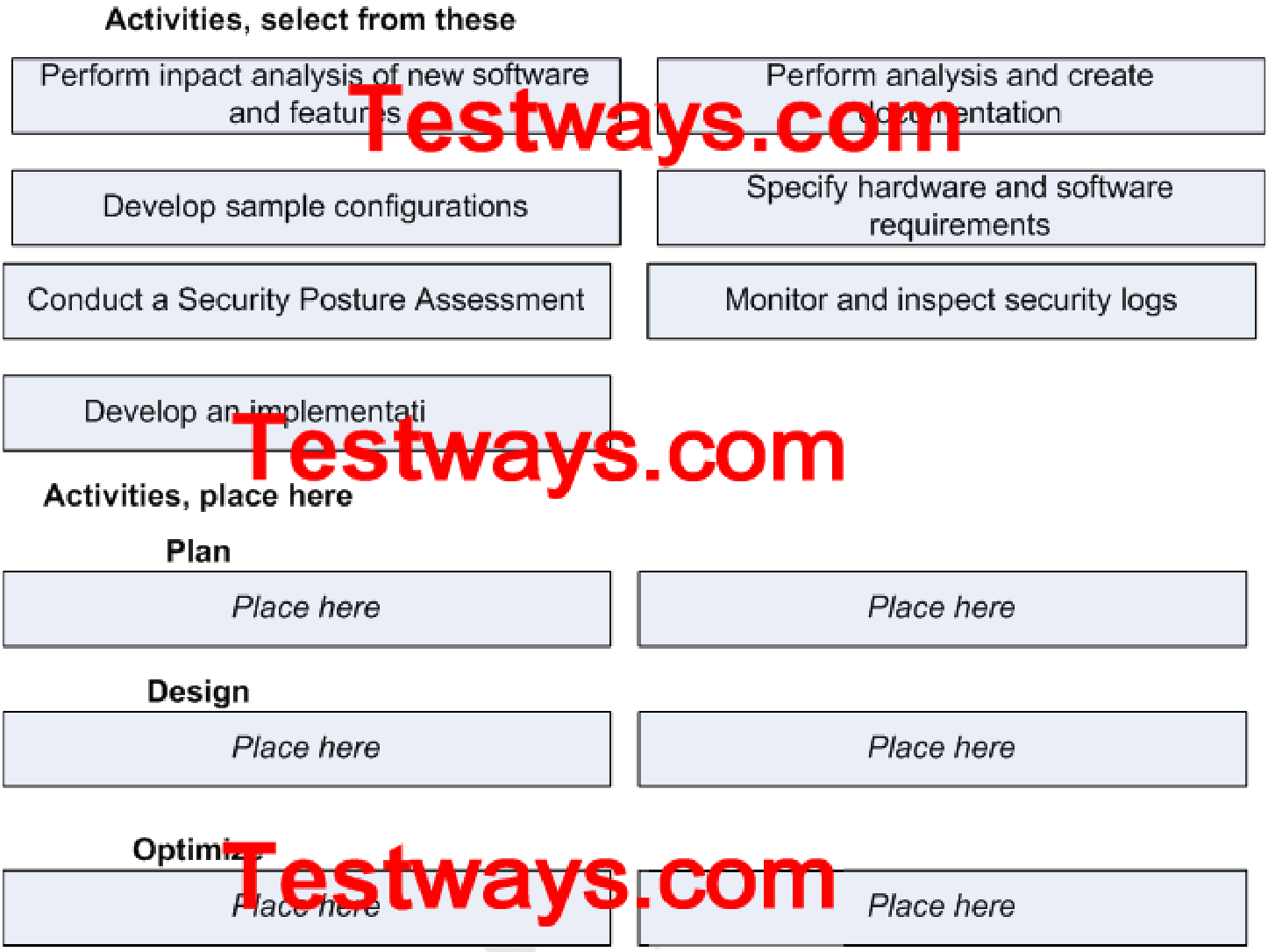
Answer: B

CertWays Q: 6
Which component of the Cisco NAC framework is responsible for compliance evaluation and policy enforcement?

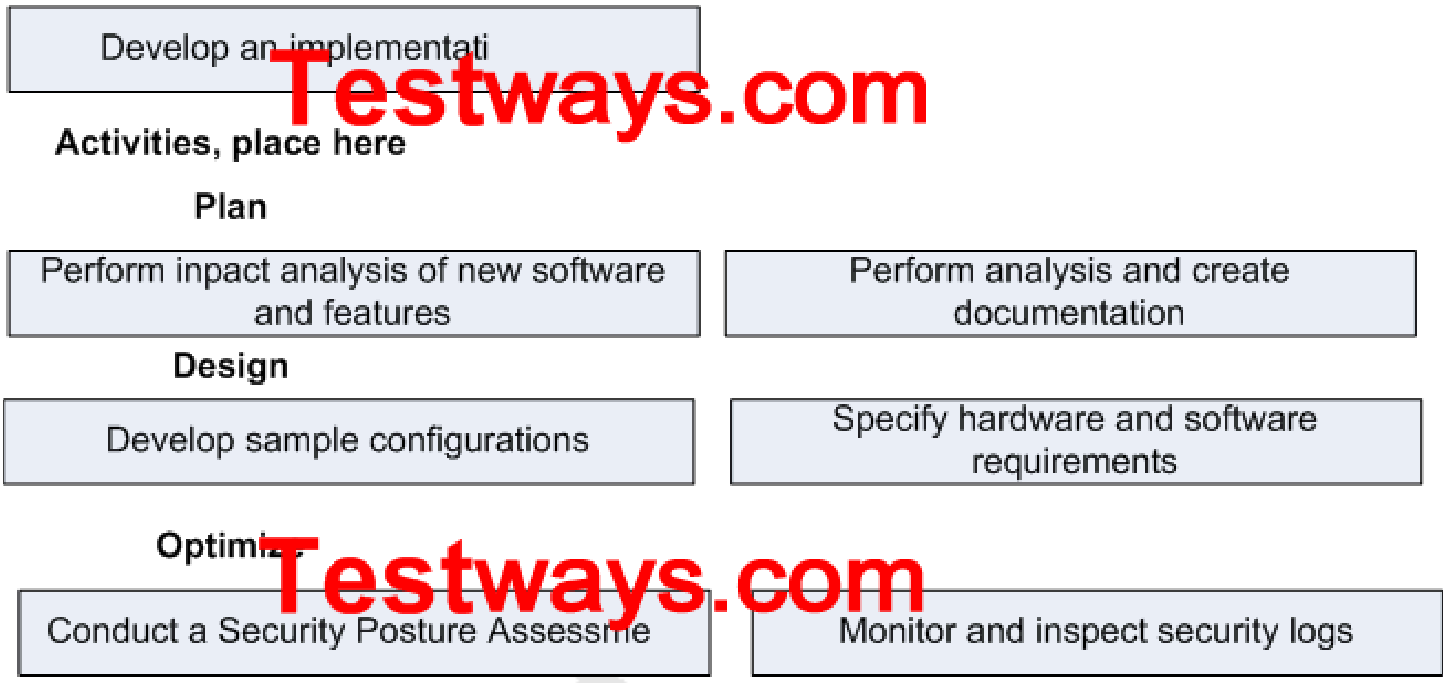
A. Cisco Secure ACS server
B. Cisco Trust Agent
C. network access devices
D. posture validation server

Answer: A

CertWays Q: 7 DRAG DROP
You work as a network technician at CertWays.com. Your trainee Sandra is curious about Network Security Lifecycles. Match each action with the appropriate task.



Answer:
Explanation:



CertWays Q: 8
What is a benefit of the Cisco Integrated Services Routers?

A. Intel Xeon CPUs
B. built-in event correlation engine
C. built-in encryption acceleration

D. customer programmable ASIC

Answer: C

CertWays Q: 9
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

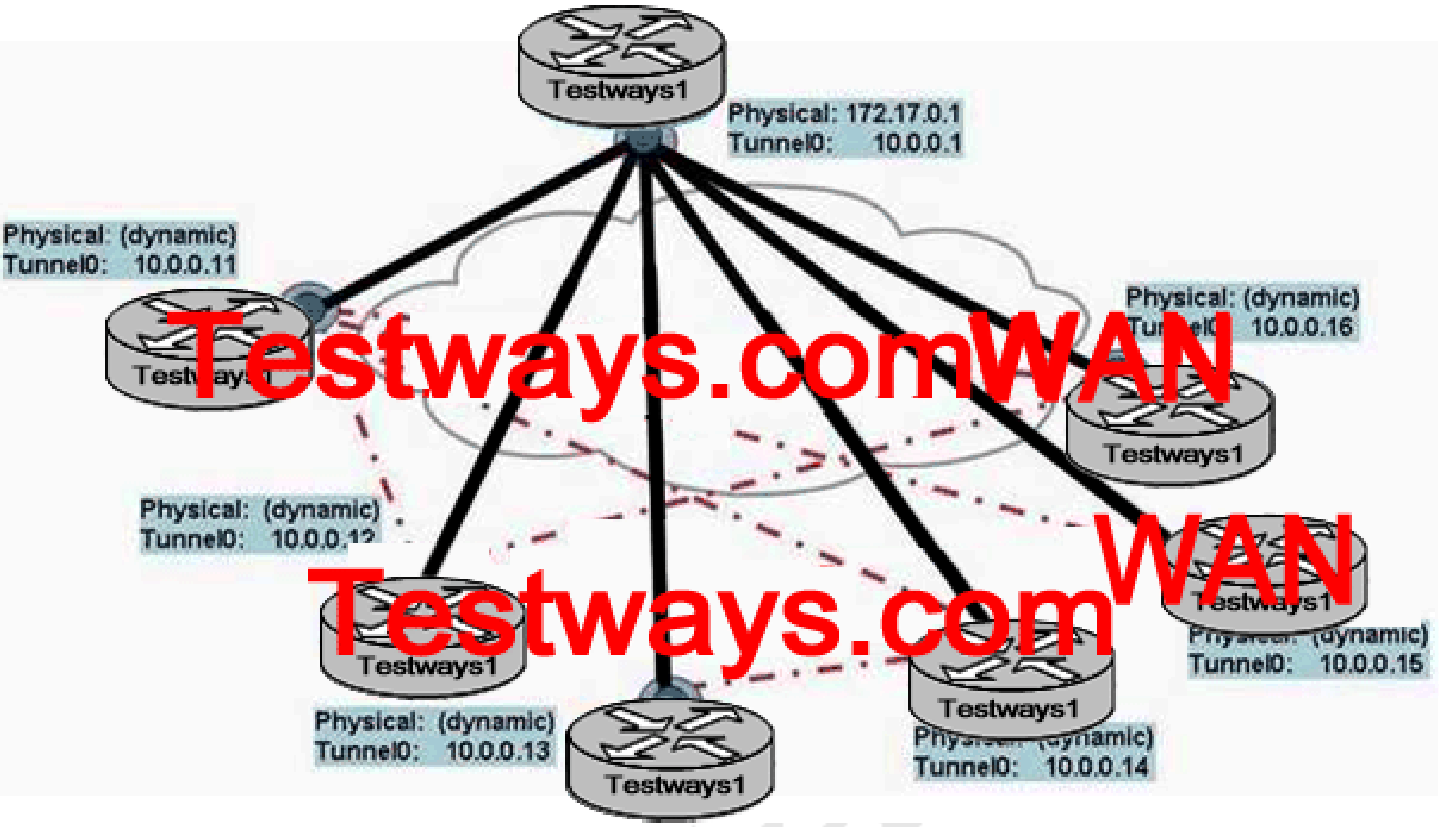
CertWays Q: 10
Which two features can the USB eToken for Cisco Integrated Services Router be used for? (Choose two.)

A. distribution and storage of VPN credentials
B. command authorization
C. one-time passwords
D. secure deployment of configurations
E. troubleshooting

Answer: A,D

CertWays Q: 11
Refer to the exhibit. As each spoke site is added, spoke-to-spoke and spoke-to-hub connectivity will be required. What is the best VPN implementation option?

Exhibit:



A. GRE over IPSec with dynamic routing
B. IPSec DMVPN
C. IPSec Easy VPN
D. V3PN

Answer: B

CertWays Q: 12
What is a benefit of IPSec + GRE?

A. bandwidth conservation
B. no need for a separate client
C. full support of Cisco dynamic routing protocols
D. support of dynamic connections

Answer: C

CertWays Q: 13
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

CertWays Q: 14
Which two statements about the Firewall Services Module are true? (Choose two.)

A. For traffic from high to low security levels, no access control list is needed.
B. Interfaces with the same security level cannot communicate without a translation rule.
C. Two VLAN interfaces connect MSFC and FWSM.
D. Up to 1 million simultaneous connections are possible.
E. Up to 100 separate security contexts are possible.

Answer: D,E

CertWays Q: 15
Andy, a network administrator at SomeCompany Ltd., is installing a new Cisco Security MARS appliance. After powering up the MARS appliance, what is a valid task?

A. Use a Category 5 crossover cable to connect the computer Ethernet port to the MARS eth0 port.
B. Connect a keyboard and monitor directly to the MARS appliance to set up its initial configuration.
C. Set the IP address of the computer to 192.168.1.100.
D. Telnet to 192.168.1.1 using the username pnadmin and the password pnadmin.

Answer: B
Explanation: B is preferred over A. because A talks about eth1 and not eth0 ... See below the three possibilities to establish initial communication for basic setup.

Establishing a Console ConnectionBefore you can perform the initial configuration of MARS Appliance, you must establish a console connection to it. You have three options for establishing an initial console connection, and four options after you complete the initial configuration. You must log in to the console using the system administrative account (pnadmin) and the password associated with that account, which is also pnadmin by default.
The three initial console connection options are:

Direct Console. Directly attach a keyboard and monitor the appliance. This option provides the most console feedback of the three console connection options, and it does not require any additional software, such as a terminal emulator or SSH client.

Serial Console. Before powering on the appliance, connect a computer to the serial port using the appropriate cable. For the location of the serial port, see the backplane figure corresponding to your appliance model in Hardware Descriptions, page 1-4. Configure your terminal emulation communication software (such as Hyper Terminal) to operate with the following settings:

-

Features, select from these

Peer router authentication

Features, place here

Application Security

Application inspection and control

Anti-X

Enhanced inline IPS

Containment and Control

Network Foundation Protection

Baud = 19200

-

Features, select from these

Peer router authentication

Features, place here

Application Security

Application inspection and control

Anti-X

Enhanced inline IPS

Containment and Control

Network Foundation Protection

Databits = 8

-

Features, select from these

Peer router authentication

Features, place here

Application Security

Application inspection and control

Anti-X

Enhanced inline IPS

Containment and Control

Network Foundation Protection

Parity = None

-

Features, select from these

Peer router authentication

Features, place here

Application Security

Application inspection and control

Anti-X

Enhanced inline IPS

Containment and Control

Network Foundation Protection

Stops = 1

-

Features, select from these

Peer router authentication

Features, place here

Application Security

Application inspection and control

Anti-X

Enhanced inline IPS

Containment and Control

Network Foundation Protection

Flow control = None

Ethernet Console. Before powering on the appliance, connect a computer to eth1 using a crossover CAT5 cable, configuring the computer's local TCP/IP settings to be on the 192.168.0.0 network. Pick an IP address other than 192.168.0.100 and 192.168.0.101, which are the default addresses assigned to eth0 and eth1, respectively. The eth1 port is reserved for administrative connections, such as the Ethernet console. For the location of the eth1 port, see the backplane figure corresponding to your appliance model in Hardware Descriptions, page 1-4. Configure your terminal emulation communication software (such as Hyper Terminal) to operate with the following settings:

-

Features, select from these

Peer router authentication

Features, place here

Application Security

Application inspection and control

Anti-X

Enhanced inline IPS

Containment and Control

Network Foundation Protection

Baud = 19200

-

Features, select from these

Peer router authentication

Features, place here

Application Security

Application inspection and control

Anti-X

Enhanced inline IPS

Containment and Control

Network Foundation Protection

Databits = 8

-

Features, select from these

Peer router authentication

Features, place here

Application Security

Application inspection and control

Anti-X

Enhanced inline IPS

Containment and Control

Network Foundation Protection

Parity = None

-

Features, select from these

Peer router authentication

Features, place here

Application Security

Application inspection and control

Anti-X

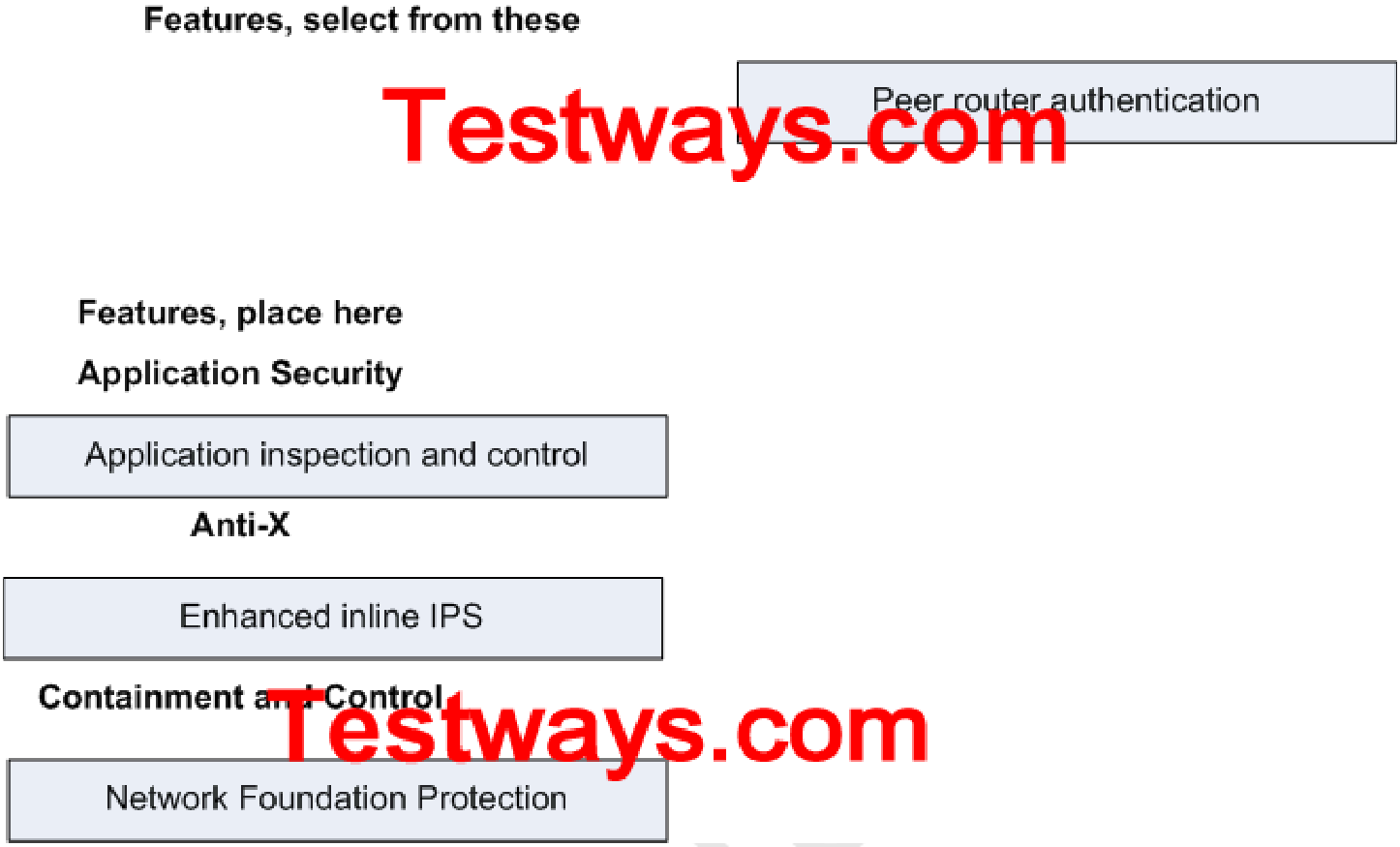
Enhanced inline IPS

Containment and Control

Network Foundation Protection

Stops = 1

-



Flow control = None

CertWays Q: 16
Which Cisco security product is an easily deployed software solution that can automatically detect, isolate, and repair infected or vulnerable devices that attempt to access the network?

A. Cisco Security Agent
B. Cisco Secure ACS server
C. NAC Appliance (Cisco Clean Access)
D. Cisco Traffic Anomaly Detector

Answer: C

CertWays Q: 17
What is a benefit of high-performance AIM that is included with Cisco Integrated Services Routers?

A. hardware-accelerated packet inspection engine
B. hardware-based encryption and compression
C. removable secure credentials
D. support of SRTP

Answer: B

CertWays Q: 18
In the context of Cisco NAC, what is a network access device?

A. workstation without Cisco Trust Agent
B. Cisco IOS router
C. AAA server
D. laptop with Cisco Trust Agent

Answer: B

CertWays Q: 19
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

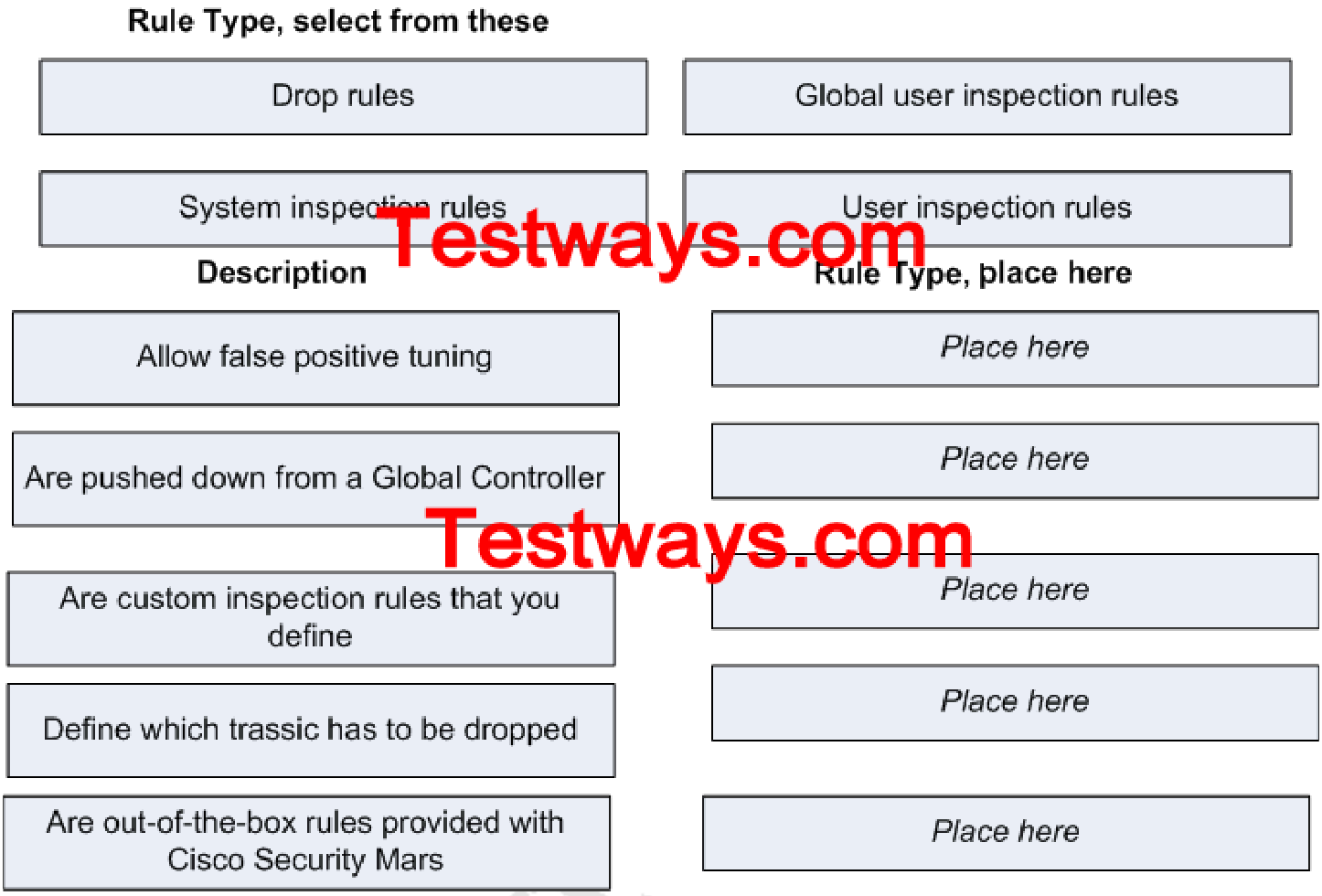
CertWays Q: 20
Which two should be included in an analysis of a Security Posture Assessment? (Choose two.)

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

CertWays Q: 21
Refer to the exhibit. Network security is a continuous process that is built around which element?

Exhibit:



A. business requirements
B. corporate security policy
C. customer needs
D. security best practice

Answer: B

CertWays Q: 22 DRAG DROP
You work as a network technician at CertWays.com. Your boss, Mrs Tess King, is curious about Cisco IOS Adaptive Threat Defense. You try to explain by matching the features with the appropriate functions.

Rule Type, select from these

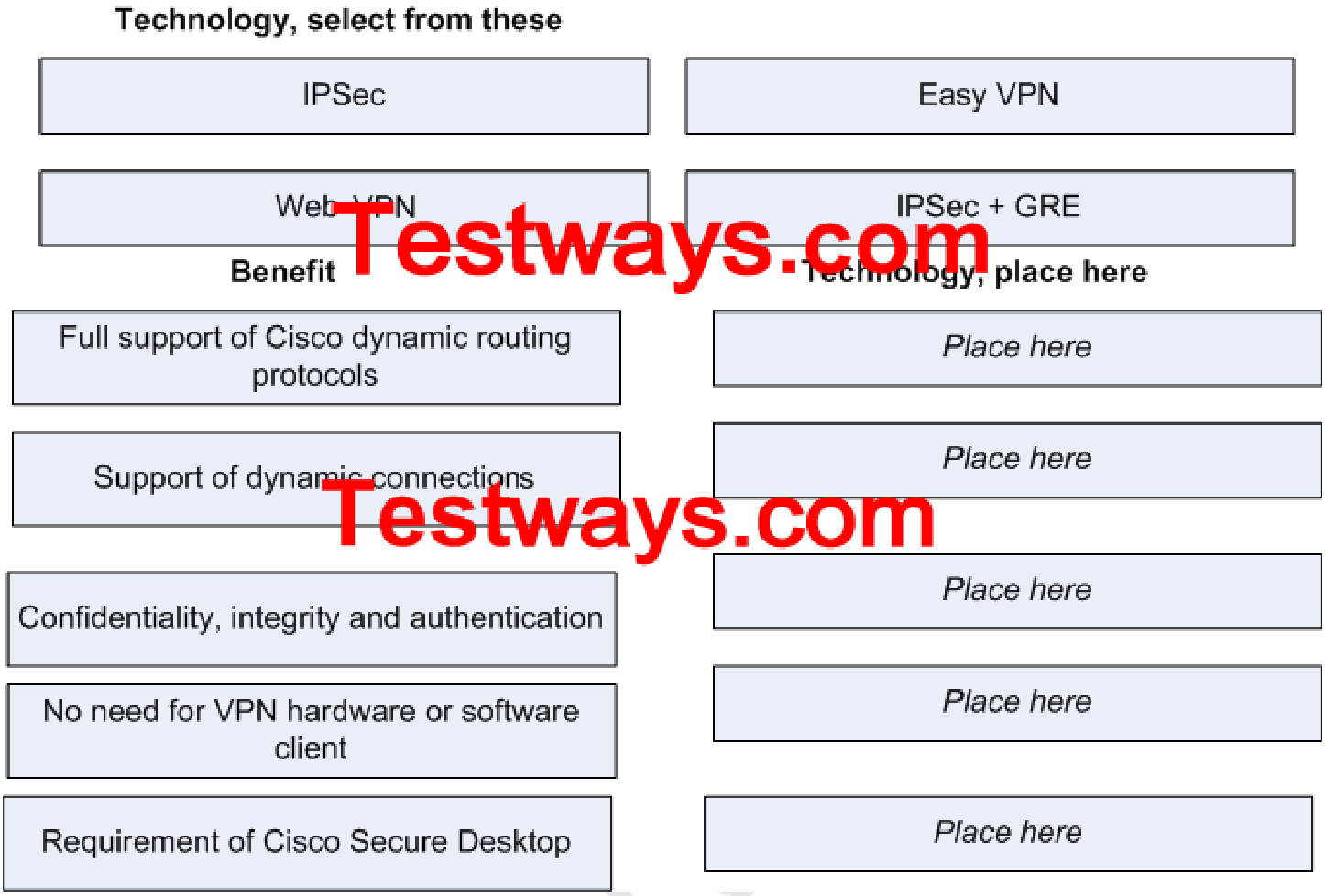
Description	Rule Type, place here
Allow false positive tuning	Drop rules
Are pushed down from a Global Controller	Global user inspection rules
Are custom inspection rules that you define	User inspection rules
Define which traffic has to be dropped	*Place here*
Are out-of-the-box rules provided with Cisco Security Mars	System inspection rules

Answer:

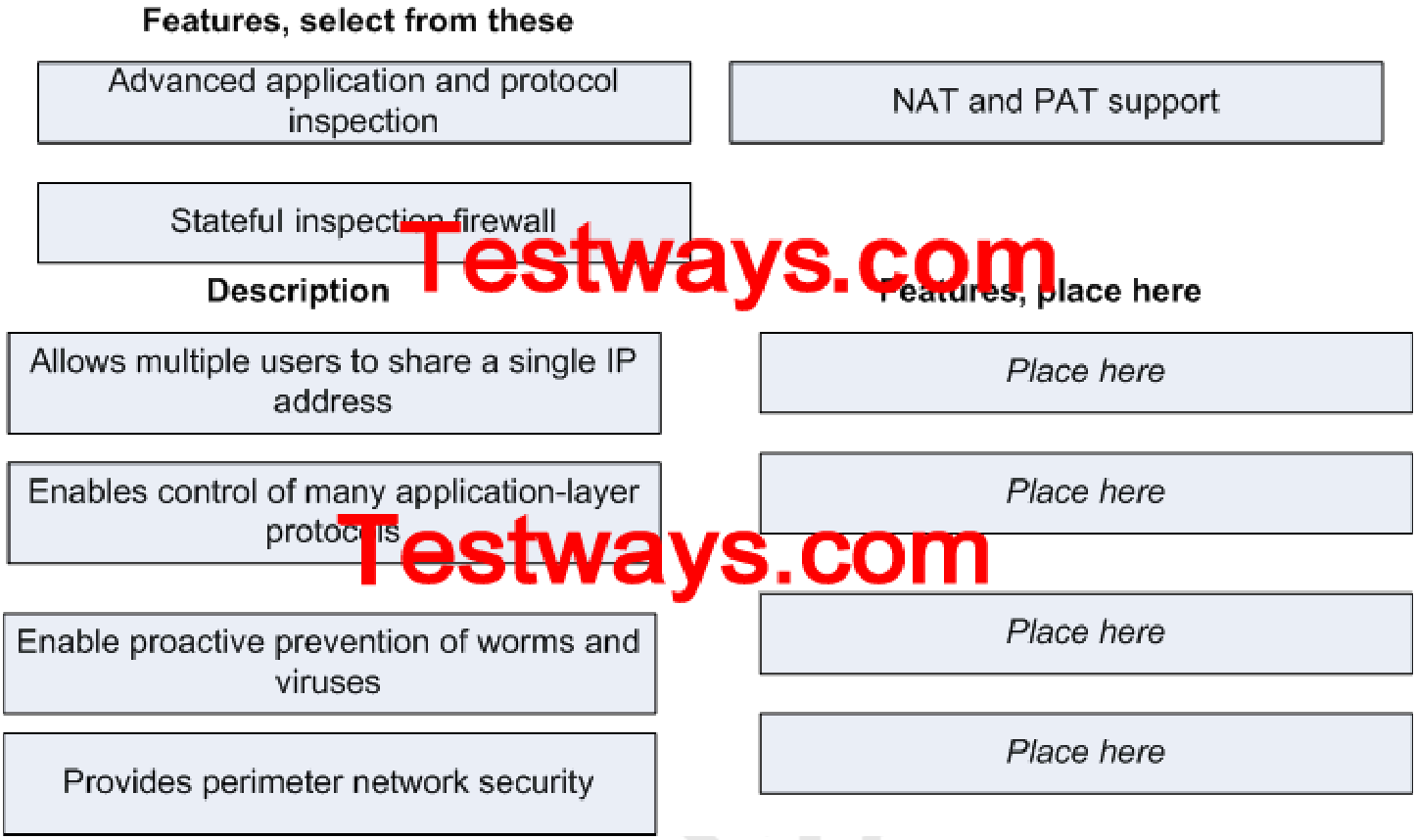
Explanation:

CertWays Q: 23 DRAG DROP
You work as a network technician at CertWays.com. Your boss, Mrs Tess King, is curious about rule types. You try to explain by matching the features with the appropriate functions.

Use each rule type once and only once.



Answer:
Explanation:



CertWays Q: 24
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

CertWays Q: 25

In which two ways can a Security Posture Assessment help organizations to understand network threats and risk? (Choose two.)

A. by coaching system administrators
B. by identifying bottlenecks
C. by identifying vulnerable systems
D. by recommending areas to improve
E. by recommending new products

Answer: C,D

CertWays Q: 26
Self-Defending Network is the Cisco vision for security systems. What is the purpose of the Cisco Secure ACS server?

A. anomaly detection
B. identity management
C. secure connectivity
D. security management

Answer: B

CertWays Q: 27
Which two are valid arguments that you can 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. Cisco products can provide end-to-end network protection against current and emerging threats.
C. The network should be secured at any expense.
D. Network security products are complex to manage and that makes them hard to penetrate.
E. Organizations that operate vulnerable networks face increasing liability.

Answer: B,E

CertWays Q: 28
What is the main reason for customers to implement the Cisco Detector and Guard solution?

A. as a replacement for IPS sensors
B. as a DDoS protection system
C. as a complete appliance-based NAC solution
D. as a replacement for firewalls

Answer: B

CertWays Q: 29
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

CertWays Q: 30
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

CertWays Q: 31
When implementing a Cisco Integrated Services Router, which feature would you apply to achieve application security?

A. access control lists
B. alerts and audit trails
C. lock-and-key (dynamic access control lists)
D. Context-based Access Control

Answer: D

CertWays Q: 32
Which statement is true about the built-in hardware-based encryption that is included with Cisco Integrated Services Routers?

A. It supports SRTP.
B. It supports 256-bit AES encryption.
C. It is two times faster than previous modules.
D. It stores VPN credentials.

Answer: B

CertWays Q: 33
Tess king is a network administrator at CertWays.com. CertWays.com wants to implement command authorization for tighter control of user access rights. Which combination of authentication server and authentication protocol is able to best meet this requirement?

A. Cisco Secure ACS server and RADIUS
B. Cisco Secure ACS server and TACACS+
C. Microsoft IAS server and RADIUS
D. Microsoft Windows Domain Controller and Kerberos

Answer: B

CertWays Q: 34 DRAG DROP
You work as a network technician at CertWays.com. Your boss, Mrs Tess King, is curious about secure features. Match the features with the appropriate description.

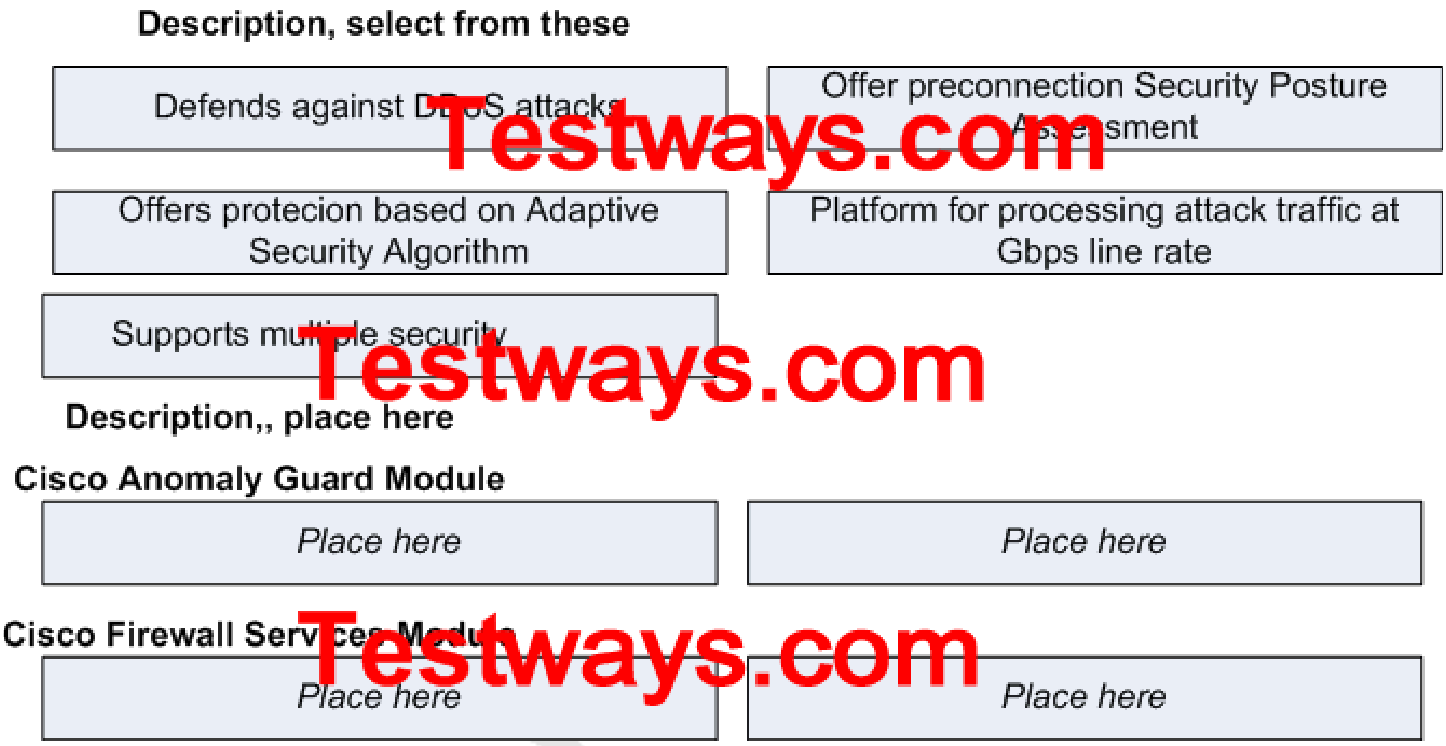
Description	Features, place here
Allows multiple users to share a single IP address	NAT and PAT support
Enables control of many application-layer protocols	Advanced application and protocol inspection
Enable proactive prevention of worms and viruses	*Place here*
Provides perimeter network security	Stateful inspection firewall

Use each feature once and only once.

Answer:
Explanation: Pending. Send your suggestion to feedback@CertWays.com

CertWays Q: 35 DRAG DROP
You work as a network technician at CertWays.com. Your boss, Mrs Tess King, is curious about secure Cisco IOS VPN technology. Match the technology with the appropriate benefit.

Use each technology once and only once.

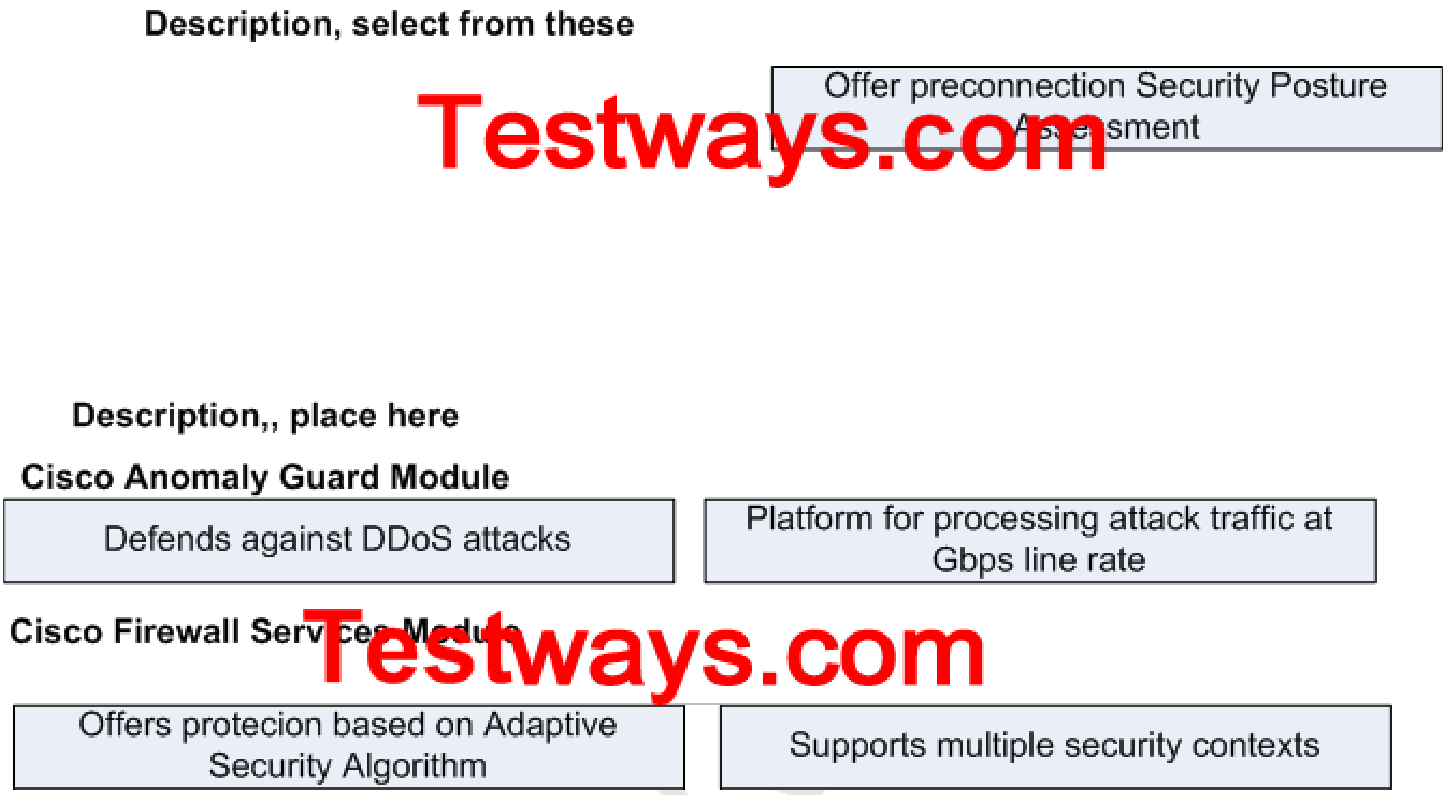


Answer:
Explanation: Pending. Send your suggestion to feedback@CertWays.com

CertWays Q: 36 DRAG DROP

You work as a network technician at CertWays.com. Your boss, Mrs Tess King, is curious about firewall features. Match the features with the appropriate descriptions.

Use each feature once and only once.



Answer:
Explanation:

CertWays Q: 37
What is a feature or function of Cisco Security MARS?

A. enforces authorization policies and privileges
B. determines security incidents based on device messages, events, and sessions
C. configures, monitors, and troubleshoots Cisco security products
D. supports AAA user login authentication

Answer: B

CertWays Q: 38
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

CertWays Q: 39 DRAG DROP
You work as a network technician at CertWays.com. Your boss, Mrs Tess King, is curious about Cisco Security modules. Match the modules with the appropriate descriptions.

Not all descriptions are used.

Products, select from these

Products, place here

Compliance

Enforcement

Management

Protection

Answer:
Explanation:

CertWays Q: 40
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

CertWays Q: 41
What could be a reason to implement Cisco Security Agent?

A. preventing Day Zero attacks
B. communicating the host posture validation to a policy server
C. tracking the Internet usage of employees
D. validating policy compliance

Answer: A

CertWays Q: 42
Which two are parts of the Network Security Lifecycle? (Choose two.)

A. Purchase
B. Operate
C. Integrate
D. Design
E. Develop

Answer: B,D

CertWays Q: 43
On the Cisco Security MARS appliance, what is used to faciliate the management of Event, IP, Service and User management?

A. groups
B. custom parser
C. rules
D. signatures
E. audit trail log

Answer: A

CertWays Q: 44
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 version 5.0 technology
D. network security event correlation
E. Cisco IOS AutoSecure

Answer: A,C

CertWays Q: 45
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

CertWays Q: 46
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

CertWays Q: 47
Which Cisco IOS feature uses multipoint GRE and the Next Hop Resolution Protocol to create dynamic IPSec tunnels between spoke (branch) sites?

A. Easy VPN
B. V3PN
C. DMVPN
D. Web VPN

Answer: C

CertWays Q: 48
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

CertWays Q: 49
Which three are included with the Cisco Security Agent? (Choose three.)

A. buffer overflow protection
B. Day Zero virus and worm protection
C. Cisco Easy VPN Client
D. host-based intrusion prevention
E. plug-in interface to query posture providers
F. packet sniffer

Answer: A,B,D

CertWays Q: 50
What is a valid step when setting up the Cisco Security MARS appliance for data archiving?

A. Specify the remote CIFS server.
B. Specify the remote FTP server.
C. Specify the remote NFS server.
D. Specify the remote TFTP server.

Answer: C

CertWays Q: 51
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

CertWays Q: 52
Which two components should be included in a detailed design document? (Choose two.)

A. data source

B. existing network infrastructure
C. organizational chart
D. proof of concept
E. vendor availability

Answer: B,D

CertWays Q: 53
Identify two ways to create a long-duration query on the Cisco Security MARS appliance. (Choose two.)

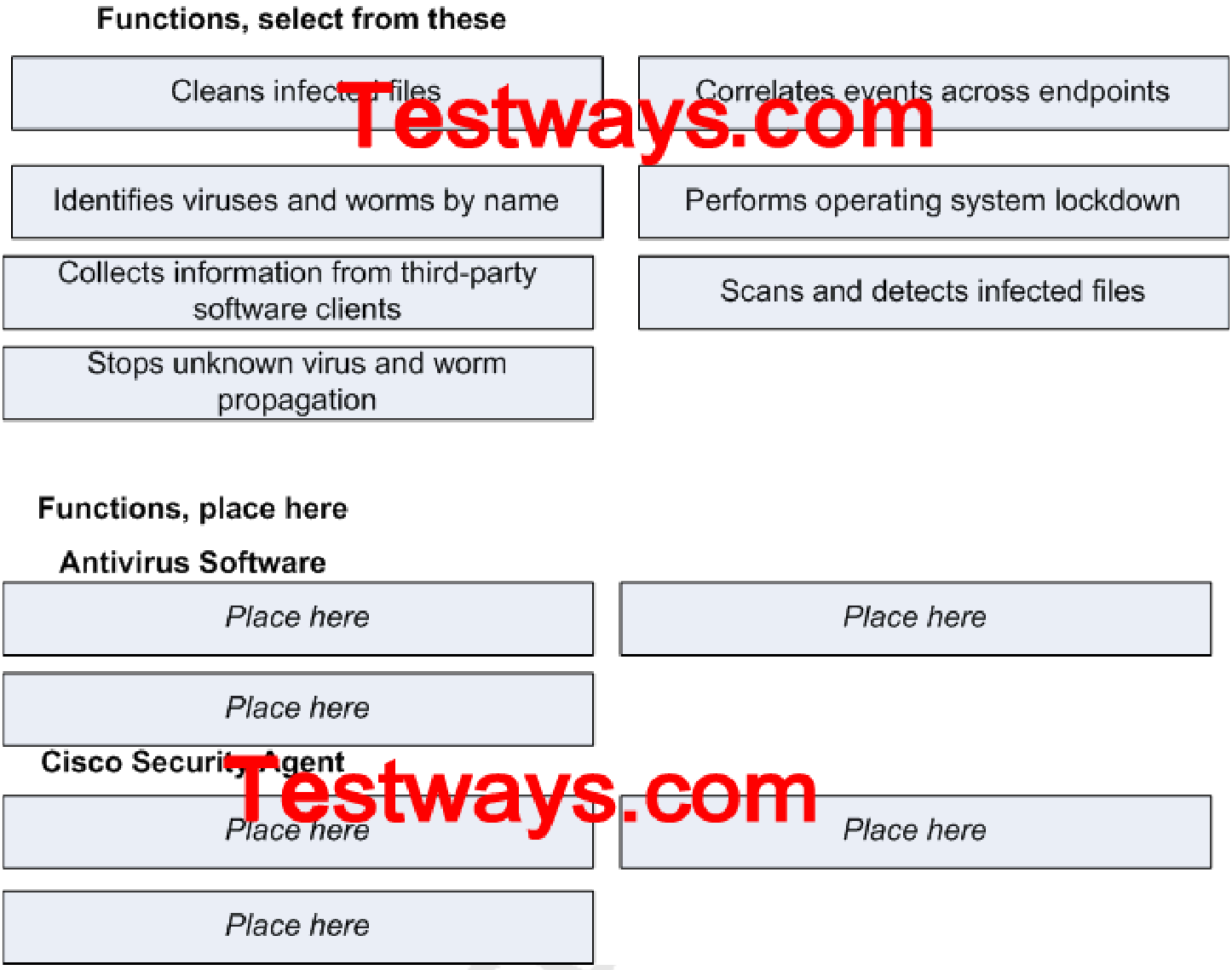
A. by modifying an existing report
B. by saving a query as a report
C. by submitting a query in line
D. by submitting a batch query
E. by saving a query as a rule

Answer: A,D

CertWays Q: 54 DRAG DROP
You work as a network technician at CertWays.com. Your boss, Mrs Tess King, is curious about Cisco Security products.. Match the products with the appropriate NAC framework.

Not all products are used.

Answer:
Explanation:



CertWays Q: 55
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

CertWays Q: 56
In which two ways does 802.1x benefit businesses in terms of trust and identity? (Choose two.)

A. allows a user-based policy to be dynamically applied to switched ports
B. identifies which client is consuming how much bandwidth
C. prevents any unauthorized device from connecting
D. probes client devices for compliance
E. stops malicious code from entering the network

Answer: A,C

CertWays Q: 57
Which three should be included in a system acceptance test plan? (Choose three.)

A. features to be tested
B. indication of references
C. pass and fail criteria
D. product data sheets
E. recommended changes
F. resource requirements and schedules

Answer: A,C,F

CertWays Q: 58
What are two beneficial functions of the CiscoWorks VPN/Security Management Solution? (Choose two.)

A. detects, locates, and mitigates rogue access points
B. performs dynamic visualization for fast and intuitive threat identification, tracking, and analysis
C. performs monitoring and tracking of network response time and availability
D. provides functions for monitoring and troubleshooting the health and performance of security devices
E. performs real-time monitoring of site-to-site VPN, remote-access VPN, firewall, and IPS services

Answer: D,E

CertWays Q: 59
Which two are valid methods for adding reporting devices into the Cisco Security MARS appliance? (Choose two.)

A. running an Import Wizard
B. importing the devices from CiscoWorks VPN/Security Management Solution
C. loading the devices from a seed file
D. running manual configuration
E. using CDP to auto discover the Cisco reporting devices

Answer: C,D

CertWays Q: 60
What is a valid method of verifying a network security design?

A. network audit
B. network health analysis
C. network performance test
D. pilot or prototype network

Answer: D

CertWays Q: 61 DRAG DROP
You work as a network technician at CertWays.com. Your boss, Mrs Tess King, is curious about Cisco Security products. Match the products with the appropriate feature.

Use each product once and only once.

Functions, select from these

Collects information from third-party software clients

Functions, place here

Antivirus Software

Cleans infected files

Identifies viruses and worms by name

Scans and detects infected files

Cisco Security Agent

Correlates events across endpoints

Performs operating system lockdown

Stops unknown virus and worm propagation

Answer:
Explanation:

CertWays Q: 62
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

CertWays Q: 63
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

CertWays Q: 64
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: B,C,E
Explanation:
Not A: Generally spyware and adware are more signature based.

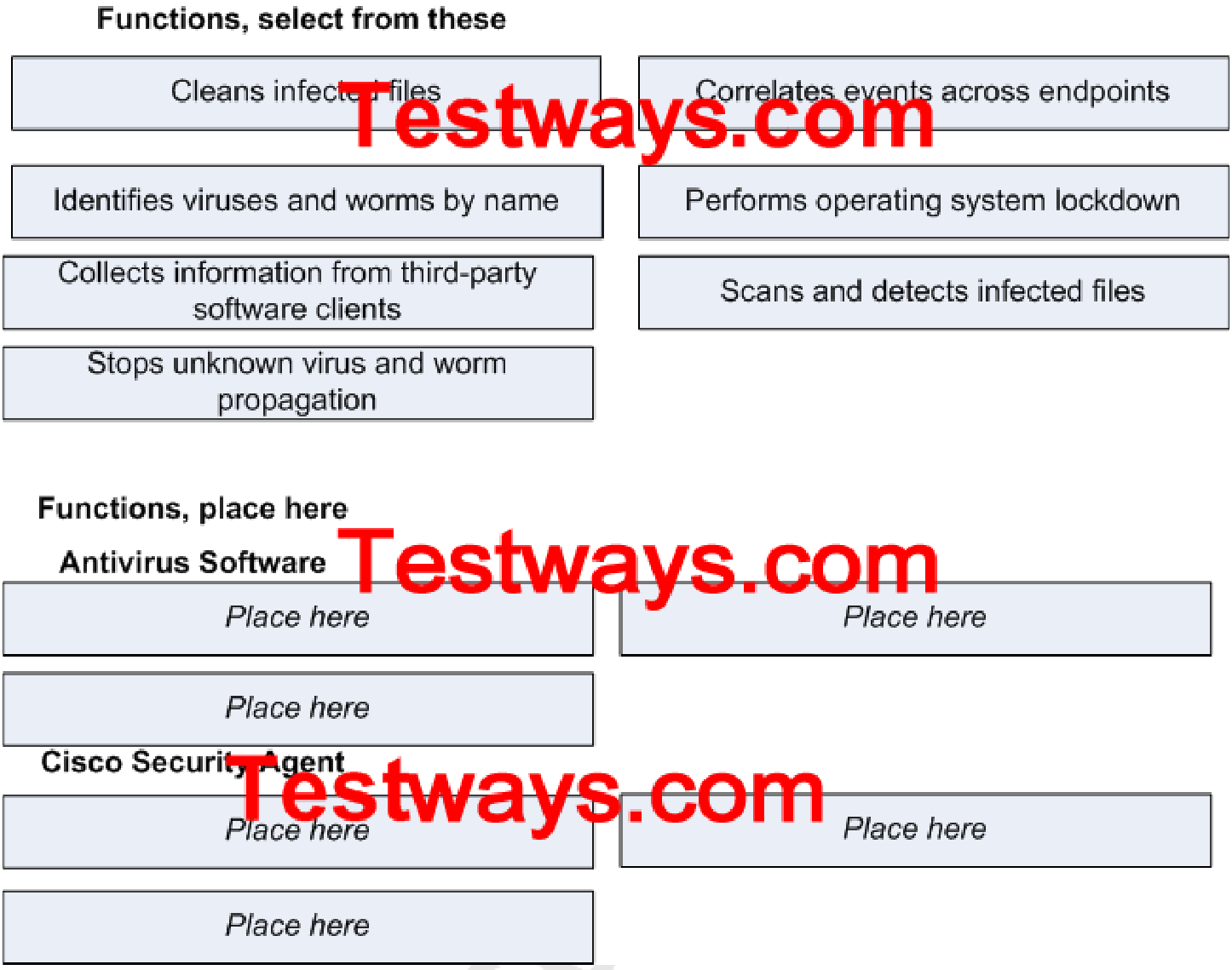
CertWays Q: 65
Which Cisco security product can be used to perform a Security Posture Assessment of client workstations?

A. Cisco Easy VPN Client
B. NAC Appliance Manager (NAM)
C. Cisco Security Agent
D. Cisco Trust Agent

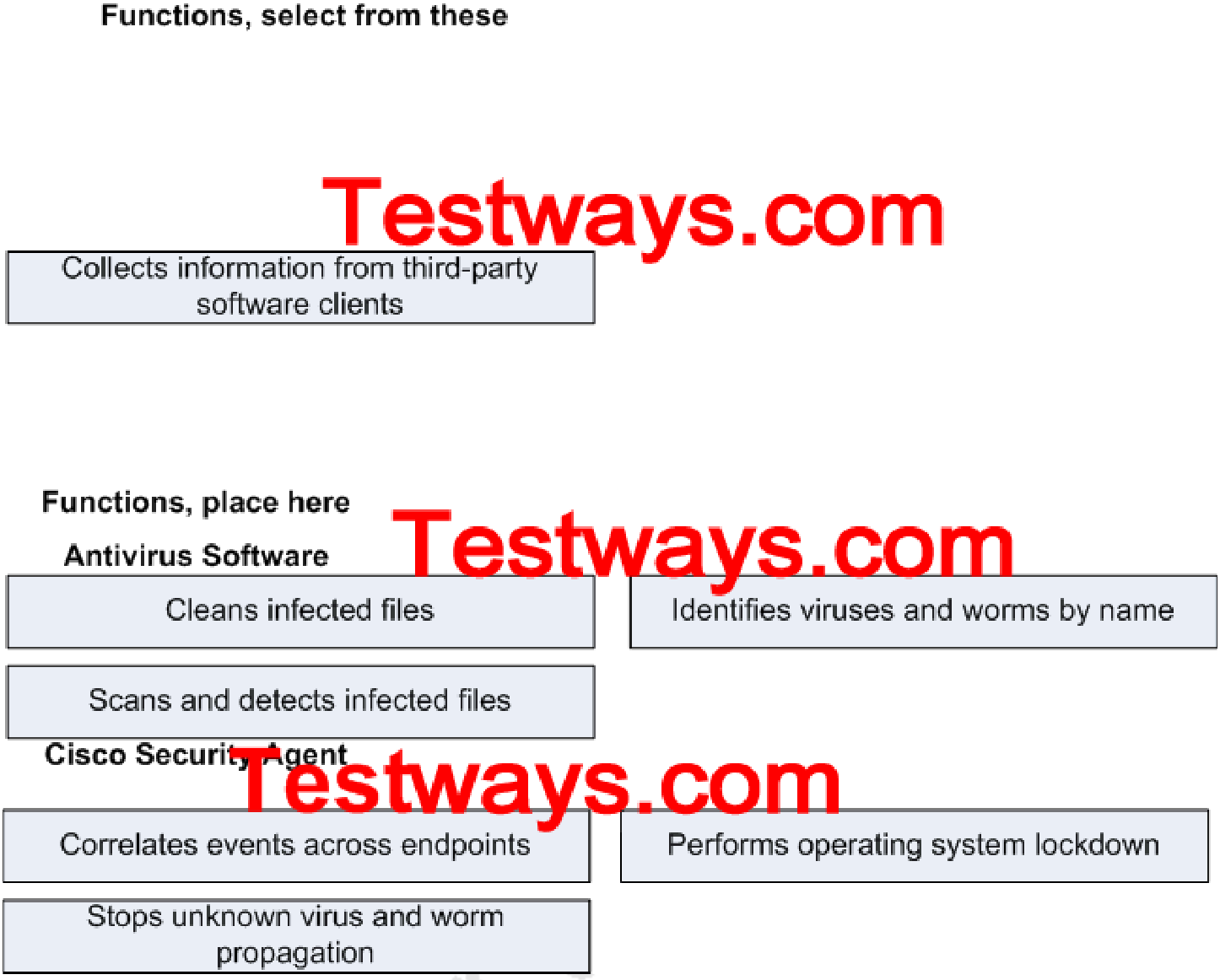
Answer: D

CertWays Q: 66 DRAG DROP
You work as a network technician at CertWays.com. Your boss, Mrs Tess King, is curious about security products. Match the products with the appropriate functions.

Not all functions are used.



Answer:
Explanation:



CertWays Q: 67
How can you configure a Cisco Security MARS appliance to send notifications via e-mail, pager, syslog, SNMP, or SMS?

A. by creating an event filter

B. by defining the rule "Action"
C. by escalating an incident
D. by running a batch query

Answer: B

CertWays Q: 68
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

CertWays Q: 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

CertWays Q: 70
By providing a detailed inspection of traffic in Layers 2 through 7, the Cisco IPS appliance offers which benefit to the customers?

A. full network access control
B. detection of Internet access misuse by employees
C. effective prevention of distributed denial of service attacks
D. prevention of protocol misuse (for example, tunneling through port 80)

Answer: D