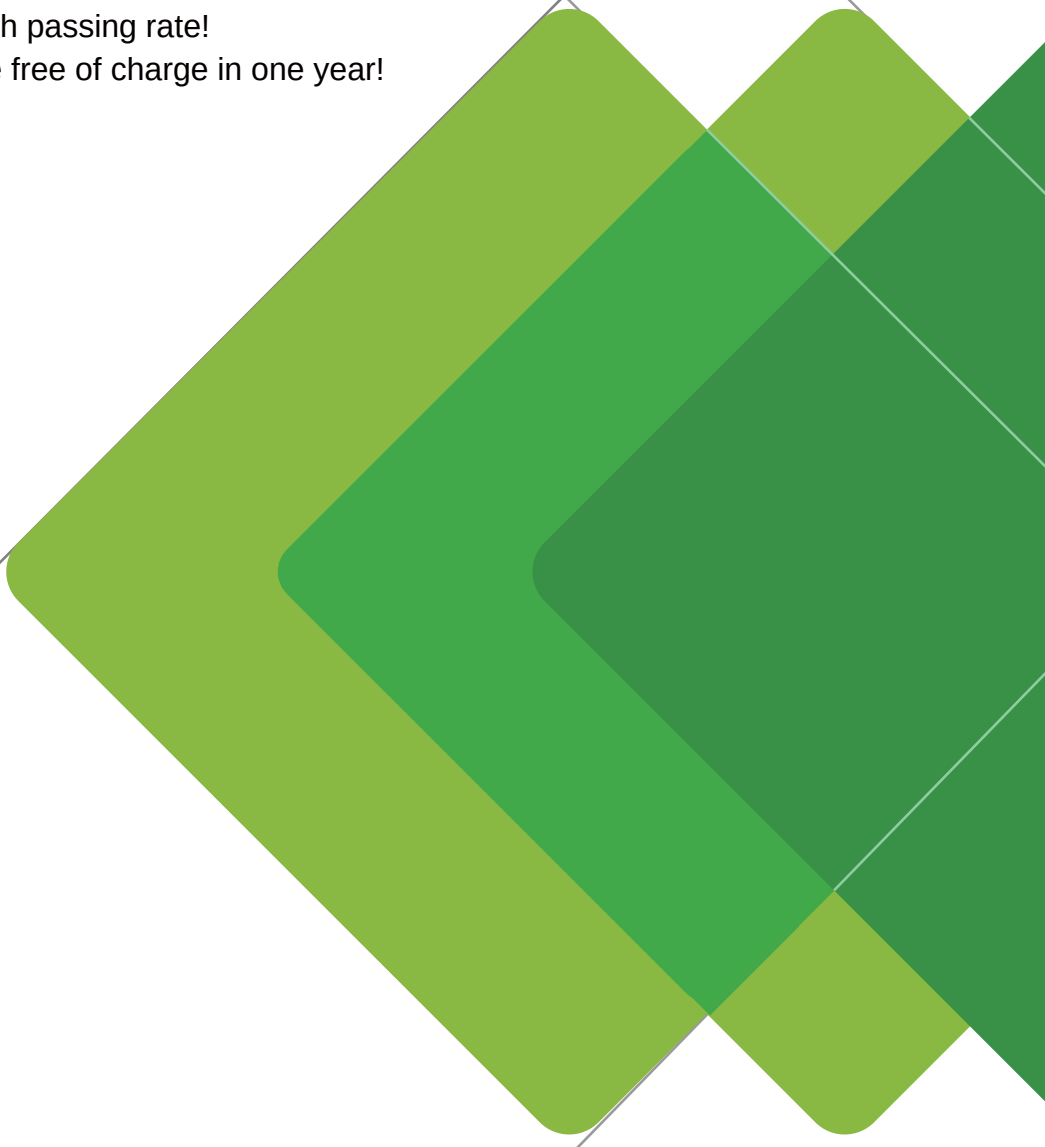
IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!



**Exam** : **642-566**

**Title** : Security Solutions for Systems Engineers

**Version** : Demo

1. Which one of the following elements is essential to perform events analysis and correlation?

A. implementation of a centralized provisioning system, such as Cisco Security Manager

B. elimination of all the true positive events

C. time synchronization between all the devices

D. implementation of different security controls and platforms when using the defense-in-depth approach

**Answer:** C

2. Refer to the following Cisco products, which two can provide a captive portal to authenticate wireless users? (Choose two.)

A. Cisco NAC Profiler

B. WLAN Controller

C. Cisco NAC Guest Server

D. Cisco ASA

**Answer:** BC

3. Which two of these statements describe features of the RSA keys? (Choose two.)

A. The private key only encrypts.

B. The private key only decrypts.

C. The public key both encrypts and decrypts.

D. The private key both encrypts and decrypts.

**Answer:** CD

4. Which item will be performed on Cisco IP Phones so that they can authenticate it before obtaining network access?

A. AAA client

B. Cisco Security Agent

C. IEEE 802.1X supplicant

D. one-time password

**Answer:** C

5. Can you tell me which one of the following platforms has the highest IPsec throughput and can support the highest number of tunnels?

A. Cisco 7200 NPE-GE+VSA

B. Cisco 7200 NPE-GE+VAM2+

C. Cisco ASR 1000-5G

D. Cisco 6500/7600 + VPN SPA

**Answer:** D

6. You are the network consultant from Cisco.com. Please point out two functions of Cisco Security Agent.

A. authentication

B. control of executable content

C. resource protection

D. spam filtering

**Answer:** BC

7. In today's typical single-tier firewall system, which three security components can be found? (Choose three.)

A. Stateful Packet Filtering with Application Inspection and Control

B. IPS

C. Network Admission Control

D. application proxy

E. Cache engine

F. server load balancing

**Answer:** ABD

8. Secure Sockets Layer (SSL) is a cryptographic protocol that provides security and data integrity for communications over TCP/IP networks such as the Interne. When SSL uses TCP encapsulation on Cisco SSL VPNs, the user's TCP session is transported over another TCP session, thus making flow control inefficient if a packet is lost. Which is the best solution of this problem?

A. Cisco Secure Desktop

B. DAP

C. DTLS

D. SSL traversal

**Answer:** C

9. Cisco NAC Appliance (formerly Cisco Clean Access) is an easily deployed Network Admission Control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether networked devices such as laptops, desktops, and other corporate assets are compliant with a network's security policies, and it repairs any vulnerabilities before permitting access to the network. Which three policy types can be assigned to a network user role in the Cisco NAC Appliance architecture? (Choose three.)

A. allowed IP address ranges

B. session duration

C. network port scanning plug-ins

D. VPN and roaming policies

**Answer:** BCD

10. Which option is correct about the relationship between the terms and their descriptions?

Term

1. true positives

2. false positives

3. ture negatives

4. false negatives

Description

I. security control has not acted,even though there was malicious activity

II. security control has not acted,as there was no malicious activity

III. security control acted as a consequence of non-malicious activity

IV. security control acted as a consequence of malicious activity

A. I-4,II-3,III-2,IV-1

B. I-4,II-3,III-1,IV-2

C. I-4,II-2,III-1,IV-3

D. I-4,II-2,III-3,IV-1

**Answer:** A

11. Observe the following Cisco software agents carefully, can you tell me which one uses content scanning to identify sensitive content and controls the transfer of sensitive content off the local endpoint over removable storage, locally or network-attached hardware, or network applications?

A. Cisco IronPort Agent 3.0

B. Cisco Trust Agent 2.0

C. Cisco NAC Appliance Agent 4.1.3

D. Cisco Security Agent 6.0

**Answer:** D

12. _____ is a valid method to verify a network security design?

A. network audit

B. network security

C. computer simulation

D. pilot or prototype network

**Answer:** D

13. Which description is true about the hybrid user authentication model for remote-access IPsec VPNs?

A. VPN servers authenticate by using digital certificates, and users authenticate by using pre-shared keys.

B. VPN servers authenticate by using digital certificates, and users authenticate by using usernames and passwords.

C. VPN servers and users authenticate by using digital certificates.

D. VPN servers and users authenticate by using pre-shared keys.

**Answer:** B

14. Look at the following items carefully, which Cisco ASA's Unified Communications proxy feature manipulates both the signaling and the media channels?

A. CUMA Proxy

B. TLS Proxy

C. H.323 Proxy

D. Phone Proxy

**Answer:** D

15. You are the network consultant from Cisco.com. Please point out two components included in a detailed design document for a security solution.

A. WEP

B. existing network infrastructure

C. IDS

D. proof of concept

**Answer:** BD

16. Which Cisco product can provide endpoint-based trusted-traffic marking while implementing QoS?

A. Cisco Trust Agent

B. Cisco Secure Services Client

C. Cisco Secure Desktop

D. Cisco Security Agent

**Answer:** D

17. Which functions can be provided by Cisco SSL VPN solution by use of the Cisco Secure Desktop? (Multiple choice.)

A. pre-login assessment

B. secure vault

C. Cache Cleaner

D. Advanced Endpoint Assessment

**Answer:** ABCD

18. Cisco Security Agent is the first endpoint security solution that combines zero-update attack protection, data loss prevention, and signature-based antivirus in a single agent. This unique blend of capabilities defends servers and desktops against sophisticated day-zero attacks, and enforces acceptable-use and compliance policies within a simple management infrastructure .What are three functions of CSA in helping to secure customer environments?

A. application control

B. control of executable content

C. identification of vulnerabilities

D. system hardening

**Answer:** ABD

19. While using the Gateway Load Balancing Protocol to enable high-availability Cisco IOS firewalls, what should be configured to maintain symmetric flow of traffic?

A. static routing

B. dynamic routing

C. CEF

D. network address translation (NAT)

**Answer:** D

20. Which one of the following platforms could support the highest number of SSL sessions?

A. Cisco 7200 NPE-GE+VAM2+

B. Cisco ASR 1000-5G

C. Cisco 6500/7600 + VPN SPA

D. Cisco ASA 5580

**Answer:** D

21. You are the network consultant from Cisco.com. Please point out two key features of the collaborative security approach.

A. integration of security features in network equipment

B. Network Admission Control

C. coordinated defense of potential entry points

D. automated event and action filters

**Answer:** BC

22. Open Shortest Path First (OSPF) is a dynamic routing protocol for use in Internet Protocol (IP) networks. An OSPF router (routerA) on the network is running at an abnormally high CPU rate. By use of different OSPF debug commands on routerA, the network administrator determines that routerA is receiving many OSPF link state packets from an unknown OSPF neighbor, thus forcing many OSPF path recalculations and affecting routerA's CPU usage. Which OSPF configuration should the administrator enable to prevent this kind of attack on routerA?

A. multi-area OSPF

B. OSPF stub area

C. OSPF MD5 authentication

D. OSPF not-so-stubby area

**Answer:** C

23. Which two methods can be used to perform IPsec peer authentication? (Choose two.)

A. pre-shared key

B. AAA

C. one-time password

D. digital certificate

**Answer:** AD

24. Cisco NAC Appliance (formerly Cisco Clean Access) is an easily deployed Network Admission Control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether networked devices such as laptops, desktops, and other corporate assets are compliant with a network's security policies, and it repairs any vulnerabilities before permitting access to the network. Which two of these statements describe features of the NAC Appliance architecture. (Choose two.)

A. NAC Appliance Client evaluates the endpoint security information.

B. NAC Appliance Server acts as an authentication proxy for internal user authentication.

C. NAC Appliance Manager determines the appropriate access policy.

D. NAC Appliance Manager acts as an authentication proxy for external authentication servers.

**Answer:** CD

25. In multi-tier applications and multi-tier firewall designs, which additional security control can be used to force an attacker to compromise the exposed server before the attacker attempts to penetrate the more protected domains?

A. Implement host IPS on the exposed servers in the DMZs.

B. Make exposed servers in the DMZs dual homed.

C. At each tier, implement a transparent proxy component within the firewall system.

D. Implement in-band network admission control at the first tier.

**Answer:** B

26. In reconnaissance attacks, which two attack methods are typically used? (Choose two.)

A. TCP/UDP port scanning and sweeping

B. buffer overflows

C. ARP spoofing

D. operating system and application fingerprinting

**Answer:** AD

27. You are the network consultant from Cisco.com. Please point out three technologies address ISO 17799 requirements for unauthorized access prevention.

A. VPN

B. Cisco Secure Access Control Server

C. 802.1X

D. Network Admission Control

**Answer:** BCD

28. Which method can be used by Cisco SSL VPN solution to provide connections between a Winsock 2, TCP-based application and a private site without requiring administrative privileges?

A. Cisco Secure Desktop

B. application plug-ins

C. port forwarding

D. smart tunnels

**Answer:** D

29. Which is the best countermeasure to protect against rogue access points that are outside the enterprise physical perimeter and that attempt to attract legitimate clients?

A. personal firewall

B. Management Frame Protection

C. wireless IDS/IPS

D. EAP-TLS bidirectional authentication

**Answer:** D

30. _____ are needed for a device to join a certificate-authenticated network?

A. the certificates of the certificate authority and the device

B. the certificates of the device and its peer

C. the certificates of the certificate authority and the peer

D. the certificates of the certificate authority, the device, and the peer

**Answer:** A