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.passapply.com/640-554.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which statement describes how the sender of the message is verified when asymmetric encryption is used?

A. The sender encrypts the message using the sender\\'s public key, and the receiver decrypts the message using the sender\\'s private key.

B. The sender encrypts the message using the sender\\'s private key, and the receiver decrypts the message using the sender\\'s public key.

C. The sender encrypts the message using the receiver\\'s public key, and the receiver decrypts the message using the receiver\\'s private key.

D. The sender encrypts the message using the receiver\\'s private key, and the receiver decrypts the message using the receiver\\'s public key.

E. The sender encrypts the message using the receiver\\'s public key, and the receiver decrypts the message using the sender\\'s public key.

Correct Answer: C

http://www.cisco.com/en/US/tech/tk1132/technologies_white_paper09186a00800e79cb.shtml

Public-Key Cryptography and Asymmetric Encryption

In asymmetric encryption, two different keys are used to render data illegible to anyone who may be eavesdropping on a conversation. The certificates contain the two components of asymmetric encryption: public key and private key.

Data that is encrypted with the public key can be decrypted with the private key, and vice versa. However, data encrypted with the public key cannot be decrypted with the public key. The parties who need to encrypt their communications will

exchange their public keys (contained in the certificate), but will not disclose their private keys. The sending party will use the public key of the receiving party to encrypt message data and forward the cipher text (encrypted data) to the other

party. The receiving party will then decrypt the cipher text with their private key.

Data encrypted with the public key cannot be decrypted with the public key. This prevents someone from compromising the cipher text after acquiring both public keys by eavesdropping on the certificate exchange.

QUESTION 2

Which action can you take to add bandwidth to a trunk between two switches and end up with only one logical interface?

A. Configure another trunk link.

B. Configure EtherChannel.

C. Configure an access port.

D. Connect a hub between the two switches.

Correct Answer: B

QUESTION 3

Which tasks is the session management path responsible for? (Choose three.)

A. Verifying IP checksums

B. Performing route lookup

C. Performing session lookup

D. Allocating NAT translations

E. Checking TCP sequence numbers

F. Checking packets against the access list

Correct Answer: BDF

The session management path is responsible for the following tasks:

Performing the access list checks

Performing route lookups

Allocating NAT translations (xlates)

Establishing sessions in the";fast pat";

Reference: http://www.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/ intro_f.html

QUESTION 4

Which components does HMAC use to determine the authenticity and integrity of a message? (Choose two.)

A. The password

B. The hash

C. The key

D. The transform set

Correct Answer: BC

Reference: https://supportforums.cisco.com/document/6531/hmac

QUESTION 5

Which two types of access lists can be used for sequencing? (Choose two.)

A. reflexive

B. standard

C. dynamic

D. extended

Correct Answer: BD

Users can apply sequence numbers to permit or deny statements and also reorder, add, or remove such statements from a named IP access list. This feature makes revising IP access lists much easier. Prior to this feature, users could add access list entries to the end of an access list only; therefore needing to add statements anywhere except the end required reconfiguring the access list entirely. Restrictions for IP Access List Entry Sequence Numbering

-

This feature does not support dynamic, reflexive, or firewall access lists.

-

This feature does not support old-style numbered access lists, which existed before named access lists. Keep in mind that you can name an access list with a number, so numbers are allowed when they are entered in the standard or extended named access list (NACL) configuration mode. Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2s/feature/guide/fsaclseq.html