



Exam : 646-301

Title : CK's VPN/Security ☐ ☐

Ver : 10.10.06

QUESTION 1:

You are a technician at Certkiller . Certkiller has its headquarters in New York. The company has just established two branch offices located in Baltimore and Detroit. You want to connect the new branch offices to the Certkiller central site. However, due to budget constraints, you need a more cost-effective, flexible solution than private WAN services.

Which solution could you implement?

- A. A V3PN solution
- B. A site-to-site VPN solution
- C. A SSL termination solution
- D. A remote access VPN solution
- E. A Redundant Services Termination solution

Answer: D

QUESTION 2:

Which of the following is the most cost effective VPN solution?

- A. VPN concentrators
- B. VPN modules for bridges
- C. VPN modules for the routers
- D. VPN modules for the firewalls
- E. VPN modules for the switches

Answer: C

QUESTION 3:

You are a technician at Certkiller . Certkiller has a VNP network. Your newly appointed Certkiller trainee wants

to know what the function of the Cisco VPN Client is.

What would your reply be?

- A. Initiates V3PN connection with Cisco VPN routers.
- B. Sets up Secure Socket Layer connection to the web host.
- C. Provides application layer connection to the remote web server.
- D. Establishes encrypted tunnels with a remote access VPN concentrator.

Answer: D

QUESTION 4:

You are a technician at Certkiller . The Certkiller VPN-enabled routers connect branch offices and regional offices. The VPN-enabled routers deliver single-box solutions that offer an integrated package of routing, firewall, intrusion detection, and VPN functions.

What is this type of VPN solution called?

- A. Site-to-site VPN
- B. VPN encryption
- C. SSL termination
- D. Remote access VPN
- E. Redundant Services Termination

Answer: A

QUESTION 5:

Certkiller has a defensible boundary within its network that allows a security policy to be strategically enforced. Your newly appointed Certkiller trainee wants to know what this boundary is called.

What would your reply be?

- A. A Firewall
- B. A perimeter network
- C. A Cisco IOS Firewall
- D. Network integrity point

Answer: B

Explanation:

A network security policy focuses on controlling the network traffic and usage. It identifies a network's resources and threats, defines network use and responsibilities, and details action plans for when the security policy is violated. When you deploy a network security policy, you want it to be strategically enforced at defensible boundaries within your network. These strategic boundaries are called perimeter networks.

Reference: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/security.htm#xtocid3

QUESTION 6:

What is the most cost effective way for Small and medium businesses to achieve firewall functionality?

- A. Use the Cisco IOS software firewall features.
- B. Use router access lists for network security.
- C. Use firewall services provided by their service provider.
- D. Use security features included in their applications software.

Answer: A

QUESTION 7:

On which devices can firewalls be implemented? (Choose all that apply.)

- A. Routers
- B. Software
- C. Switches
- D. Web appliances
- E. Dedicated hardware devices

Answer: A, B, E

QUESTION 8:

In conjunction with the Cisco PIX Firewall, what functionality can be used to manage access to Internet sites and selectively block individual of groups of Internet sites?

- A. 3DES
- B. URL filtering
- C. TCP port filtering
- D. Centralized configurations
- E. Access Control List (ACLs)

Answer: B

QUESTION 9:

What is the first line of defense that most organizations implement to define and protect sensitive portions of their networks and guard against intrusive access from potentially harmful applications?

- A. User accounting
- B. Firewall security
- C. A Virtual Private Network.
- D. An Intrusion Protection system

Answer: B

QUESTION 10:

You are a technician at Certkiller . You tell your newly appointed Certkiller trainee that Cisco PIX Firewalls utilize transparent identity verification at the firewall, and that it makes smart decisions for access or denial. After authentication, the Cisco PIX shifts session flows so that all subsequent traffic receives more rapid routing than proxy servers enable.

Your trainee now wants to know what this process is called. What would your reply be?

- A. CDP
- B. LEAP
- C. RADIUS
- D. Cut-Through Proxy
- E. Cut-Through Switching

Answer: D

QUESTION 11:

Why would the IT group in an organization be in favor of centralized Security Management tools? (Choose all that apply.)

- A. Because they provide convenient billing services.
- B. Because they aid in identifying new threats more quickly.
- C. Because they make their job easier installing and monitoring security functions.
- D. Because they provide assurance that the security policy is being applied uniformly.

Answer: B, C, D

QUESTION 12:

Which technology allows you to secure the transmission of data across the Internet?

- A. Data encryption
- B. Browser security
- C. Intrusion Detection
- D. High-speed switching
- E. Quality of Service (QoS)

Answer: A

QUESTION 13:

You are a technician at Certkiller . The Certkiller network has a set of hardware and software that is implemented on the network infrastructure to enforce the security policy of the company. Your newly appointed Certkiller trainee wants to know what this set of hardware and software is called.

What would your reply be?

- A. Router
- B. Switch
- C. VPN concentrator
- D. Cisco PIX Firewall
- E. Cisco Intrusion Detection (IDS) System

Answer: E

QUESTION 14:

Which of the following hides internal network IP addresses from the outside?

- A. A firewall
- B. Host Standby Protocol
- C. Advanced Quality of Service
- D. Network Address Translation
- E. Context-based Access Control

Answer: D

QUESTION 15:

You are a technician at Certkiller . Certkiller has two Cisco PIX Firewalls that run parallel. This ensures that if one firewall malfunctions, the second automatically maintains security operations and ensures that the firewall is always on. Your newly appointed Certkiller trainee wants to know what this configuration is called.

What would your reply be?

- A. URL filtering
- B. Hot Standby
- C. Standards-based VPN
- D. Centralized Configuration Builder

Answer: B

QUESTION 16:

Certkiller has chosen not to implement a firewall solution. What is Certkiller 's last means of perimeter defense between its network resources and the Internet?

- A. Their routers

- B. Their client machines
- C. Their service provider
- D. The Intrusion Protection System
- E. The Security Management System

Answer: A

QUESTION 17:

Which of the following security functions are performed by Host IDS? (Choose all that apply.)

- A. Secure session encryption using industry standards.
- B. Facilitation of client changes and updates to their passwords.
- C. Protection of critical and vulnerable servers within the network.
- D. Proactive event notification that is sent to network administration.
- E. Real-time monitoring of network traffic at pre-determined points in the network.

Answer: C, D, E

QUESTION 18:

You are a technician at Certkiller . Certkiller has implemented both Network IDS and Host IDS. Your newly appointed Certkiller trainee wants to know what benefit this implementation offers. What would your reply be?

- A. Host IDS can protect vulnerable servers and Network IDS can protect a network from probes.
- B. Wireless LANs become more secure with the additional LEAP and encryption provided by Network IDS and Host IDS.
- C. Router performance can be increased by offloading Network IDS and Host IDS functions to security appliances and servers.
- D. Private VLAN security provided through Network and Host IDS decreases propagation of attacks by isolating critical servers.

Answer: A

QUESTION 19:

You are a network engineer at Certkiller . You have proposed that Certkiller implement a Cisco Intrusion Protection system. The Certkiller board of directors wants to know how the Cisco Intrusion Protection addresses the financial impact of a possible network outage. What would your reply be?

- A. It allows for simplified network management.

- B. It identifies and reacts to known or suspected network intrusion and anomalies.
- C. It reduces additional financial losses by shutting down the network on intrusion.
- D. It prevents losses that are due to both hacker attacks and internal violations of security policy.

Answer: B, D

QUESTION 20:

You are a technician at Certkiller . You want to implement a Cisco product that is best for real-time monitoring and protecting a network (from unauthorized activities, denial of service attacks, port sweeps) and is also able to take actions against these attacks.

Which Cisco product would meet your requirements?

- A. Cisco Aironet 350
- B. Cisco Security Agent
- C. Cisco IDS 4200 family
- D. Cisco VPN Concentrator
- E. Cisco PIX Firewall Appliances

Answer: C

QUESTION 21:

You are a network technician at Certkiller . Certkiller has implemented Network Intrusion Detection system on its network. Your newly appointed Certkiller trainee wants to know how Network Intrusion Detection works.

What would your reply be?

- A. It intercepts and analyzes operating system and application calls based on a security policy definition.
- B. It decrypts encrypted data and passes it on to a management console for monitoring and interpretation.
- C. Real-time monitoring detects possible attacks which are inspected by a sensor and compared with a signature database for further action.
- D. It protects servers from worms and other harmful attacks by monitoring normal application behavior and cuttings off request that do not fit the normal behavior pattern.

Answer: C

QUESTION 22:

Which of the following will benefit most from an Intrusion Protection system that can be managed from remote sites via management solution?

- A. Data Capturer

- B. Data Center Manager
- C. Chief Financial Officer
- D. Chief Executive Officer
- E. Chief Information Officer

Answer: B

QUESTION 23:

You are a technician at Certkiller . Your newly appointed Certkiller trainee is not familiar with VPN technology but is familiar with the terminology. You want to explain means of ensuring that e-commerce transactions are secure.

What would you discuss with the trainee?

- A. The effectiveness of secure HTTP.
- B. The difference between SSL and IPSec.
- C. The difference between LEAP and IPSec.
- D. The effectiveness of router based firewalls.
- E. The availability of hacking tools on the Internet.

Answer: B

QUESTION 24:

You are a technician at Certkiller . Your newly appointed Certkiller trainee wants to know what the role of the Cisco Security Agent is.

What would your reply be?

- A. It protects networks from unauthorized activities, port sweeps, and denial of service attacks.
- B. It provides host intrusion prevention, distributed firewalls, and malicious code protection for servers and desktops.
- C. It increases server security by providing tools for automatically applying new patch updates to all critical servers on the network.
- D. It protects servers and desktops by monitoring each packet and comparing the contents with a database of attack signatures.

Answer: D

QUESTION 25:

You are a technician at Certkiller . Your newly appointed Certkiller trainee wants to know what the functions of the Cisco Security Agent are.

What would your reply be? (Choose all that apply.)

- A. It provides zero-updates for the network administrator.
- B. It provides preventive protection against entire classes of attacks.
- C. It is scalable to thousands of agents per manager to support large and deployments.
- D. It provides real-time monitoring of network traffic at pre-defined points in the network.

Answer: B, C, D

QUESTION 26:

Which Cisco technology addresses the problem of Intrusion Protection solutions that generate too many false alarms?

- A. Cisco SystemWorks
- B. Cisco Security Agent
- C. Cisco Threat Response
- D. Host Intrusion Detection System
- E. Network Intrusion Detection System

Answer: C

QUESTION 27:

You are a technician at Certkiller . Your newly appointed Certkiller trainee wants to know how Cisco Threat Response (CTR) helps to make Intrusion Protection more efficient. What would your reply be?

- A. It increases performance on the sensors for better price performance.
- B. It performs intelligent investigation of potential attacks to reduce false positives up to 95%.
- C. It automatically modifies security policies based on the types of attacks that are detected and can customize responses to those attacks.
- D. It gives network managers additional access to Quality of Service parameters so that voice traffic can be securely transported across the network.

Answer: C

QUESTION 28:

What is a primary purpose of the Cisco Threat Response?

- A. It reduces false alarms.
- B. It remediates costly intrusions.
- C. It shuts down the network in the event of an attack.

D. It proactively notifies network administrations when common attacks are detected.

Answer: D

QUESTION 29:

You are a network technician at Certkiller . Your newly appointed Certkiller trainee wants to know what an Identify Solution does.

What would your reply be? (Choose all that apply.)

- A. It validates the identity of every user.
- B. It tracks and reports user and accounting data.
- C. It utilizes OSPF technology to efficiently route authorized user traffic through the network.
- D. It controls access to information from many different kinds of users and a variety of access points.

Answer: A, B, D

QUESTION 30:

Which of the following questions best positions the ROI advantages of an Identify Solution?

- A. How do you currently control access to your network?
- B. Do you have any concern related to the growth of your network?
- C. Does your current Identity Solution offer the ability to easily enable group network devices?
- D. Would it be valuable to you to be able to integrate and Identity Solution with your existing systems?

Answer: A

QUESTION 31:

You are the network administrator at Certkiller . You have proposed that the company implement an Identity Solution. The Certkiller CEO wants to know how this solution will provide cost savings.

What would your reply be?

- A. They prevent email spam proliferation from unidentified users.
- B. They integrate with existing Cisco IOS router and VPN solutions.
- C. They eliminate redundant security solutions, such as Cisco Intrusion Detection.
- D. They eliminate network upgrades by providing more efficient user management.

Answer: B

QUESTION 32:

What is the key security benefit that the Cisco Secure ACS provides?

- A. It has one license model with no clients/suppliant requirements.
- B. It offers centralized control of all user authentication, authorization, and accounting.
- C. Different levels of security can be concurrently used with Cisco Secure ACS for different requirements.
- D. It supports large networked environments with redundant servers, remote databases, and user database backup services.

Answer: B

QUESTION 33:

With regard to VNP security, what does AAA stand for?

- A. Authentication, Access, Accounting
- B. Authorization, Admittance, Auditing
- C. Administration, Auditing, Accounting
- D. Authorization, Analysis, Administration
- E. Authentication, Authorization, Accounting

Answer: E

QUESTION 34:

Which of the following are functions of a site-to-site VPN? (Choose all that apply.)

- A. It reduces reliance on the service provider.
- B. It eliminates the need for and expense of toll free 800 numbers.
- C. It extends the WAN as an extranet to business partners and suppliers.
- D. It delivers Internet access and web-based applications across multiple locations.

Answer: A, C

QUESTION 35:

What is the key scalability benefit that the Cisco Secure ACS provides?

- A. It has one license model with no clients/suppliant requirements.
- B. It offers centralized control of all user authentication, authorization, and accounting.
- C. Different levels of security can be concurrently used with Cisco Secure ACS for different requirements.
- D. It supports large networked environments with redundant servers, remote databases, and user database backup services.

Answer: B

QUESTION 36:

Why is a Security Management system's ability to scale so as to manage thousands of network devices important?

- A. It allows for the future growth of the network.
- B. It allows for a more secure network environment.
- C. It allows for more efficient network bandwidth usage.
- D. It allows for more devices to be managed with fewer people.
- E. It reduces human error by eliminating the network administrators.

Answer: B

QUESTION 37:

With regard to the Cisco Security Management solution, which of the following statements are true? (Choose all that apply.)

- A. It can manage all security devices including non-Cisco appliances.
- B. The CiscoWorks Monitoring Center for Security is the flagship multidevice management solution.
- C. The complete network Security Management system is needed to coordinate and monitor all of the security components.
- D. Embedded Security Device Manager (EDSM) enables the configuration of Cisco security devices without requiring CLI knowledge.

Answer: C, D

QUESTION 38:

You are a network technician at Certkiller . Your newly appointed Certkiller trainee wants to know what functions of the Cisco Security Management System are. What will your reply be?

- A. In depth layered security and defense.
- B. Multi-site management and secure connectivity.
- C. Multi-device management and secure connectivity.
- D. Embedded device management, multiple device management, and policy management.

Answer: D

QUESTION 39:

Which of the following is an advantage of implementing a security policy through centralized Security Management tools?

- A. Security decisions can be made once, in advance for the whole network.
- B. Security decisions can be made locally, close to where new threats appear.
- C. Security decisions can be made by the user, to fit their individual business needs.
- D. Security decisions can be made locally, by the business manager nearest the user or customer.

Answer: A

QUESTION 40:

For which of the following devices can you use Cisco Security Management Centers to configure, monitor, and troubleshoot? (Choose all that apply.)

- A. Cisco firewalls
- B. Cisco Catalyst switches
- C. Cisco VPN concentrators
- D. Cisco intrusion detection sensors
- E. Cisco content networking switches

Answer: A, C, D

QUESTION 41:

You are a network technician at Certkiller . The Certkiller CEO is concerned about updating the security software on the remote Certkiller VPN devices.

Which topics should you discuss with the Certkiller CEO?

- A. Hiring additional personnel to update remote sites.
- B. Selecting encryption algorithms for VPN implementation.
- C. Complying with industry standards using Cisco SAFE Blueprint.
- D. Implementing the Cisco SAFE Blueprint and the use of Security Management.

Answer: D

QUESTION 42:

Why is the Cisco SAFE Blueprint useful in terms of cost saving?

- A. It allows for immediate implementation.
- B. It can propose alternative and modular implementations.
- C. It specifies only Cisco products, excluding competing products.
- D. It avoids the cost issue because it does not make specific recommendations.

Answer: B

QUESTION 43:

You work as a network consultant. You are contracted by Certkiller to develop a security strategy. Certkiller does not have a security policy for the entire enterprise. How would you develop an effective account strategy for Certkiller ?

- A. Offer to write a security policy for the customer.
- B. Inform the customer about the risks to the business.
- C. Find a reference account that demonstrates the negative consequences of not having a security policy.
- D. Use the Cisco SAFE Blueprint to consult with the customer in building and implementing a security policy.

Answer: D

QUESTION 44:

In the Cisco SAFE Blueprint, which module addresses secure connectivity to ISPs and public telephone networks?

- A. Extranet Edge
- B. Enterprise Edge
- C. Enterprise Campus
- D. Service Provider Edge
- E. Service Provider Campus

Answer: A

QUESTION 45:

Which customer executive would the benefit of VPN solutions and products that integrate security into the overall network architecture, which illustrates the importance of security along with that of switches and routers most appeal to?

- A. Chief Security Officer
- B. Chief Financial Officer
- C. Chairman of the Board

- D. Chief Executive Officer
- E. Chief Information Officer

Answer: E

QUESTION 46:

Which of the following is a characteristic of the Cisco SAFE Blueprint?

- A. Static design
- B. Modular approach
- C. Two fundamental areas
- D. Division into security zones
- E. Developed by an industry association

Answer: B

QUESTION 47:

You are the network administrator at Certkiller . Certkiller expects to grow their network dramatically in the near future. The company is concerned about the current security policy being adequate for the expanded network.

What should the account team recommend?

- A. The account team should consult with government agencies for legal compliance.
- B. The account team should purchase the Cisco SAFE Blueprints to conduct a review of their security policy.
- C. The Cisco SAFE Blueprint can help the account team plan and verify necessary changes to their security policy.
- D. The account team should require their prospective equipment vendors to demonstrate how their equipment will comply with their security policy.

Answer: C

QUESTION 48:

For which of the following is the Cisco SAFE Blueprint is the most reliable and effective tool?

- A. The building of a test network.
- B. Compliance with government regulation.
- C. The expansion and scaling of an existing network.
- D. The first installation ("greenfield") of a network only.
- E. Contracting outsourcing and service provider networking services.

Answer: C

QUESTION 49:

With regard to the use of products in the Cisco SAFE Blueprint, which of the following statements is true?

- A. You can only use Cisco security products.
- B. You only use network-based IDS for perimeter security.
- C. You should use best of breed products from any vendor.
- D. You can only use security products with Microsoft operating systems.
- E. You can only use Cisco security products with SUN operating systems.

Answer: A

QUESTION 50:

Certkiller currently has a contracted Frame Relay network services. The company wants to convert to VPN services. The IT director wants a checklist to ensure the company has not incurred new security vulnerabilities or lost security protections.

Which of the following statements about checklists is true?

- A. Government agencies supply the correct checklist.
- B. The Cisco SAFE Blueprint is a theoretical document only.
- C. The Cisco SAFE Blueprint is the best and most complete checklist.
- D. Industry standards are the safest guides and should be used as the checklist.
- E. The international Common Criteria is the most complete and most widely adopted checklist.

Answer: C

QUESTION 51:

For which of the following would you use the Cisco SAFE Blueprint to effectively plan for? (Choose all that apply.)

- A. Security audits
- B. All types of threats and vulnerabilities.
- C. Compliance with government regulations.
- D. Network installation, expansion, and upgrading.
- E. Equipment placement and capacities specifications.

Answer: A, D, E

QUESTION 52:

Which Cisco SAFE Blueprint module should you use for a customer that is looking at e-commerce and contemplating VPN connectivity for their sales representatives?

- A. Enterprise Edge Module
- B. Enterprise Campus Module
- C. Extranet Connectivity Module
- D. Service Provider Edge Module
- E. Service Provider Campus Module

Answer: A

QUESTION 53:

Which of the following represents the effective uses of the Cisco SAFE Blueprint? (Choose all that apply.)

- A. Security policy enforcement.
- B. Guidance for performing network security audits.
- C. Prevention of attacks to networks, network devices, and computers.
- D. Enforcement of non-disclosure agreements, background checks, and security clearances for vendors and contractors.
- E. Designing guidelines for physical access by personnel to networks, plant, equipment, offices, and headquarters.

Answer: A, B, C

QUESTION 54:

You are the network administrator at Certkiller . Certkiller experiences a security failure that leads to a catastrophic loss of intellectual property. What should you do immediately?

- A. Implement legal proceedings.
- B. Outsource your security services.
- C. Use the Cisco SAFE Blueprint to guide a security audit.
- D. Rewrite their security policy, using the Cisco SAFE Blueprint.

Answer: C

QUESTION 55:

Which of the following represents the effective uses of the Cisco SAFE Blueprint? (Choose all that apply.)

- A. Designing guidelines for implementing security policy.
- B. Designing guidelines for adding security functionality and features to an existing network.
- C. Providing performance and processing requirements and capacity and load balancing of security equipment.
- D. Designing guidelines for physical access by personnel to networks, plant, equipment, offices, and headquarters.
- E. Enforcement of non-disclosure agreements, background checks, and security clearances for vendors and contractors.

Answer: A, B, C

QUESTION 56:

You are the network administrator at Certkiller . Certkiller has a Cisco PIX Firewall at the corporate site. The company wants to implement a remote access VPN solution without incurring the cost of purchasing another product.

How can Certkiller accomplish this?

- A. By upgrading to a higher level firewall.
- B. By using the WAN port for a VPN module.
- C. By installing and configuring the VPN accelerator card.
- D. By using the maintenance plan upgrade to the next level of Cisco PIX OS.

Answer: C

QUESTION 57:

For which of the following can the Cisco SAFE Blueprints be used?

- A. As a guide for planning secure access to the Internet only.
- B. As a guide for planning secure connectivity within the intranet only.
- C. As a guide for planning secure connectivity within and between the extranet.
- D. As a guide for planning secure connectivity within and between any networks being used.

Answer: D

QUESTION 58:

Through which means do Cisco VPNs provide protection from data interception?

- A. SHTTP, IPSec, and SSL termination
- B. Encryption, IPSec, and Cut-Through Proxy
- C. Secure connectivity, IPSec, and SSL termination

D. Secure connectivity, encryption, and Traffic authentication

Answer: D

QUESTION 59:

What is the most commonly used technology for VPN encryption in remote intranet environments?

- A. SSL
- B. LEAP
- C. IPSec
- D. TACAS
- E. RADIUS

Answer: C

QUESTION 60:

Why is a VPN solution cost effective?

- A. The gear to set up and run a VPN is inexpensive.
- B. The VPN equipment is not owned by the customer.
- C. The service provider can charge for access to the VPN.
- D. Long distance chargers and leased line fees are eliminated.

Answer: D

QUESTION 61:

What are two benefits CiscoWorks VMS provides? (Choose two.)

- A. Integrated billing services.
- B. Efficient centralized configuration of security devices
- C. Self correcting recovery from Denial of Service attacks
- D. Integrated management for different types of security devices

Answer: A, B

QUESTION 62:

Your customer upgraded their network. It is now larger and more complex to administer. What should you discuss with the IT director?

- A. The benefits of outsourcing
- B. The features of site-to-site VPN
- C. The features of provisioned services
- D. The features of Security Management

Answer: D

QUESTION 63:

A business has successfully included distributors in its intranet, and now wants to include suppliers and vendors.

For intranet security, you recommend that they rely on _____.

- A. The service provider's Security Management
- B. Accurate and up-to-date access list on all the edge routers
- C. The security features in the applications the new users will be using
- D. Updating the security policy, using the Cisco SAFE guidelines for all elements.

Answer: D

QUESTION 64:

Which three statements are true about Cisco Embedded Security Device Managers (ESDMs)? Choose three

- A. ESDMs can be useful when deploying new equipment-
- B. ESDMs allow security administrators to work one device at a time
- C. ESDMs can be useful for managing the security of a large network.
- D. ESDMs are useful for recovering from security breaches on multiple devices.

Answer: A, B, C

QUESTION 65:

How does Cisco Intrusion Protection address the issue of unauthorized access to critical sensitive data?

- A. Provides embedded device, multi-device and policy management control
- B. Reduces additional financial losses by shutting down the network on intrusions
- C. Enables the configuration of Cisco IDS sensor using Command Line Interface (CLI)
- D. Supports corporate security policy by constantly validating, assessing, and reporting on the security status of all network components

Answer: D

QUESTION 66:

What are three good reasons for purchasing Intrusion Protection? Choose three

- A. Security breaches are increasingly the result of outside attackers.
- B. Users inside the network can cause significant damage, either intentionally or by accident.
- C. Organizations need additional security technologies to counter risks that firewalls alone cannot address.
- D. As the sophistication or hacker tools increases the technical knowledge and skill to deploy these complex attacks decreases.

Answer: B, C, D

QUESTION 67:

Which three statements are true about Network IDS (NIDS)? Choose three.

- A. NIDS is generally not impacted on the host.
- B. NIDS can protect all hosts on an monitored network.
- C. NIDS are often better at preventing specific attacks than host IDS.
- D. NIDS can detect network probes and Denial of Service (DoS) attacks.
- E. NIDS requires that client software be installed on all hosts in the network.

Answer: A, B, C

QUESTION 68:

Which action can be performed when a Cisco IDS sensor detects an attack?

- A. VPN client notification and alert can be sent.
- B. TCP Reset can terminate the attacking session.
- C. A router can isolate the network from the intruder.
- D. A counterattack can be launched at the IP address of the offending packet.

Answer: B

QUESTION 69:

How does the Cisco Security Agent protect against unknown attacks?

- A. By instantaneously updating the signature database as soon as its signature is interpreted.
- B. By comparing the signature of the attack against other known attacks that may be similar in function

- C. By analyzing each packet on the network to detect intrusions that can cause damage to the network
- D. By monitoring operating systems and applications for suspicious activity that falls outside normal behavior defined in the security policy

Answer: D

QUESTION 70:

When contemplating a VPN/Security installation, why is manageability a critical concern for the customer?

- A. All devices must be configured to allow specified traffic only.
- B. All devices must be configured to allow or disallow specified traffic only.
- C. All devices must be configured to allow or disallow specified traffic and recognize unauthorized traffic.
- D. All devices must be configured to allow or disallow traffic and shut off the network in cases of attack.

Answer: C

QUESTION 71:

Your account team is selling to a large, global company, that has many large manufacturing divisions, sales offices around the world, small subsidiaries, and medium businesses in many countries.

The Cisco SAFE Blueprint can help your account team propose security solutions for the account's _____.

- A. Subsidiaries
- B. Sales and branch offices
- C. Entire network and all sites
- D. Headquarters and large divisions

Answer: C

QUESTION 72:

The Cisco SAFE Blueprint can be used in planning the detection and prevention of _____.

- A. Governmental audits.
- B. Accidental loss of data and disaster recovery.
- C. Extortion, blackmail, and other criminal activities.
- D. Hacking attempts, viruses, worms, and unauthorized access.

Answer: D

QUESTION 73:

What are three characteristics of the Cisco SAFE Blueprint? (Choose three)

- A. Static
- B. Modular
- C. Dynamic
- D. Theoretical

Answer: B, C, D

QUESTION 74:

What results from using the Cisco SAFE Blueprint to plan network security?

- A. Equipment costs for implementing redundancies are increased.
- B. The users have a greater responsibility for enforcing security policy.
- C. The network is less responsive due to added security processing demands on the equipment.
- D. There are fewer disruptions due to network security breaches and therefore productivity increases.

Answer: D

QUESTION 75:

Which Cisco SAFE Blueprint module provides internal users with connectivity to Internet services and provides Internet users access to information on public servers?

- A. WAN
- B. E-commerce
- C. Corporate Internet
- D. VPN/remote access

Answer: C

QUESTION 76:

A charitable organization is implementing online donations.
What should they do to secure their data?

- A. Not allow online transactions.
- B. Only allow access to registered users.
- C. Consider all of the SAFE Blueprint principles.
- D. Establish rigorous authentication procedures.

Answer: C

QUESTION 77:

The Cisco SAFE Blueprint can be used to plan security for networks that are _____.

- A. Government certified.
- B. Composed of Cisco products only.
- C. Homogenous networks of routers and switches only.
- D. Heterogeneous networks equipped by multiple vendors.

Answer: D

QUESTION 78:

The Cisco SAFE Blueprint can help customers plan for _____

- A. Networks of any scale.
- B. Enterprise networks only.
- C. Service provider networks.
- D. Commercial and governmental networks only.

Answer: A

QUESTION 79:

Which module, within the Enterprise Campus area of the Cisco SAFE Blueprint, routes and switches from one network to another as fast as is possible?

- A. Core
- B. Server
- C. Edge Distribution
- D. Building Distribution

Answer: A

QUESTION 80:

Why is the Cisco SAFE Blueprint modular?

- A. To allow redundant network design.

- B. To allow ease in ordering the separate SAFE modules.
- C. To allow for greater flexibility in attack mitigation, implementation, and deployment.
- D. To allow one area of the document to be changed without affecting the other areas.

Answer: C

QUESTION 81:

A customer is planning to add mission-critical applications that will require priority processing and increased security as compared to their existing applications.

What should they do?

- A. Use the Cisco SAFE Blueprint to develop a new security policy.
- B. Compare industry standards to derive their own list of requirements.
- C. Use the Cisco SAFE Blueprint to identify the network services, priorities, and capacities needed.
- D. Depend on the applications vendors to specify the added requirements and capacities needed.

Answer: C

QUESTION 82:

Your customer has asked for your account team's help in implementing their security policy.

Why is the Cisco SAFE Blueprint a useful guide to both you and the customer?

- A. It recommends implementation all-at-once.
- B. It changes the security policy to a standard policy.
- C. It is a fee-based consulting service available only from Cisco directly.
- D. It can be used with heterogeneous networks and third-party products as well as Cisco products.

Answer: D

QUESTION 83:

Why is the Cisco SAFE Blueprint an effective planning tool?

- A. It was developed by the U.S. government.
- B. It recommends a multilayer defense against attacks.
- C. It has been endorsed by several industry associations.
- D. It specifies equipment to buy by manufacturer and model numbers.

Answer: B

QUESTION 84:

A large, global business has revised its security policy for the entire organization, including headquarters, major divisions, branch offices, and subsidiaries (which are small and medium businesses).
The Cisco SAFE Blueprint recommends implementing for the new policy _____.

- A. Only at headquarters and the larger divisions.
- B. At the same time, throughout the entire organization.
- C. Independently at each site, to insulate other sites from possible security vulnerabilities.
- D. Modularly, according to a schedule that the staff, vendors, and consultants can install and activate effectively.

Answer: D

QUESTION 85:

Why is intrusion Protection needed?

- A. Intrusion Protection allows network managers to use a single database for authentication of all remote users.
- B. Intrusion Protection gives networks an added layer of defense to protect from external attacks and internal attacks.
- C. Intrusion Protection can more easily connect to remote branch offices using automatic encryption tools to protect data transmission.
- D. Intrusion Protection increases the resilience of networks by providing instantaneous failover without the need to re-establish sessions.

Answer: B

QUESTION 86:

Using a physical analogy, Intrusion Protection devices can be compared to_____.

- A. Badge readers that log entry to buildings.
- B. Armored transport cars between buildings that permit source, confident transit.
- C. Guards that monitor entry points throughout the building and prevent intruders from breaking in to the facility.
- D. A door lock at the perimeter of the building that permit only authorized users to enter (such as those with a key are a badge).

Answer: C

QUESTION 87:

Why would a company choose to implement Networks IDS using the IDS Module in a Catalyst 6000?

- A. The Catalyst 6000 IDS Module is the only way to provide IDS for VLANs.
- B. The Catalyst 6000 IDS Module provides additional firewall protection for all users connected to the switch.
- C. The Catalyst 6000 IDS Module allows the company to integrate IDS functions into the core of their network.
- D. The Catalyst 6000 IDS Module provides comprehensive support of common password protocols required for user authentication.

Answer: C

QUESTION 88:

What are two ROI justifications for an Identity Solution? (Choose two)

- A. Reduces administrative costs.
- B. Reduces cost to track and prosecute malicious users.
- C. Investment protection to leveraging the existing infrastructure.
- D. Protection of financial returns from intellectual property and secure data.

Answer:

QUESTION 89:

What does an Identity Solution do?

- A. Verifies that data are being sent from a trusted source.
- B. Identifies malicious code hidden in a user's data stream.
- C. Controls access to proprietary or confidential information.
- D. Improves network performance by restricting user access to certain segments of the network.

Answer: C

QUESTION 90:

What is the cause of most Enterprise security issues?

- A. Unattended workstations.
- B. Inadequate tracking of network users.
- C. Failure to apply patches to applications and operating systems.
- D. Poor implementation of user identification and password mechanisms.

Answer: D

QUESTION 91:

Cisco IOS Firewall provide stateful packet filtering, intrusion detection, per-user authentication, VPN functionality, and multiprotocol routing features.

How does the account team propose these features?

- A. Integrated solution
- B. Hot Standby solution
- C. Standards-based VPN solution
- D. Centralized management solution

Answer: A

QUESTION 92:

There are several methods for implementing firewalls.

What major advantage does a dedicated firewall device have when throughput and security are desired?

- A. The management console is easily installed.
- B. The hackers know most routerbased firewall code.
- C. The device contains proprietary operating systems.
- D. The connection to the device is monitored by security personnel.

Answer: C

QUESTION 93:

When planning to implement firewalls for perimeter security, IT professionals are concerned with ____.

- A. User ID's and passwords.
- B. The costs of travel to each site to install firewalls.
- C. Installing client software on each remote computer.
- D. The additional processing performance required of devices.

Answer: D

QUESTION 94:

An organization is installing dedicated Cisco PIX Firewall appliances to replace software-based firewall functions.

What are three benefits of this action? (Choose three)

- A. Faster processing
- B. More robust filtering services
- C. Lower equipment acquisition costs.
- D. Protection from operating system vulnerabilities.

Answer: A, B, D

QUESTION 95:

Network perimeter security is a first line defense system.

Which three types of devices can provide this level of security? (Choose three)

- A. routers
- B. switches
- C. VPN concentrators
- D. Dedicated firewall appliances

Answer: A, B, D

QUESTION 96:

To reduce costs, and IT department has decided to implement VPN services to replace Frame Relay leased lines.

When converting, what happens to their security concerns?

- A. They will increase, because the VPN is tunneling through the unsecured Internet.
- B. They will decrease, because, VPN security is inherently more secure than hardware connections between routers.
- C. They will remain the same, because the service provider will take over responsibility for the organization's security policy.
- D. They will remain the same, because the VPN service provider will provide the same level of security across the VPN tunnel as over the leased line.

Answer: A

QUESTION 97:

Cisco IOS Firewalls scale from low-end to high-end routing series to provide functionality to different market segments.

Which router series include the Cisco IOS Firewall option?

- A. Catalyst 4000 series

- B. Cisco 10000, and 12000 series
- C. Cisco 800, 1700, 2600 series only
- D. Cisco 800, 1700, 2600, 3700, and 7000 series

Answer: D

QUESTION 98:

Which Cisco firewall solution provides basic firewall functions and does not require a dedicated hardware device?

- A. Cisco PIX Firewall
- B. Cisco IOS Firewall
- C. Cisco Secure ACS
- D. Cisco Catalyst Firewall Module

Answer: B

QUESTION 99:

Network integrity refers to the safety of network devices and the secure flow of information between them. Network integrity also involves _____. (Choose three)

- A. payload data
- B. configuration
- C. user passwords
- D. configuration updates
- E. remote user authentication

Answer:

QUESTION 100:

Which industry standard does the Cisco PIX Firewall support for encryption for site-to-site and remote access VPNs?

- A. LEAP
- B. IPSec
- C. RADIUS
- D. TACACS

Answer: B

QUESTION 101:

What is the basic functions of a firewall?

- A. To scan for viruses.
- B. To stop unauthorized access to the network.
- C. To provide network connectivity to the switches.
- D. To provide management capacities to the routers.

Answer: B

QUESTION 102:

Which technology allows remote users the same access over a public network that they would have over a private one?

- A. Extranets
- B. Spanning Tree
- C. Internet portals
- D. Virtual Private Network

Answer: D

QUESTION 103:

You have proposed four VPN routers and a robust firewall to your client. Which type of solution are you implementing?

- A. Site-to-site VPN
- B. AAA redundancy
- C. VPN redundancy
- D. Remote access VPN

Answer: A

QUESTION 104:

The customer has agreed to implement a Cisco site-to-site VPN. They are concerned about managing the remote sites.

What is your recommendation?

- A. Cisco VPN Monitor

- B. Cisco Secure ACS
- C. Cisco Traffic Directory
- D. Cisco WAN Management

Answer: A

QUESTION 105:

What is an advantage of deploying VPNs?

- A. Cost savings
- B. Intrusion Protection
- C. Application integration
- D. Wireless LAN implementation

Answer: A

QUESTION 106:

A VPN is a secure, encrypted tunnel.

What does the remote user tunnel through? (Choose two)

- A. Internet
- B. Fiber optic
- C. Frame Relay
- D. Converged network

Answer: A

QUESTION 107:

The HR director is concerned about the speed with which information can be delivered but is more concerned about confidential information being viewed by other employees.

Which two solutions should you recommend? (Choose two)

- A. site-to-site VPN
- B. Access Control List
- C. Remote access VPN
- D. Cisco IP/TV broadcast

Answer:

QUESTION 108:

What does remote access VPN do? (Choose two)

- A. Eliminates modem-technology management issues.
- B. Extends the WAN as an extranet to business partners and suppliers.
- C. Delivers Internet access and web-based applications across multiple locations.
- D. Provides secure business-quality connections over the Internet, allowing for cost savings, better performance, and more reliable remote access connections.

Answer: A, B, D

QUESTION 109:

A customer is discussing the high cost of their leased lines as a rationale for not moving ahead with implementing a firewall solution.

This is a good time to discuss_____.

- A. Leasing options for the firewall.
- B. How VPNs can save them money.
- C. Promotions that will lower the cost of the firewall.
- D. How IDS can monitor their leased lines for threats.

Answer: B

QUESTION 110:

Which technology in Cisco VPNs makes voice and multimedia transmission possible?

- A. V3PN
- B. Easy VPN
- C. 3DES encryption
- D. Remote access VPN

Answer: A

QUESTION 111:

Your customer has VPN capable routers at remote sites but has never used the functionality. What is required to make the VPN function properly?

- A. A VPN concentrator at each site.

- B. A VPN termination device at the corporate site.
- C. A VPN management console at each remote location.
- D. A VPN concentrator, firewall, and VPN router at the corporate site.

Answer: B

QUESTION 112:

What is one advantage of Cisco Integrated Security?

- A. Cisco device managers allow users to make business required exceptions to the Security Policy.
- B. A Cisco IDS sensor can automatically report security breaches directly to law enforcement agencies.
- C. Cisco Security Agent Monitor can protect servers and desktops from Trojan horses and buffer overflows.
- D. A Cisco IDS sensor can directly modify the Access Control List (ACL) in a Cisco router to deny access to an offending IP address.

Answer: D

QUESTION 113:

Cisco Intrusion Detection Systems include host and network sensors.
Which two additional sensors are offered? (Choose two)

- A. switch sensors
- B. reboot sensors
- C. firewall sensors
- D. power failure sensors

Answer:

QUESTION 114:

When positioning the ROI on Intrusion Protection you should discuss _____.

- A. Simplified network management.
- B. Protection of proprietary or confidential data.
- C. Costs of badge readers and security checkpoints.
- D. Protection of valuable assets and network resources.

Answer: A