IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **640-554**

Title : Implementing Cisco IOS Network Security (IINS v2.0)

Version : Demo

1. Topic 1, Common Security Threats

Which two features are supported by Cisco IronPort Security Gateway? (Choose two.)
A. Spam protection
B. Outbreak intelligence
C. HTTP and HTTPS scanning
D. Email encryption
E. DDoS protection
Answer: A,D
Explanation:
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10154/data-sheetc78-729751.html
Product Overview
Over the past 20 years, email has evolved from a tool used primarily by technical and research professionals to become the backbone of corporate communications. Each day, more than 100 billion corporate email messages are exchanged. As the level of use rises, security becomes a greater priority. Mass spam campaigns are no longer the only concern. Today, spam and malware are just part of a complex picture that includes inbound threats and outbound risks. Cisco® Email Security solutions defend mission-critical email systems with appliance, virtual, cloud, and hybrid solutions. The industry leader in email security solutions, Cisco delivers:

2.Which two characteristics represent a blended threat? (Choose two.)
A. man-in-the-middle attack
B. trojan horse attack
C. pharming attack
D. denial of service attack
E. day zero attack
Answer: B,E
Explanation:
http://www.cisco.com/web/IN/about/network/threat_defense.html
Rogue developers create such threats by using worms, viruses, or application-embedded attacks. Botnets can be used to seed an attack, for example, rogue developers can use worms or application-embedded attacks, that is an attack that is hidden within application traffic such as web traffic or peer-to-peer shared files, to deposit "Trojans". This combination of attack techniques - a virus or worm used to deposit a Trojan, for example-is relatively new and is known as a blended attack. A blended attack can also occur in phases: an initial attack of a virus with a Trojan that might open up an unsecured port on a computer, disable an access control list (ACL), or disarm antivirus software, with the goal of a more devastating attack to follow soon after. Host Firewall on servers and desktops/laptops, day zero protection & intelligent behavioral based protection from application vulnerability and related flaws (within or inserted by virus, worms or Trojans) provided great level of confidence on what is happening within an organization on a normal day and when there is a attack situation, which segment and what has gone wrong and gives flexibility and control to stop such situations by having linkages of such devices with monitoring, log-analysis and event co-relation system.

3.Which two options represent a threat to the physical installation of an enterprise network? (Choose

two.)
A. surveillance camera
B. security guards
C. electrical power
D. computer room access
E. change control
Answer: C,D
Explanation:
http://www.cisco.com/E-Learning/bulk/public/celc/CRS/media/targets/1_3_1.swf

4.Which option represents a step that should be taken when a security policy is developed?
A. Perform penetration testing.
B. Determine device risk scores.
C. Implement a security monitoring system.
D. Perform quantitative risk analysis.
Answer: D
Explanation:
The security policy developed in your organization drives all the steps taken to secure network resources. The development of a comprehensive security policy prepares you for the rest of your security implementation. To create an effective security policy, it is necessary to do a risk analysis, which will be used to maximize the effectiveness of the policy and procedures that will be put in place. Also, it is essential that everyone be aware of the policy; otherwise, it is doomed to fail. Two types of risk analysis are of interest in information security:
Reference: http://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=2

5.Which type of security control is defense in depth?
A. threat mitigation
B. risk analysis
C. botnet mitigation
D. overt and covert channels
Answer: A
Explanation:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap1.html
SAFE Design Blueprint
The Cisco SAFE uses the infrastructure-wide intelligence and collaboration capabilities provided by Cisco products to control and mitigate well-known and zero-day attacks. Under the Cisco SAFE design blueprints, intrusion protection systems, firewalls, network admission control, endpoint protection software, and monitoring and analysis systems work together to identify and dynamically respond to attacks. As part of threat control and containment, the designs have the ability to identify the source of a threat, visualize its attack path, and to suggest, and even dynamically enforce, response actions. Possible response actions include the isolation of compromised systems, rate limiting, packet filtering, and more. Control is improved through the actions of harden, isolate, and enforce. Following are some of the objectives of the Cisco SAFE design blueprints:
• Adaptive response to real-time threats—Source threats are dynamically identified and may be blocked in

realtime.
• Consistent policy enforcement coverage - Mitigation and containment actions may be enforced at different places in the network for defense in-depth.
• Minimize effects of attack - Response actions may be dynamically triggered as soon as an attack is detected, minimizing damage.
• Common policy and security management - A common policy and security management platform simplifies control and administration, and reduces operational expense.