640-554 Q&As

Implementing Cisco IOS Network Security (IINS v2.0)

Pass Cisco 640-554 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/640-554.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which characteristic is the foundation of Cisco Self-Defending Network technology?

A. secure connectivity

B. threat control and containment

C. policy management

D. secure network platform

Correct Answer: D

http://www.cisco.com/en/US/solutions/ns170/networking_solutions_products_genericcontent0900aecd8051f378.html Create a Stronger Defense Against Threats Each day, you reinvent how you conduct business by adopting Internet-based business models. But Internet connectivity without appropriate security can compromise the gains you hope to make. In today\\'s connected environment, outbreaks spread globally in a matter of minutes, which means your security systems must react instantly. Maintaining security using tactical, point solutions introduces complexity and inconsistency, but integrating security throughout the network protects the information that resides on it. Three components are critical to effective information security: ?A secure network platform with integrated security to which you can easily add advanced security technologies and services ?Threat control services focused on antivirus protection and policy enforcement that continuously monitor network activity and prevent or mitigate problems ?Secure communication services that maintain the privacy and confidentiality of sensitive data, voice, video, and wireless communications while cost-effectively extending the reach of your network

QUESTION 2

Which protocol secures router management session traffic?

A. SSTP

B. POP

C. Telnet

D. SSH

Correct Answer: D

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

Encrypting Management Sessions

Because information can be disclosed during an interactive management session, this traffic must be encrypted so that a malicious user cannot gain access to the data being transmitted. Encrypting the traffic allows a secure remote access connection to the device. If the traffic for a management session is sent over the network in cleartext, an attacker can obtain sensitive information about the device and the network. An administrator is able to establish an encrypted and secure remote access management connection to a device by using the SSH or HTTPS (Secure Hypertext Transfer Protocol) features. Cisco IOS software supports SSH version 1.0 (SSHv1), SSH version 2.0 (SSHv2), and HTTPS that uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for authentication and data encryption. Note that SSHv1 and SSHv2 are not compatible.

Cisco IOS software also supports the Secure Copy Protocol (SCP), which allows an encrypted and secure connection for copying device configurations or software images. SCP relies on SSH. This example configuration enables SSH on a Cisco IOS device: ! ip domain-name example.com ! crypto key generate rsa modulus 2048 ! ip ssh time-out 60 ip ssh authentication-retries 3 ip ssh source-interface GigabitEthernet 0/1 ! line vty 0 4 transport input ssh !

QUESTION 3

Which IPsec component takes an input message of arbitrary length and produces a fixed-length output message?

A. the transform set

B. the group policy

C. the hash

D. the crypto map

Correct Answer: C

QUESTION 4

Which actions can a promiscuous IPS take to mitigate an attack? (Choose three.)

A. modifying packets

B. requesting connection blocking

C. denying packets

D. resetting the TCP connection

E. requesting host blocking

F. denying frames

Correct Answer: BDE

Promiscuous Mode Event Actions The following event actions can be deployed in Promiscuous mode. These actions are in affect for a user- configurable default time of 30 minutes. Because the IPS sensor must send the request to another device or craft a packet, latency is associated with these actions and could allow some attacks to be successful. Blocking through usage of the Attack Response Controller (ARC) has the potential benefit of being able to perform to the network edge or at multiple places within the network. Request block host: This event action will send an ARC request to block the host for a specified time frame, preventing any further communication. This is a severe action that is most appropriate when there is minimal chance of a false alarm or spoofing. Request block connection: This action will send an ARC response to block the specific connection. This action is appropriate when there is potential for false alarms or spoofing. Reset TCP connection: This action is TCP specific, and in instances where the attack requires several TCP packets, this can be a successful action. However, in some cases where the attack only needs one packet it may not work as well. Additionally, TCP resets are not very effective with protocols such as SMTP that consistently try to establish new connections, nor are they effective if the reset cannot reach the destination host in time. Reference: http://www.cisco.com/web/about/security/intelligence/ipsmit.html

QUESTION 5

Which two statements about SSL-based VPNs are true? (Choose two.)

A. Asymmetric algorithms are used for authentication and key exchange.

B. SSL VPNs and IPsec VPNs cannot be configured concurrently on the same router.

C. The application programming interface can be used to modify extensively the SSL client software for use in special applications.

D. The authentication process uses hashing technologies.

E. Both client and clientless SSL VPNs require special-purpose client software to be installed on the client machine.

Correct Answer: AD

http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/25/software/user/guide/IKE.html

Add or Edit IKE Policy

Priority

An integer value that specifies the priority of this policy relative to the other configured IKE policies. Assign the lowest numbers to the IKE policies that you prefer that the router use. The router will offer those policies first during negotiations.

Encryption

The type of encryption that should be used to communicate this IKE policy. Cisco SDM supports a variety of encryption types, listed in order of security. The more secure an encryption type, the more processing time it requires.

Note If your router does not support an encryption type, the type will not appear in the list.

Cisco SDM supports the following types of encryption:

- Data Encryption Standard (DES) — This form of encryption supports 56-bit encryption.
- Triple Data Encryption Standard (3DES) — This is a stronger form of encryption than DES, supporting 168-bit encryption.
- AES-128 — Advanced Encryption Standard (AES) encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than triple DES.
- AES-192 — Advanced Encryption Standard (AES) encryption with a 192-bit key.

AES-256 — Advanced Encryption Standard (AES) encryption with a 256-bit key.

Hash

The authentication algorithm to be used for the negotiation. There are two options:

- Secure Hash Algorithm (SHA)
- Message Digest 5 (MD5)

Authentication

The authentication method to be used.

- Pre-SHARE. Authentication will be performed using pre-shared keys.
- RSA_SIG. Authentication will be performed using digital signatures.

D-H Group

Diffie-Hellman (D-H) Group. Diffie-Hellman is a public-key cryptography protocol that allows two routers to establish a shared secret over an unsecure communications channel. The options are as follows:

- group1 — 768-bit D-H Group. D-H Group 1.
- group2 — 1024-bit D-H Group. D-H Group 2. This group provides more security than group 1, but requires more processing time.
- group5 — 1536-bit D-H Group. D-H Group 5. This group provides more security than group 2, but requires more processing time.

Note

- If your router does not support group5, it will not appear in the list.
- Easy VPN servers do not support D-H Group 1.

Lifetime This is the lifetime of the security association, in hours, minutes and seconds. The default is one day, or

24:00:00.

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.lead4pass.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: