ISLEVER

640-554

Implementing Cisco IOS Network Security (IINS v2.0)

DEMO

https://www.islever.com/640-554.html

https://www.islever.com/cisco.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

QUESTION NO: 1

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-sheet-c78-729751.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:
• Fast, comprehensive email protection that can block spam and threats before they even hit your network
• Flexible cloud, virtual, and physical deployment options to meet your ever-changing business needs
• Outbound message control through on-device data-loss prevention (DLP), email encryption, and optional integration with the RSA enterprise DLP solution
• One of the lowest total cost of ownership (TCO) email security solutions available

QUESTION NO: 2

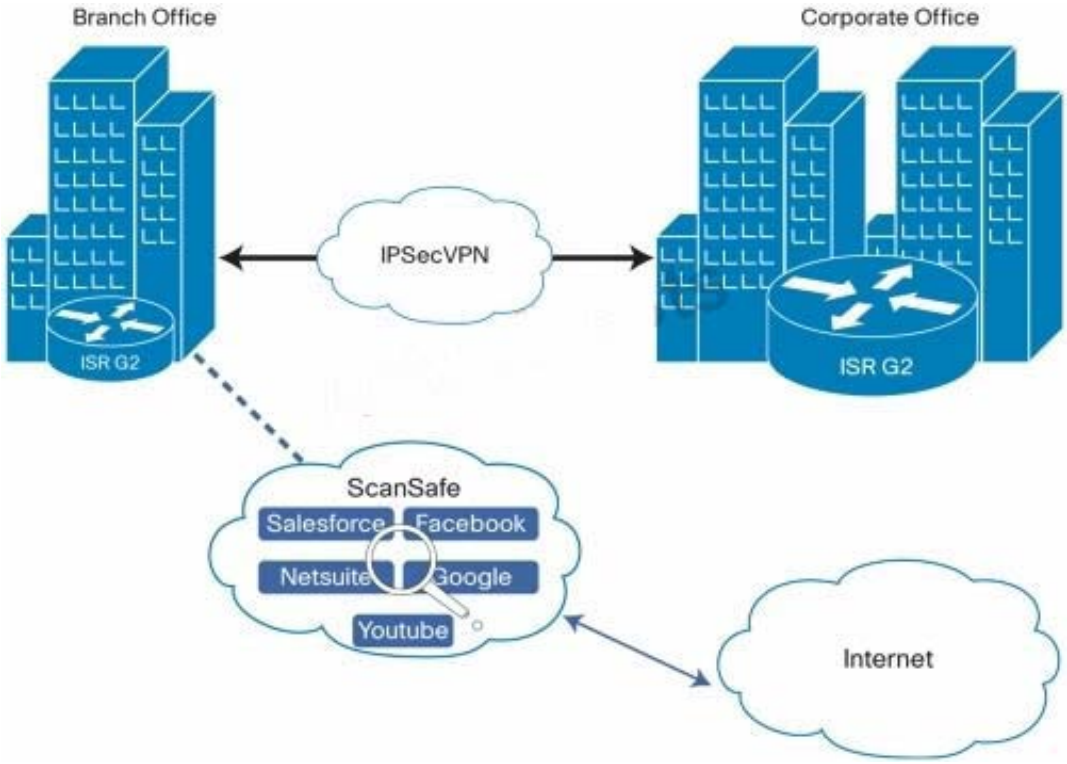
Which option is a feature of Cisco ScanSafe technology?

A. spam protection
B. consistent cloud-based policy
C. DDoS protection
D. RSA Email DLP

Answer: B

Explanation:
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6525/ps6538/ps6540/data_sheet_c78-655324.html

Cisco Enterprise Branch Web Security
The Cisco® Integrated Services Router G2 (ISR G2) Family delivers numerous security services, including firewall, intrusion prevention, and VPN. These security capabilities have been extended with Cisco ISR Web Security with Cisco ScanSafe for a simple, cost-effective, on-demand web security solution that requires no additional hardware. Organizations can deploy and enable market-leading web security quickly and easily, and can enable secure local Internet access for all sites and users, saving bandwidth, money, and resources.
Figure 1. Typical Cisco ISR Web Security with Cisco ScanSafe Deployment



Cisco ISR Web Security with Cisco ScanSafe enables branch offices to intelligently redirect web traffic to the cloud to enforce granular security and control policy over dynamic Web 2.0 content, protecting branch office users from threats such as Trojans, back doors, rogue scanners, viruses, and worms. The Cisco ISR Web Security with Cisco ScanSafe feature will be available in the Security SEC K9 license bundle

QUESTION NO: 3

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.

QUESTION NO: 4

Under which higher-level policy is a VPN security policy categorized?

A. application policy
B. DLP policy
C. remote access policy
D. compliance policy
E. corporate WAN policy

Answer: C
Explanation:
http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security