Exam : 642-564

Title : Security Solutions for Systems Engineers

Ver : 10-12-07

QUESTION 1:

A new MARS appliance has been installed in the Certkiller network. Which protocol is used for transporting the event data from Cisco IPS 5.0 and later devices to the Cisco Security MARS appliance?

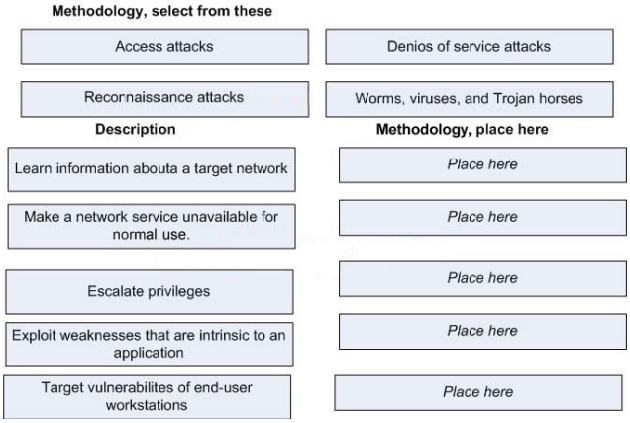
A. RDEP over SSL
B. SDEE over SSL
C. SSH
D. SYSLOG
E. All of the above

Answer: B

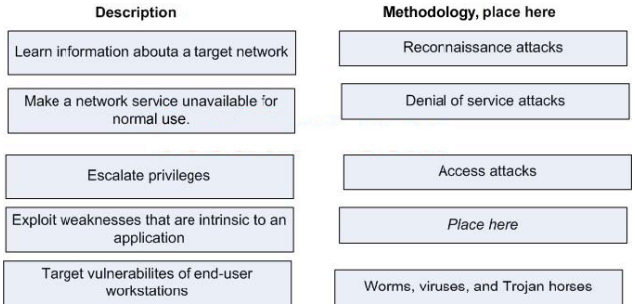
Explanation:
For Cisco IPS 5.x devices, MARS pulls the logs using SDEE (Security Device Event Exchange) over SSL. Therefore, MARS must have HTTPS access to the sensor.
Reference:
http://www.cisco.com/en/US/products/ps6241/products_user_guide_chapter09186a008074f213.html

QUESTION 2:

DRAG DROP
You work as a network technician at Certkiller .com. Your boss, Mrs Certkiller, 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.

QUESTION 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
E. None of the above

Answer: D

Explanation:
In the Cisco Router and Security Device Manager, the Security Audit is a feature that examines your existing router configurations and then updates your router in order to make your router and network more secure. Security Audit is based on the Cisco IOS AutoSecure feature; it performs checks on and assists in configuration of almost all of the AutoSecure functions.
Security Audit operates in one of two modes-the Security Audit wizard, which lets you choose which potential security-related configuration changes to implement on your router, and One-Step Lockdown, which automatically makes all recommended security-related configuration changes.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_chapter09186a0080656061.htm

---

QUESTION 4:

A new MARS appliance has been installed in the Certkiller network. 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

Explanation:
Cisco Security MARS obtains network intelligence by understanding the topology and device configurations from routers, switches, and firewalls, and by profiling network traffic. The system's integrated network discovery function builds a topology map containing device configuration and current security policies, which enables it to model packet flows through your network. Since the appliance does not operate inline and makes minimal use of existing software agents, there is little impact on network or system performance.
The appliance centrally aggregates logs and events from a wide range of popular network devices (such as routers and switches), security devices and applications (such as firewalls, intrusion detection systems [IDSs], vulnerability scanners, and antivirus applications), hosts (such as Windows, Solaris, and Linux syslogs), applications (such as databases, Web servers, and authentication servers), and network traffic (such as Cisco NetFlow).
Cisco Security MARS transforms raw network and security data into intelligence that can be used to subvert valid security incidents and maintain compliance. This easy-to-use family of threat mitigation appliances enables operators to centralize, detect, mitigate, and report on priority threats using the network and security devices already deployed in your infrastructure. The threat mitigation features of MARS can be used to isolate and prevent problems from spreading in the network by stopping them key layer 2 and layer 3 network points.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 6, page 4-1 through 4-14.

QUESTION 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
F. None of the above

Answer: B

Explanation:
The Control Plane Policing feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of CiscoIOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

To configure, follow these detailed steps:

	Command or Action	Purpose
Step 1	**Enable** Example: Router> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** Example: Router# **configure terminal**	Enters global configuration mode.
Step 3	Control-plane Example: Router(config)# control-plane	Enters control-plane configuration mode to attach a QoS policy that manages CP traffic.
Step 4	**Service-policy** (**input** | **output**) *policy-map-name* Example: Router(config-cp)# **service-policy input control-plane-policy**	Attaches a QoS service policy to the control plane. • **input**—Applies the specified service policy to packets received on the control plane. • **output**—Applies the specified service policy to packets transmitted from the control plane and enables the router to silently discard packets. • *policy-map-name*—Name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a008052446b.html

---

QUESTION 6:

The Certkiller network is using NAC. 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

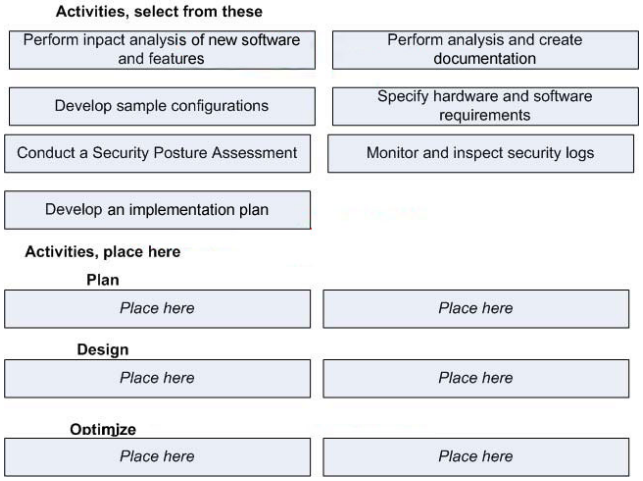
Answer: A

Explanation:
Cisco Secure ACS extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework, thereby allowing greater flexibility and mobility, increased security, and user productivity gains.
Cisco Secure ACS is an important component of the Cisco Network Admission Control (NAC)-an industry initiative sponsored by Cisco Systems that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. Cisco Secure ACS 4.0 acts as a policy decision point in NAC deployments, evaluating credentials, determining the state of the host, and sending out per-user authorization to the network access devices.
Reference: http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html

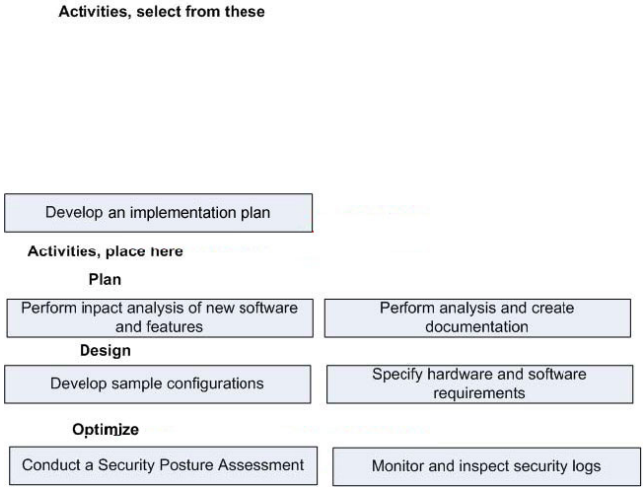
---

QUESTION 7:

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



Answer:



QUESTION 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

Explanation:
The Cisco 800, 1800, 2800, and 3800 Integrated Services Routers (ISR) were designed to incorporate security in every router by making hardware-based encryption a standard feature. This built-in, hardware-based encryption acceleration offloads the VPN

processes to provide increased VPN throughput with minimal impact on the router CPU. If additional VPN throughput or scalability is required, optional VPN encryption advanced integration modules (AIMs) are available.

QUESTION 9:

The Certkiller network has just implemented CSA for all end hosts. 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

Explanation:
The functions of the CSA are system hardening, resource protection, control of executable content, application control, and detection.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 4, page 4-3.

QUESTION 10:

The Certkiller network just upgraded to the ISR router series. Which two features can the USB eToken for Cisco Integrated Services Router be used for? (Choose two)

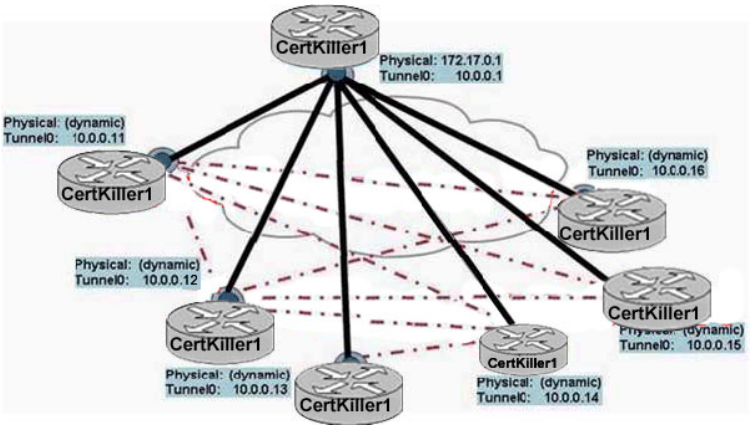
A. Distribution and storage of VPN credentials
B. Command authorization
C. One-time passwords
D. Secure deployment of configurations
E. Troubleshooting

Answer: A, D

Explanation:
The Cisco IOS Software-level integration of Aladdin's eToken drivers provides partners and customers with enhanced security router practices:
1. Secure Provisioning of Cisco Router Configurations: Combining eToken drivers with Cisco integrated services routers helps Cisco partners mount router configuration on eToken and securely send them to end customers.
2. Portable Credential Storage for Cisco VPN: VPN credential storage on eToken provides off-platform generation and secure storage of VPN credentials. Encryption keys are loaded when eToken is plugged in, and removed when eToken is removed.
Reference: http://www.aladdin.com/etoken/demos/cisco/ask.asp

QUESTION 11:

Refer to the exhibit below. As each spoke site is added, spoke-to-spoke and spoke-to-hub connectivity will be required. What is the best VPN implementation option in this scenario?
Exhibit:



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

Answer: B

Explanation:
The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IP Security (IPsec) Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP).
Benefits of Dynamic Multipoint VPN (DMVPN)
Hub Router Configuration Reduction:
Currently, for each spoke router, there is a separate block of configuration lines on the hub router that define the crypto map characteristics, the crypto access list, and the GRE tunnel interface. This feature allows users to configure a single mGRE tunnel interface, a single IPsec profile, and no crypto access lists on the hub router to handle all spoke routers. Thus, the size of the configuration on the hub router remains constant even if spoke routers are added to the network.
DMVPN architecture can group many spokes into a single multipoint GRE interface, removing the need for a distinct physical or logical interface for each spoke in a native IPsec installation.
Automatic IPsec Encryption Initiation
GRE has the peer source and destination address configured or resolved with NHRP. Thus, this feature allows IPsec to be immediately triggered for the point-to-point GRE tunneling or when the GRE peer address is resolved via NHRP for the multipoint GRE tunnel.

Support for Dynamically Addressed Spoke Routers
When using point-to-point GRE and IPsec hub-and-spoke VPN networks, the physical interface IP address of the spoke routers must be known when configuring the hub router because IP address must be configured as the GRE tunnel destination address. This feature allows spoke routers to have dynamic physical interface IP addresses (common for cable and DSL connections). When the spoke router comes online, it will send registration packets to the hub router: within these registration packets, is the current physical interface IP address of this spoke.
Dynamic Creation for Spoke-to-Spoke Tunnels
This feature eliminates the need for spoke-to-spoke configuration for direct tunnels. When a spoke router wants to transmit a packet to another spoke router, it can now use NHRP to dynamically determine the required destination address of the target spoke router. (The hub router acts as the NHRP server, handling the request for the source spoke router.) The two spoke routers dynamically create an IPsec tunnel between them so data can be directly transferred.
VRF Integrated DMVPN
DMVPNs can be used to extend the Multiprotocol Label Switching (MPLS) networks that are deployed by service providers to take advantage of the ease of configuration of hub and spokes, to provide support for dynamically addressed customer premises equipment (CPEs), and to provide zero-touch provisioning for adding new spokes into a DMVPN.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110ba1.html

---

QUESTION 12:

The Certkiller network is using GRE on their IPSec VPN WAN. 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

Explanation:
Normal IP Security (IPSec) configurations cannot transfer routing protocols, such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), or non-IP traffic, such as Internetwork Packet Exchange (IPX) and AppleTalk. IPSec with GRE uses generic routing encapsulation (GRE) in order to accomplish routing between the different networks. All routing protocols will be supported as all traffic will be encapsulated within a GRE packet.

QUESTION 13:

Which two are true about Cisco AutoSecure? (Choose two)

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

Answer: A, C

Explanation:
Cisco AutoSecure performs the following functions:
1. Disables the following Global Services
1. Finger
2. PAD
3. Small Servers
4. Bootp
5. HTTP service
6. Identification Service
7. CDP
8. NTP
9. Source Routing
2. Enables the following Global Services
1. Password-encryption service
2. Tuning of scheduler interval/allocation
3. TCP synwait-time
4. TCP-keepalives-in and tcp-kepalives-out
5. SPD configuration
6. No ip unreachables for null 0
3. Disables the following services per interface
1. ICMP
2. Proxy-Arp
3. Directed Broadcast
4. Disables MOP service
5. Disables icmp unreachables
6. Disables icmp mask reply messages.
4. Provides logging for security
1. Enables sequence numbers & timestamp
2. Provides a console log
3. Sets log buffered size
4. Provides an interactive dialogue to configure the logging server ip address.
5. Secures access to the router
1. Checks for a banner and provides facility to add text to automatically configure:
2. Login and password
3. Transport input & output
4. Exec-timeout

5. Local AAA
6. SSH timeout and ssh authentication-retries to minimum number
7. Enable only SSH and SCP for access and file transfer to/from the router
8. Disables SNMP If not being used
6. Secures the Forwarding Plane
1. Enables Cisco Express Forwarding (CEF) or distributed CEF on the router, when available
2. Anti-spoofing
3. Blocks all IANA reserved IP address blocks
4. Blocks private address blocks if customer desires
5. Installs a default route to NULL 0, if a default route is not being used
6. Configures TCP intercept for connection-timeout, if TCP intercept feature is available and the user is interested
7. Starts interactive configuration for CBAC on interfaces facing the Internet, when using a Cisco IOS Firewall image,
8. Enables NetFlow on software forwarding platforms
Reference:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns336/networking_solutions_white_paper09186a008018

QUESTION 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

Explanation:
The Firewall Service Module (FWSM) is a high performance module used in Catalyst 6500 series switches and 7600 series routers. It is capable of 5.5GB of throughput, supporting 1 million simultaneous connections, 100,000 connection setup and teardowns per second, and 256,000 NAT and PAT translations. It also supports up to 100 separate security contexts (virtual firewalls) with a license upgrade.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 2, page 4-2 and 4-7.

QUESTION 15:

The Certkiller network administrator 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: A

Explanation:
When installing the CS-MARS appliance and connecting to it for the first time, when the CS-MARS booted up, connect a UTP Cat 5 crossover cable to your computer's Etheret port and connect the other end of the crossover cable to the CS-MARS' Ethernet 0 (eth0) port.
Incorrect Answers:
B: To start the configuration process, you must connect another computer that is running Microsoft Internet Explorer to the appliance.
C: The default IP address of the CS-MARS device is 192.168.0.100, and it is recommended that the IP address of you computer is set to 192.168.0.101/24.
D: Although the default user name/password is indeed pnadmin/pnadmin, you should connect to 192.168.0.100, not 192.168.1.1
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 6, page 4-65.

QUESTION 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

Explanation:
Cisco NAC Appliance (formerly Cisco Clean Access) is an easily deployed Network Admission Control (NAC) product that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and repairs any vulnerabilities before permitting access to the network.
When deployed, Cisco NAC Appliance provides the following benefits:

1. Recognizes users, their devices, and their roles in the network. This first step occurs at the point of authentication, before malicious code can cause damage.
2. Evaluates whether machines are compliant with security policies. Security policies can include specific antivirus or antispyware software, OS updates, or patches. Cisco NAC Appliance supports policies that vary by user type, device type, or operating system.
3. Enforces security policies by blocking, isolating, and repairing noncompliant machines.
Noncompliant machines are redirected into a quarantine area, where remediation occurs at the discretion of the administrator.

QUESTION 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

Explanation:
The VPN Advanced Integration Module (AIM) for the Cisco 1841 Integrated Services Router and Cisco 2800 and3800Series Integrated Services Routers optimizes the Cisco Integrated Services Router platforms for virtual private networks in both IP Security (IPSec) and Secure Sockets Layer (SSL) Web and VPN deployments.
The Cisco VPN and SSL AIM provides up to 40 percent better performance for IPsec VPN over the built-in IPsec encryption, and up to twice the performance for SSL Web VPN encryption. The Cisco VPN and SSL AIM supports all three of these functions in hardware: SSLencryption in hardware, VPN IPsec encryption in hardware using either Data Encryption Standard (DES) or Advanced Encryption Standard (AES), and the IP Payload Compression Protocol (IPPCP) in hardware.
Reference:
http://www.cisco.com/en/US/products/ps5853/products_data_sheet0900aecd804ff58a.html

---

QUESTION 18:

In the context of Cisco NAC, what is a network access device?

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

Answer: B

Explanation:
In NAC, network devices that can or will enforce admission control policy include routers, switches, wireless access points, wireless LAN controllers, and security appliances. These devices demand host credentials and relay this information to policy servers, where network admission control decisions are made.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 4, page 1-11 and 1-13.

QUESTION 19:

How does Cisco CSA protect endpoints?

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

Answer: C

Explanation:
The technology used to control the host is the CSA INCORE (Interceptor Correlate Rules Engine) technology which supports four interceptors:
File System- All file read or write requests are intercepted and checked against a defined set of rules.
Network- Packet events at the driver (NDIS) or transport (TDI) level
Configuration - Read or write requests to the registry on Windows or to the RC files on UNIX.
Execution space - Deals with maintaining the integrity of each application's dynamic run-time environment.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 4, page 4-3

QUESTION 20:

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

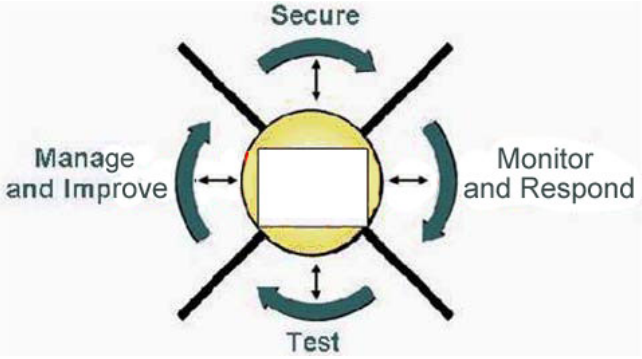
A. A detailed action plan
B. An identification of bottlenecks inside the network
C. An identification of critical deficiencies
D. A recommendations based on security best practice
E. A service offer

Answer: C, D

Explanation:
As the first step in planning network security, it is required to make an evaluation of the organization's network security posture. The Security Posture Assessment provides a snapshot of the security state of the network by conducting a thorough assessment of the network devices, servers, databases, and desktops.
Analyze the effectiveness of the network security in reference to recognized industry best practices, allowing identifying the relative strengths and weaknesses of the environment and documenting specific vulnerabilities that could threaten the business.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 1, page 1-29

QUESTION 21:

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



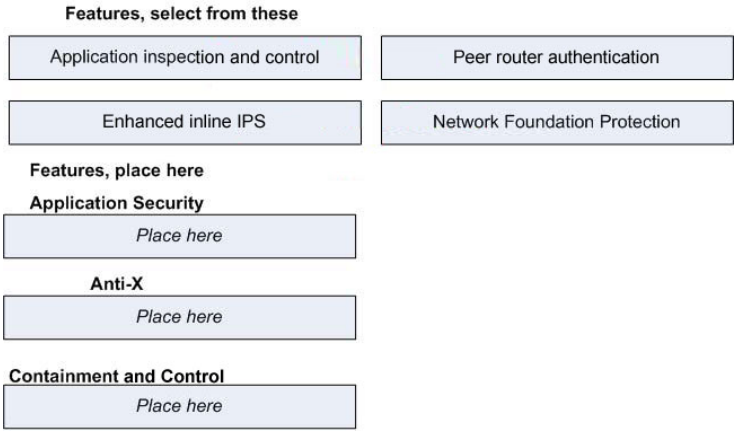
A. Business requirements
B. Corporate security policy
C. Customer needs
D. Security best practice

Answer: B

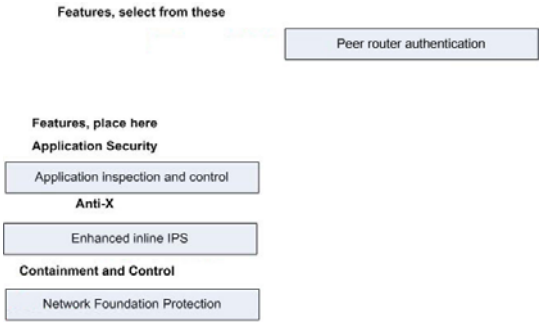
Explanation:
Network security is a continuous process built around a security policy. The diagram above is found in the reference link below, with the words "Security Policy" found in the blank box.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 1, page 1-24

QUESTION 22:

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

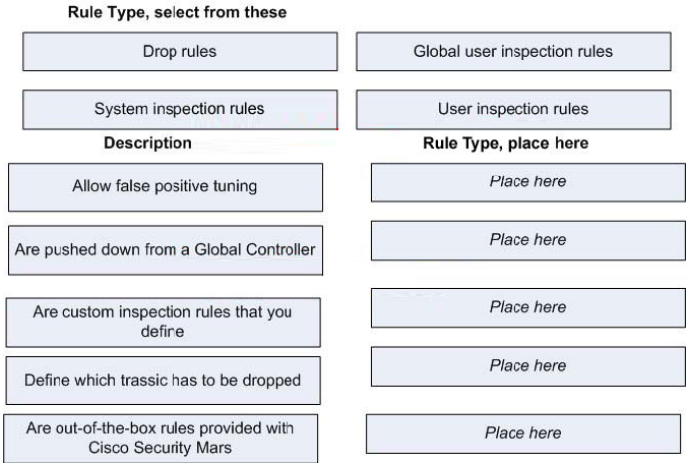


Answer:

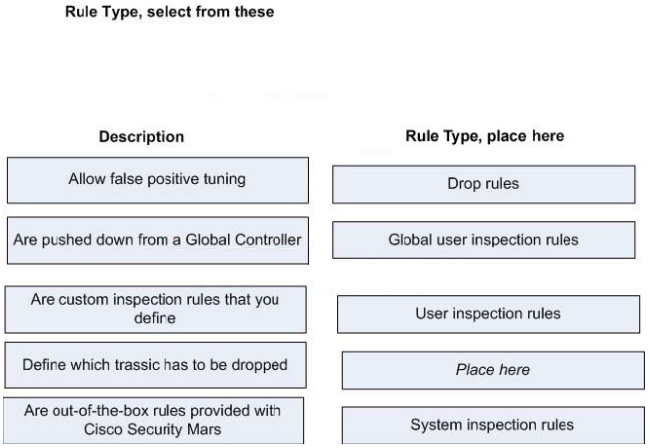


QUESTION 23:

DRAG DROP
You work as a network technician at Certkiller .com. Your boss, Mrs Certkiller, 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:



QUESTION 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

Explanation:
The functions of the CSA are system hardening, resource protection, control of executable content, application control, and detection.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 4, page 4-3.

QUESTION 25:

The Certkiller network is undergoing a Security Posture Assessment. 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

Explanation:

A Security Posture Assessment is designed to identify vulnerabilities that allow outside, untrusted networks to gain access to internal, trusted networks and systems, and recommend solutions for improvement.
With a Security Posture Assessment, your organization can:
? Reduce the risk of intentional or accidental access to IT assets and information
? Identify security vulnerabilities in your network infrastructure
? Develop a prioritized list of steps required to fix identified vulnerabilities
? Improve compliance with federal and state regulations that require security assessments
? Reduce the time and resources trying to stay current with new and emerging vulnerabilities
? Validate current security policies and practices against industry best practices and verifying areas that require security budget or staffing

---

QUESTION 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

Explanation:
Cisco Secure Access Control Server (ACS) provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications. Cisco Secure ACS helps to ensure enforcement of assigned policies by allowing network administrators to control:
1. Who can log into the network
2. The privileges each user has in the network
3. Recorded security audit or account billing information
4. Access and command controls that are enabled for each configuration's administrator

---

QUESTION 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

Explanation:
Organizations today face an increasing amount of security legislation that require companies to protect their date, including CFAA (Computer Fraud and Abuse Act) HIPAA (Health Insurance Portability and Accountability Act), and GLBA (The Gramm-Leach-Bliley Act) just to name a few. This legislation means an increased amount of liability and accountability for network security. The Cisco Self Defending Network suite of solutions can be used to provide end to end network security.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 1, page 1-3

QUESTION 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

Explanation:
The Distributed Denial of Service (DDoS) attacks are attacks in which malicious individuals cause thousands of compromised computers ("zombies") to run automated scripts that cripple a protected server's (the zone) network resources with spurious requests for service. The attacks can be, for example, a flood of bogus home page requests to a web server that shuts out legitimate consumers, or efforts that compromise the availability and accuracy of Domain Name System (DNS) servers. Although often launched by an individual, the zombies actually executing the attacking code may number in the hundreds of thousands, and are distributed over multiple autonomous systems, administered by multiple organizations. These distributed attacks generate a volume of traffic that cannot be handled by the lower bandwidths available at a typical zone, including the largest corporations.
The Cisco Traffic Anomaly Detector Module (Detector module) is a Cisco IOS application module that you can install in the Catalyst 6500 series switch.
It is a denial-of-service (DoS) detection product. It receives a copy of the traffic on the switch, analyzes that traffic, and sends out an alert when a DoS attack is detected.The Detector can detect attacks and activate protection mechanisms. It is best suited to work alongside with the Cisco Guard but it can also operate as a separate DDoS detection and alarm component. The Detector gets a copy of the traffic either by using the port mirroring feature (such as SPAN) of a switch, or by means of splitting. Then it constantly monitors the traffic, and closely remains tuned to zone traffic characteristics for evolving

attack patterns. The Detector module can also activate a configured Cisco Anomaly Guard Module to mitigate these attacks.
Reference:
http://www.cisco.com/en/US/products/hw/modules/ps2706/products_module_configuration_guide_chapter09186

QUESTION 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

Explanation:
An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Contrast this with public-key cryptology, which utilizes two keys - a public key to encrypt messages and a private key to decrypt them.
Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted.
Symmetric-key cryptography is sometimes called secret-key cryptography. The most popular symmetric-key system is the Data Encryption Standard (DES).

QUESTION 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

Explanation:
The Cisco Security Agent resides between the applications and the kernel, enabling maximum application visibility with minimal impact to the stability and performance of the underlying operating system. The software's unique architecture intercepts all

operating system calls to file, network, and registry sources, as well as to dynamic run-time resources such as memory pages, shared library modules, and COM objects. The agent applies unique intelligence to correlate the behaviors of these system calls, based on rules that define inappropriate or unacceptable behavior for a specific application or for all applications. This correlation and subsequent understanding of an application's behavior is what allows the software-as directed by the security staff-to prevent new intrusions.
Because the Cisco Security Agent intercepts system calls at the operating system level, there is no need to replace any system programs.
Reference:
www.cisco.com/en/US/products/sw/secursw/ps5057/products_data_sheet0900aecd80440398.html

---

QUESTION 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

Explanation:
CBAC intelligently filters TCP and UDP packets based on application-layer protocol session information and can be used for intranets, extranets and the Internet. CBAC is implemented on Cisco IOS routers via the firewall feature set.
Without CBAC, traffic filtering is limited to access list implementations that examine packets at the networklayer, or at most, the transportlayer. However, CBAC examines not only networklayer and transportlayer information but also examines the application-layer protocol information (such as FTP connection information) to learn about the state of the TCP or UDP session. This allows support of protocols that involve multiple channels created as a result of negotiations in the control channel. Most of the multimedia protocols as well as some other protocols (such as FTP, RPC, and SQL*Net) involve multiple channels.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800c

---

QUESTION 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

Explanation:
The ISR router series provides built-in VPN encryption acceleration for IPSec DES, 3DES, and AES 128, 192, and 256.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 1, page 2-13.

QUESTION 33:

Certkiller is a network administrator at Certkiller .com. Certkiller .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

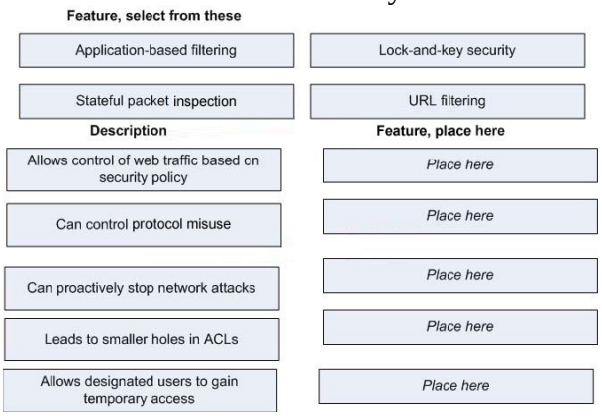
Answer: B

Explanation:
Cisco Secure Access Control Server (ACS) for Windows provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications. Cisco Secure ACS helps to ensure enforcement of assigned policies by allowing network administrators to control:
* Who can log into the network
* The privileges each user has in the network
* Recorded security audit or account billing information
* Access and command controls that are enabled for each configuration's administrator
Cisco Secure ACS is a major component of Cisco trust and identity networking security solutions. It extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework, thereby allowing greater flexibility and mobility, increased security, and user productivity gains.
The TACACS+ protocol provides authentication between the network access server and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between a network access server and a TACACS+ daemon are encrypted. TACACS+ was designed by Cisco to overcome some of the imitations of RADIUS and is therefore considered to be more secure. RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information, making it difficult to decouple authentication and authorization. RADIUS also encrypts only the password in the access-request packet from the client to the server.

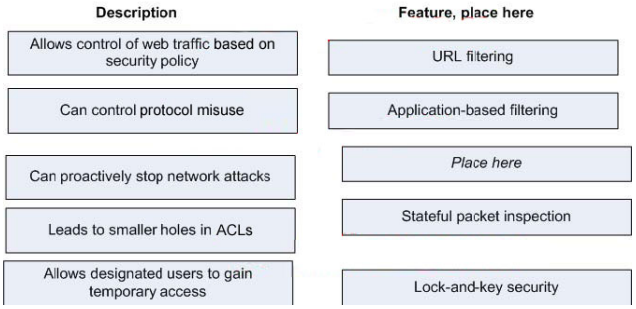
The remainder of the packet is in the clear. Other information, such as username, authorized services, and accounting, can be captured by a third party.
Reference:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/secsols/aaasols/c262c1.htm#1034907

QUESTION 34:

DRAG DROP
You work as a network technician at Certkiller .com. Your boss, Mrs Certkiller, is curious about secure features. Match the features with the appropriate description. Use each feature once and only once.



Answer:



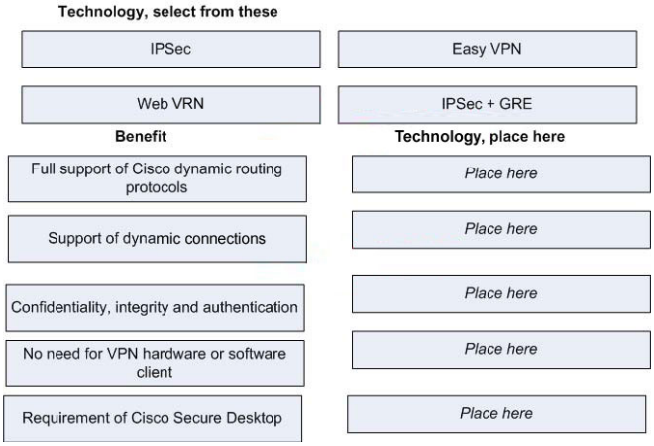
Explanation:
Allows control of web traffic based on sec policy - URL filtering
Can control protocol misuse - Application-based filtering (NBAR - Network Based Application Recognition)
Can proactively stop Net Attacks - unmatched (This describes IPS, which is not an option)
Leads to smaller holes in ACL - State full inspection (No need to authorize return traffic)
Allows designated users to gain temporary access- Lock-and-Key

---

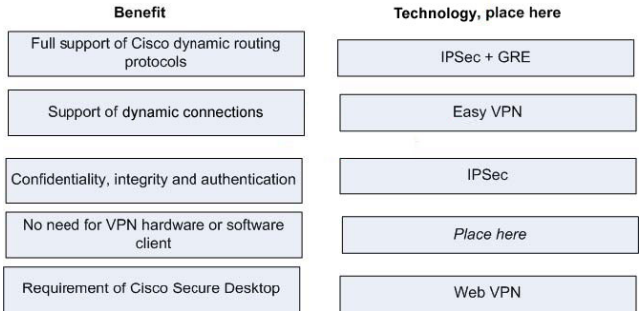
QUESTION 35:

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

Use each technology once and only once.



Answer:



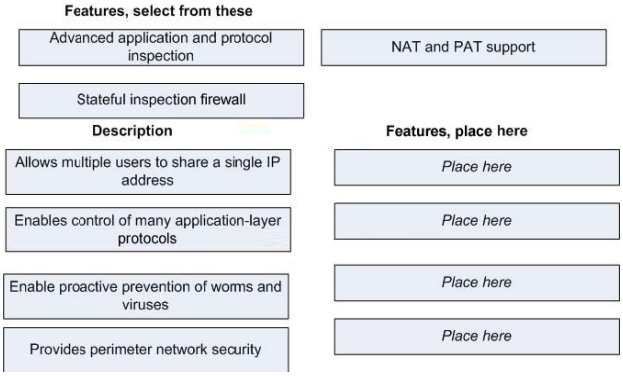
Explanation:

QUESTION 36:

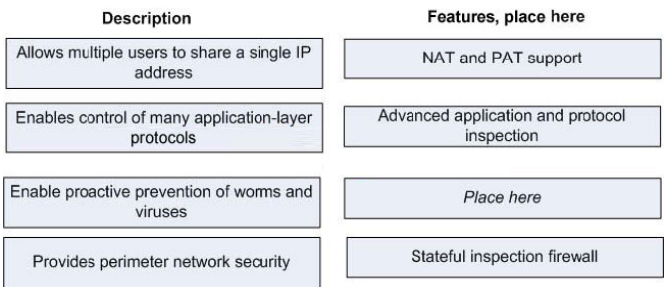
DRAG DROP

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

Use each feature once and only once.



Answer:



Explanation:

QUESTION 37:

Cisco MARS is being used in the Certkiller network. What is a feature or function of Cisco Security MARS?

A. MARS enforces authorization policies and privileges
B. MARS determines security incidents based on device messages, events, and sessions
C. MARS configures, monitors, and troubleshoots Cisco security products
D. MARS supports AAA user login authentication
E. None of the above

Answer: B

Explanation:
With MARS, as events and data messages are received, the information is normalized against the topology, discovered device configurations, same source and destination applications (across Network Address Translation [NAT] boundaries), and similar attack types. Similar events are grouped into sessions in real time. System- and user-defined correlation rules are then applied to multiple sessions to identify incidents.

QUESTION 38:

Cisco Clean Access has been implemented in the Certkiller network. 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

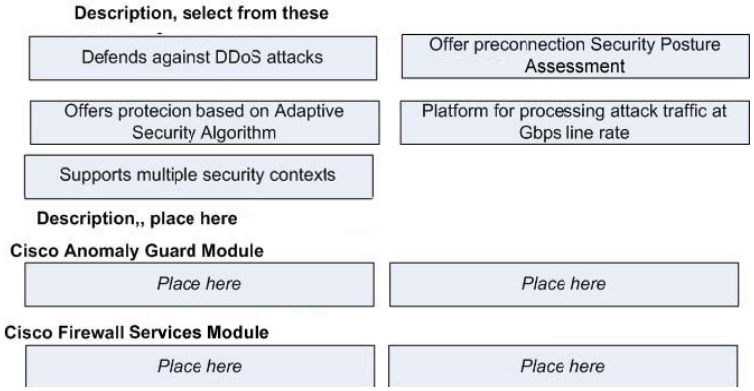
Answer: A, E

Explanation:
Cisco NAC Appliance (formerly Cisco Clean Access) is an easily deployed Network Admission Control (NAC) product that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and repairs any vulnerabilities before permitting access to the network.
Networks with Cisco NAC Appliance can realize benefits such as:
* Minimized network outages
* Enforcement of security policies
* Significant cost savings with automated device repairs and updates
Reference: http://www.cisco.com/en/US/products/ps6128/index.html

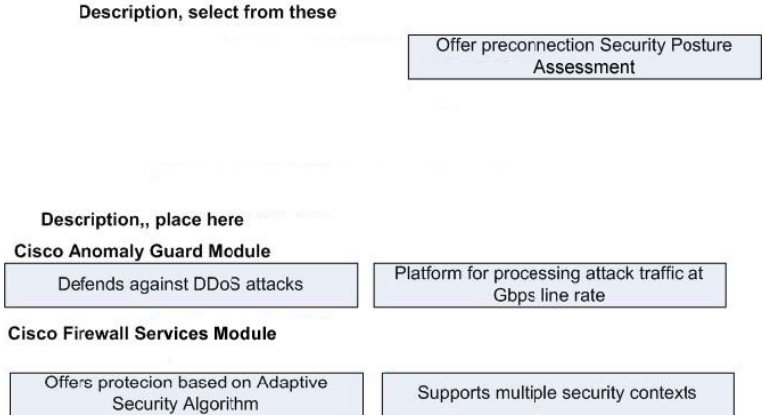
---

QUESTION 39:

DRAG DROP
You work as a network technician at Certkiller .com. Your boss, Mrs Certkiller, is curious about Cisco Security modules. Match the modules with the appropriate descriptions.
Not all descriptions are used.



Answer:



Explanation:

QUESTION 40:

A new MARS appliance has been installed in the Certkiller network. 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

Explanation:
Cisco routers and switches that are running Cisco IOS Software release 12.2 can be configured to provide different types of data to MARS:
Syslog messages. The syslog messages provide information about activities on the network, including accepted and rejected sessions.
SNMP traffic. SNMP RO community strings support the discovery of your network's topology.
NAC-specific data. NAC logs events that are specific to its configuration, including Extensible Authentication Protocol (EAP) over UDP messages and 802.1x accounting messages.
Access lists or NAT statements. You must enable SSH or Telnet access if the configuration on the Cisco router or swtich includes access lists or NAT statements.
Spanning tree messages (Switch only). You must have STP (spanning tree protocol) configured correctly on the switches to enable L2 discovery and mitigation. STP provides MARS with access to the L2 MIB, which is required to identify L2 re-routes of traffic and to perform L2 mitigation. MARS also uses the MIB to identify trunks to other switches, which are used to populate VLAN information used in L2 path calculations. STP, which is enabled by default on Cisco Switches, should remain enabled, as it is required for L2 mitigation.
Reference:
http://www.cisco.com/en/US/products/ps6241/products_user_guide_chapter09186a008074f215.html

---

QUESTION 41:

What could be a reason to implement Cisco Security Agent?

A. To prevent Day Zero attacks
B. To communicate the host posture validation to a policy server
C. To track the Internet usage of employees
D. To validate policy compliance

Answer: A

Explanation:
Current supported versions of Cisco Security Agent 4.0.3.x, 4.5.1.x, 5.0.0.x, and 5.1.0.x are effective in stopping all known exploits seen to date, thus providing "Zero-Day" protection at the end host. CSA host intrusion prevention system software effectively stops both the initial buffer overflow attempt and any subsequent steps to exploit the Microsoft Windows VML document arbitrary code execution vulnerability.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_security_response09186a008074f075.ht

---

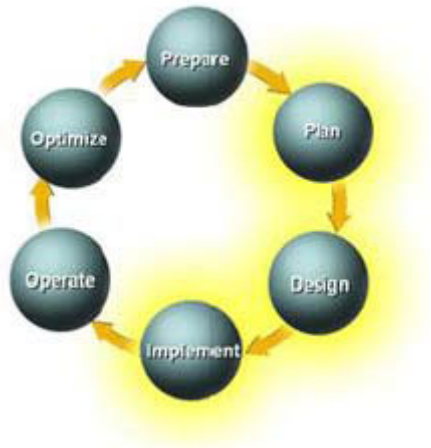
QUESTION 42:

Which two are parts of the Network Security Lifecycle? (Choose two)

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

Answer: B, D

Explanation:
The Network Security lifecycle is based on the lifecycle of the network itself as shown in the figure below. It includes the Preparation, Planning, Design, Implementation, Operation, and Optimization components..



QUESTION 43:

A new MARS appliance has been installed in the Certkiller network. On the Cisco Security MARS appliance, what is used to facilitate the management of Event, IP, Service and User management?

A. Groups

B. Custom parser
C. Rules
D. Signatures
E. Audit trail log

Answer: A

Explanation:
Using a creating event groups is one of the most powerful ways to leverage rules. You can take any event or series of events, group them, and use them with rules to concentrate your searches for attacks. Groups are also used to facilitate the IP management, Service Management, and User Management tabs within the MARS local and Global Controllers.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 6, page 4-35 through 4-36.

QUESTION 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

Explanation:
The Cisco Intrusion Prevention System (IPS) Version 5.0 Solutions deliver a new generation of highly accurate and intelligent in-line prevention services complemented by new network anti-virus, anti-spyware and worm mitigation capabilities for improved threat defense across multiple form factors including appliances, switch-integrated modules, and Cisco IOSSoftware-based solutions using enhanced application inspection engines.

QUESTION 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

Explanation:
A Security policy is used to define and set a good foundation for securing the network, including:
Definition: Define the data assets to be covered by the security policy (statement of authority and scope).
Identity: How do you identify the hosts and applications affected by this policy.
Trust: Under what conditions is communication allowed between hosts.
Enforceability: How will the policies implementation be verified.
Risk Assessment: What is the impact of a policy violation and how to detect them.
Incident Response: What actions are required upon violation of a security policy.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 1, page 1-25.

QUESTION 46:

A new MARS appliance has been installed in the Certkiller network. 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

Explanation:
The MARS GlobalController is a security threat mitigation (STM) appliance. Once you deploy multiple LocalControllers, you can deploy a GlobalController that summarizes the findings of two or more LocalControllers. In this way, the GlobalController enables you to scale your network monitoring without increasing the management burden. The GlobalController provides a single user interface for defining new device types, inspection rules, and queries, and it enables you to manage LocalControllers under its control. This management includes defining administrative accounts and performing remote, distributed upgrades of the LocalControllers.
Reference:
http://www.cisco.com/en/US/products/ps6241/products_user_guide_chapter09186a008053fdeb.html

---

QUESTION 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

Explanation:
The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IP Security (IPsec) Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP).
With DMVPN, The Dynamic Creation for Spoke-to-Spoke Tunnels feature eliminates the need for spoke-to-spoke configuration for direct tunnels. When a spoke router wants to transmit a packet to another spoke router, it can now use NHRP to dynamically determine the required destination address of the target spoke router. (The hub router acts as the NHRP server, handling the request for the source spoke router.) The two spoke routers dynamically create an IPsec tunnel between them so data can be directly transferred.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110ba1.html

---

QUESTION 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

Explanation:
In transparent mode, the FWSM acts like a "bump in the wire," or a "stealth firewall," and is not a router hop. The FWSM connects the same network on its inside and outside interfaces, but each interface must be on a different VLAN (only 2 VLANs). No dynamic routing protocols or NAT are required. However, like routed mode, transparent mode also requires ACLs to allow any traffic through aside from ARP packets. Transparent mode can allow certain types of traffic in an ACL that are blocked by routed mode, including unsupported routing protocols and multicast traffic. Transparent mode can also optionally use EtherType ACLs to allow non-IP traffic. Transparent mode only supports two interfaces, an inside interface and an outside interface, with each interface in the same IP subnet.
Reference:
http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_module_configuration_guide_chapte

---

QUESTION 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

Explanation:
The Cisco Security Agent resides between the applications and the kernel, enabling maximum application visibility with minimal impact to the stability and performance of the underlying operating system. The software's unique architecture intercepts all operating system calls to file, network, and registry sources, as well as to dynamic run-time resources such as memory pages, shared library modules, and COM objects. The agent applies unique intelligence to correlate the behaviors of these system calls, based on rules that define inappropriate or unacceptable behavior for a specific application or for all applications. This correlation and subsequent understanding of an application's behavior is what allows the software-as directed by the security staff-to prevent new intrusions on the individual hosts. The Cisco Security Agent provides numerous benefits, including:
The ability to aggregate and extend multiple endpoint security functions -the Cisco Security Agent provides host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation, all within a single agent
Preventive Protection against entire classes of attacks, Including port scans, buffer overflows, Trojan horses, malformed packets, malicious HTML requests, and e-mail worms
"Zero Update "prevention for known and unknown attacks
Reference:
http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/products_data_sheet0900aecd80440398.html

---

QUESTION 50:

A new MARS appliance has been installed in the Certkiller network. 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

Explanation:
You can archive data from a MARS Appliance and use that data to restore the operating system (OS), system configuration settings, dynamic data (event data), or the complete system. The appliance archives and restores data to and from an external network-attached storage (NAS) system using the network file system (NFS) protocol. Only a NFS or a NAS using the NFS protocol is supported on the Cisco MARS.

QUESTION 51:

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

A. A complete network blueprint
B. Configuration for each device
C. A detailed part list
D. An operating expense
E. Risk analysis

Answer: A, C

Explanation:
Network design development is for developing a strategy, plan, and design for integrating a new security solution into the core network infrastructure. The organization's security goals are reviewed ad then an in-depth analysis of the technical, procedural, and resource requirements for a customized security deployment that meets these goals are defined. The created design document should include a complete network blueprint as well as a detailed parts list for all network devices.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 1, page 1-31.

QUESTION 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

Explanation:
During the design phase, Cisco recommends services that help you develop a

comprehensive detailed design to meet business and technical requirements, and create plans to guide implementation-phase activities.
The design phase takes input from the entire scope of requirements discussed previously (services, network, security, and operations) and transparently brings together all elements. The choices made during the network design phase determine whether the network can meet business goals. It is critical to gather all the facts first and approach the design in such a way that any future changes can be made with minimal disruption.
Activities and deliverables in the design phase might include:
Producing a low-level design
Developing a staging plan and proof of concept
Identifying required changes in the existing network
Developing a migration plan
Developing an acceptance test plan
Developing the operation design
Reference:
http://www.cisco.com/warp/public/437/services/docs/CiscoServicesforWirelineOverview.pdf

---

QUESTION 53:

A new MARS appliance has been installed in the Certkiller network. 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

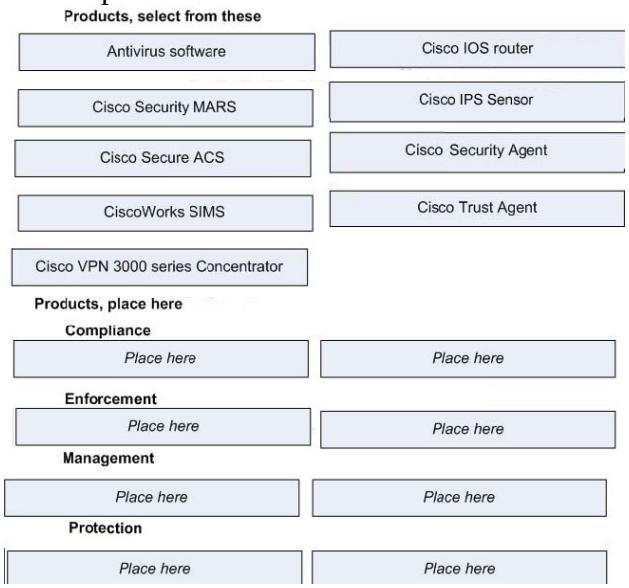
Explanation:
There are two ways to perform a long-duration query on the MARS:
1.
Modifying an existing report.
Advantages:
The report is compiled relatively quickly.
You can compile data gathered over a longer time period
Disadvantage.
This type of query can only be used without any changes to query criteria other than time range, and can only be used with the following reports:
2.
Performing a batch query.
Advantages:
You can modify any of the query criteria.
Best suited for data that spans a short time period.

Disadvantages
This type of query can be slow and may take a substantial amount of time to complete.
Only Admin users can perform a batch query.
Reference:
http://www.cisco.com/en/US/products/ps6241/products_user_guide_chapter09186a008053fdf5.html

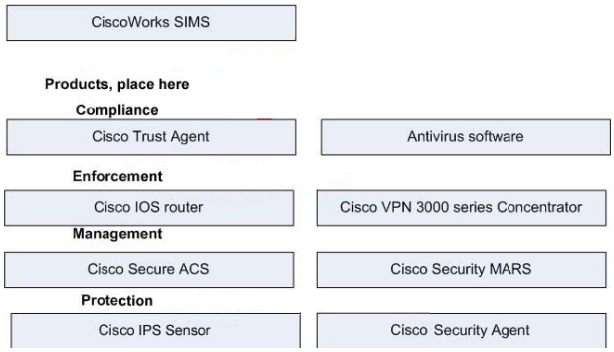
---

QUESTION 54:

DRAG DROP
You work as a network technician at Certkiller .com. Your boss, Mrs Certkiller, is curious about Cisco Security products. Match the products with the appropriate NAC framework.
Not all products are used.



Answer:



QUESTION 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

Explanation:
Reasons for Network Security:
1. Security Legislation
2. Prevent Network Misuse
3. Prevent Unauthorized Access
4. Comply with company policy
5. Defend Attacks
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 1, page 1-2.

QUESTION 56:

In which two ways does 802.1x benefit businesses in terms of trust and identity?
(Choose two)

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

Answer: A, C

Explanation:
802.1X is an IEEE standard for media-level access control, offering the capability to permit or deny network connectivity, control VLAN access dynamically and apply traffic policy, based on user or machine identity.

QUESTION 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

Explanation:
When creating an acceptance test plan, begin with a thorough understanding of the objectives and scope of the deployment. A review of the plan that analyzes technical requirements, procedures, and resources needs to be done.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 1, page 1-32.

QUESTION 58:

What are two beneficial functions of the CiscoWorks VPN/Security Management Solution? (Choose two)

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

Answer: D, E

Explanation:
CiscoWorks VMS includes the following applications, organized by functional area:
* Firewall management - Enables the large-scale deployment of Cisco firewalls. Smart Rules is an innovative feature that allows a security policy to be consistently applied to all firewalls. Smart Rules allows a user to define common rules once, reducing configuration time and resulting in fewer administrative errors. See CiscoWorks Management Center for Firewalls and CiscoWorks Auto Update Server Software.
* Network IPS management and router-based IPS management - Enables configuration of network IPS and router-based IPS. Many sensors can be configured quickly using group profiles. Additionally, a powerful signature management feature is included to help increase the accuracy and specificity of detection. See CiscoWorks Management Center for IPS Sensors.
* Host IPS management
- Scalable to thousands of endpoints per manager to support large enterprise deployments. The open and extensible architecture offers the capability to define and enforce security according to corporate policy. Offers "zero update" prevention for known and unknown attacks. See CiscoWorks Management Center for Cisco Security Agents.
* VPN router management - Provides functions for the setup and maintenance of large deployments of VPN connections and Cisco IOS firewalls on Cisco security routers and Cisco Catalyst 6000 VPN service modules. See CiscoWorks Management Center for VPN Routers. For the largest VPN router deployments, customers may also consider the Cisco IP Solution Center Security Management software, which is purchased separately from CiscoWorks VMS. See Cisco IP Solution Center Security Management.

* Security monitoring - Provides integrated monitoring to help administrators achieve a comprehensive view of security across the network, with event correlation to detect threats not apparent with individual events. See CiscoWorks Monitoring Center for Security.
* Performance monitoring - Provides functions for monitoring and troubleshooting the health and performance of security and VPN devices. See CiscoWorks Monitoring Center for Performance.
* Operational management -Allows network managers to build a complete network inventory, report on hardware and software changes, and manage software updates to multiple devices. See CiscoWorks Resource Manager Essentials.
* Common Services - Provides an application infrastructure for CiscoWorks VMS functions to share a common model for data storage, login, user role definitions, access privileges, and security protocols. See CiscoWorks Common Services Software.
Reference: http://www.cisco.com/en/US/products/sw/cscowork/ps2330/index.html

---

QUESTION 59:

A new MARS appliance has been installed in the Certkiller network. 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

Explanation:
The 3 ways to add devices into CS-MARS are:
1. Import from seed file (preferred when there is a large number of devices)
2. SNMP auto discovery (L3 Devices)
3. Configure manually
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 6, page 4-69.

QUESTION 60:

What is a valid method of verifying a network security design?

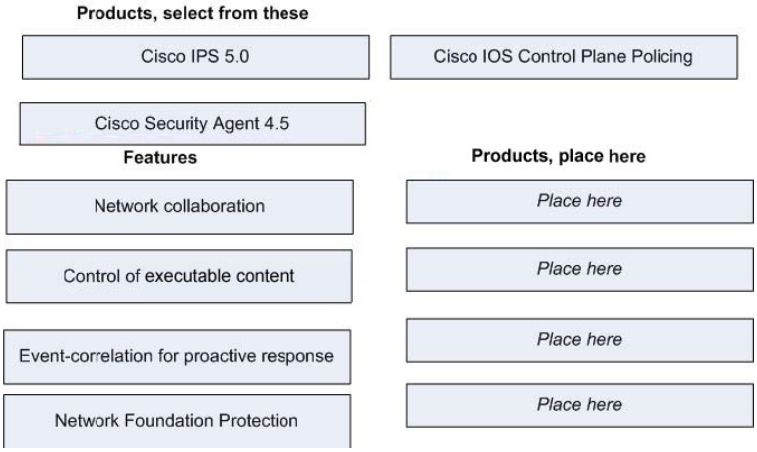
A. Network audit
B. Network health analysis
C. Network performance test
D. Pilot or prototype network

Answer: D

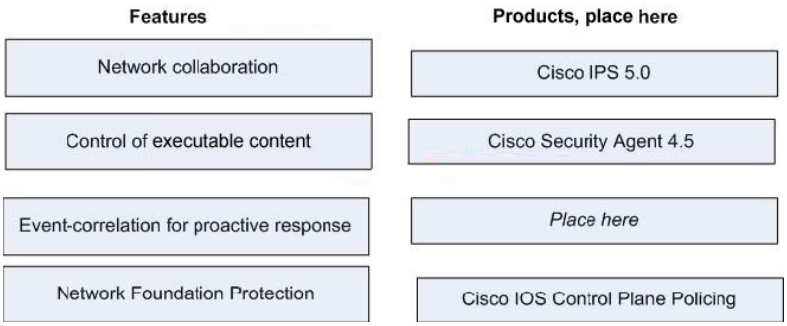
Explanation:
In the "Test Key Components" phase of a network security design, testing the key components helps in understanding what features they offer, how they work and what performance values can be expected. The testing should be done in a controlled environment, such as a test lab or pilot network.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 1, page 1-37.

QUESTION 61:

DRAG DROP
You work as a network technician at Certkiller .com. Your boss, Mrs Certkiller, is curious about Cisco Security products. Match the products with the appropriate feature.
Use each product once and only once.



Answer:



QUESTION 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

Explanation:
The Meta Event Generator (MEG), delivered by Cisco IPS Sensor Software Version 5.0, takes the guesswork out of making an accurate assessment on the occurrence of multifaceted worms, such as Nimda. As worms propagate through the network, they typically generate multiple IPS events of varying degrees of severity. When there is no relationship established between such disparate events they could be assigned low severity ratings since, by themselves, they do not pose a significant threat. However, when these events are considered in the context of a sequence of related events, they could collectively indicate worm or virus activity. Cisco's Meta-Event Generator links these seemingly unrelated lower severity alarms into a high severity, high risk event, enabling the user to confidently drop the associated packets.
In summary, MEG delivers an extensible architecture that provides sensor-level event correlation and corroboration, taking the guesswork out of event management and giving the user the enhanced capability of making intelligent decisions for the mitigation of malicious activities that relate to such events. The effectiveness of IPSs is greatly enhanced when such correlation algorithms are embedded into the sensor, as opposed to performing such methods at the monitoring console. When event correlation isd performed at the sensor level, the sensor can proactively take automated response actions that can effectively stop worms and viruses.
Reference:
www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_white_paper0900aecd801e78e5.shtml

---

QUESTION 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: D, E

Explanation:
By converging SSL and IPsec VPN services with comprehensive threat defense technologies, the Cisco ASA 5500 Series provides highly customizable network access tailored to meet the requirements of diverse deployment environments while providing advanced endpoint and network-level security.

To help ensure that threats do not go unnoticed, the Cisco ASA 5500 Series offers numerous methods to identify policy violations, anomalous activity, and vulnerability exploitation. They include stateful pattern recognition for stopping attacks hidden inside a data stream; protocol analysis tovalidate network traffic; traffic anomaly detection to identify attacks that cover multiple sessions and connections; protocol anomaly detection to identify attacks based on observed deviations in the normal RFC behavior of a protocol or service; and Layer 2 analysis to detect man-in-the-middle attacks. Specialized safeguards "scrub" network traffic to prevent "detection evasion" attempts; these safeguards include IP fragmentation reassembly and normalization, TCP stream reassembly and normalization, TCP evasion control, IP antispoofing, and deobfuscation.
Reference:
http://www.cisco.com/en/US/products/ps6120/products_data_sheet0900aecd802c1d00.html

---

QUESTION 64:

What are three functions of the 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

Explanation:
The CSA is an intrusion prevention system for hosts. As such it prevents a host from different kinds of malicious traffic, spyware, adware, and misbehaving software products. It includes an application control component that is capable of controlling and protecting applications. There is application run control as well as executable file version control, protection against code injection, protection of process memory, protection against buffer overflows and keystroke logging.
Reference: Security Solutions for SE (SSSE) v1.0 Student Guide, Module 4, page 4-2 and 4-3

QUESTION 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

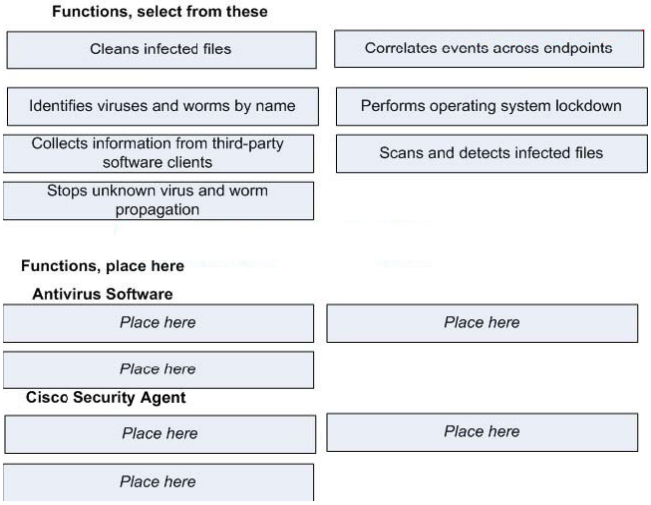
Answer: D

Explanation:
Cisco Trust Agent is a component of the Cisco Network Admission Control (NAC) solution. It is a specialized application that runs on your network endpoints. Cisco Trust Agent collects security posture information from the NAC-compatible applications that are installed on the endpoint and reports that information to a posture validation server for processing. Based on the assessment of the security posture information, the network endpoint is then granted access to the network, granted access to a remediation server, or denied access to the network until the endpoint is brought into compliance with security policy.
Reference:
http://www.cisco.com/en/US/products/ps5923/prod_release_note09186a00802aee82.html

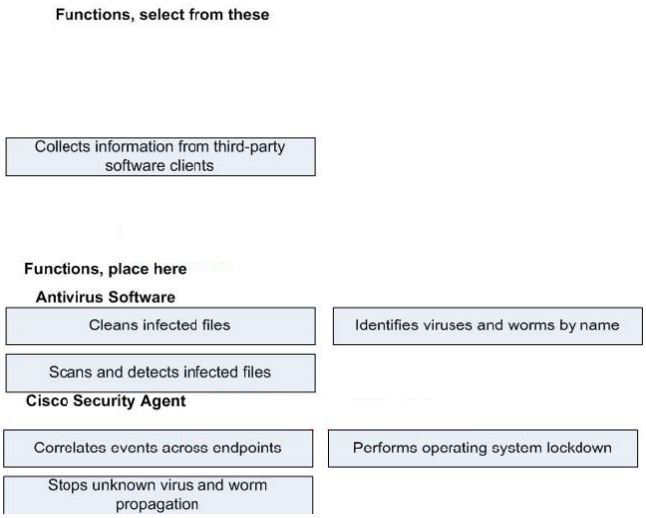
---

QUESTION 66:

DRAG DROP
You work as a network technician at Certkiller .com. Your boss, Mrs Certkiller, is curious about security products. Match the products with the appropriate functions. Not all functions are used.



Answer:



QUESTION 67:

A new MARS appliance has been installed in the Certkiller network. 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
E. None of the above

Answer: B

Explanation:
To send alert notifications to individual users or groups of users, configure the Action parameters of a rule to create an alert action. This procedure configures alerts for pre-existing rules. When you create a rule, the Action parameters are configured after the count number parameter.
Reference:
http://www.cisco.com/en/US/products/ps6241/products_user_guide_chapter09186a008053fdf3.html

---

QUESTION 68:

A new MARS appliance has been installed in the Certkiller network. What are three advantages of Cisco Security MARS? (Choose three)

A. It performs automatic mitigation on Layer 2 devices
B. It ensures that the user device is not vulnerable
C. It fixes vulnerable and infected devices automatically
D. It provides rapid profile-based provisioning capabilities

E. It is network topology aware
F. It contains scalable, distributed event analysis architecture

Answer: A, E, F

Explanation:
A: Cisco AutoMitigate capabilities identify available "choke-point" devices along the attack path and automatically provide the appropriate layer 2 device commands that the user can employ to mitigate the threat. The results can be used to quickly and accurately prevent or contain an attack. For layer 3 devices, MARS can recommend the mitigation procedures that security analysts can then use to manually perform.
E: Cisco Security MARS obtains network intelligence by understanding the topology and device configurations from routers, switches, and firewalls, and by profiling network traffic. The system's integrated network discovery function builds a topology map containing device configuration and current security policies, which enables it to model packet flows through your network.
F: As the local Cisco Security MARS appliances execute queries and rules across the enterprise, the results are efficiently consolidated for rapid and centralized analysis at the system's Global Controller. This scalable architecture yields an additional level of distributed processing and storage. The result is more cost-effective deployment and greater manageability, which addresses the requirements of large and geographically dispersed organizations.
Reference:
www.cisco.com/en/US/products/ps6241/products_data_sheet0900aecd80272e64.html

---

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

Explanation:
The Cisco Self Defending Network can help mitigate application abuse on servers, on desktops, and across networks in campus, branch office, and data center environments. It provides a system-based approach that is integrated, collaborative, and adaptive to enforce the prevention of application abuse and attacks.
Products That Help Prevent Application Abuse
* Cisco ASA 5500 Series Adaptive Security Appliances

* Cisco IPS 4200 Series Sensors
* Cisco Security Agent
* Catalyst Security Modules
o Cisco Catalyst 6500 Series Firewall Services Module
o Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Module
* IOS FW/IPS
* VMS
* CS - MARS
Reference:
http://www.cisco.com/en/US/netsol/ns479/networking_solutions_sub_solution_home.html

---

QUESTION 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)
E. None of the above.

Answer: D

Explanation:
A Cisco reference to "port 80 misuse" is addressing the problem that many applications/protocols are being tunneled over port 80 that are not strictly Web traffic-instant messaging, peer-to-peer, file-sharing (kazaa, gnutella), etc. Most corporate edge devices allow port 80 traffic to flow inorder not to obstruct Web commerce; however, this openness is also a vector of attack. Cisco IPS now allows tight policy control over instant messaging (IM), point-to-point (P2P), Multipurpose Internet Mail Extensions (MIME) type filtering, as well as command/method control over HTTP(allow http get, but not set or put), preventing the misuse of protocols by corporate employees.