



Exam: 646-301

Title : VPN/Security

Ver : 04.21.04

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 form 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 realtime 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 cutting 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 System Works
- 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 Identity 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/supplicant 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/supplicant 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 Cisco Works 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 ecommerce 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
