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.geekcert.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 command will block external spoofed addresses?

A. access-list 128 deny ip 10.0.0.0 0.0.255.255 any

B. access-list 128 deny ip 192.168.0.0 0.0.0.255 any

C. access-list 128 deny ip 10.0.0.0 0.255.255.255 any

D. access-list 128 deny ip 192.168.0.0 0.0.31.255 any

Correct Answer: C

QUESTION 2

Information about a managed device\\'s resources and activity is defined by a series of objects. What defines the structure of these management objects?

A. MIB

B. FIB

C. LDAP

D. CEF

Correct Answer: A

Management Information Base (MIB) is the database of configuration variables that resides on the networking device.

QUESTION 3

Which RADIUS server authentication protocols are supported on Cisco ASA firewalls? (Choose three.)

A. EAP

B. ASCII

C. PAP

D. PEAP

E. MS-CHAPv1

F. MS-CHAPv2

Correct Answer: CEF

The ASA supports the following authentication methods with RADIUS servers:

PAP -- For all connection types.

CHAP and MS-CHAPv1 -- For L2TP-over-IPsec connections.

MS-CHAPv2 -- For L2TP-over-IPsec connections, and for regular IPsec remote access connections when the password management feature is enabled. You can also use MS-CHAPv2 with clientless connections. Authentication Proxy modes

-- For RADIUS-to Active-Directory, RADIUS-to-RSA/SDI, RADIUS- to-Token server, and RSA/SDI-to-RADIUS connections

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/aaa_radius.html

QUESTION 4

Which syslog level is associated with LOG_WARNING?

A. 1

B. 2

C. 3

D. 4

E. 5

F. 6

G. 7

H. 0

Correct Answer: D

Level Number	Severity Level	Description
0	emergencies	System is unusable.
1	alert	Immediate action is needed.
2	critical	Critical conditions.
3	error	Error conditions.
4	warning	Warning conditions.
5	notification	Normal but significant conditions.
6	informational	Informational messages only.
7	debugging	Debugging messages only.

QUESTION 5

Which three statements about the IPsec ESP modes of operation are true? (Choose three.)

A. Tunnel mode is used between a host and a security gateway.

B. Tunnel mode is used between two security gateways.

C. Tunnel mode only encrypts and authenticates the data.

D. Transport mode authenticates the IP header.

E. Transport mode leaves the original IP header in the clear.

Correct Answer: ABE

http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/2.0/ip_security/provisioning/guide/IPsecPG1.html

The Encapsulating Security Payload (ESP)

The Encapsulating Security Payload (ESP) contains six parts as described below. The first two parts are not encrypted, but they are authenticated. Those parts are as follows:

?The Security Parameter Index (SPI) is an arbitrary 32-bit number that tells the device receiving the packet what group of security protocols the sender is using for communication. Those protocols include the particular algorithms and keys,

and how long those keys are valid. ?The Sequence Number is a counter that is incremented by 1 each time a packet is sent to the same address and uses the same SPI. The sequence number indicates which packet is which, and how many

packets have been sent with the same group of parameters. The sequence number also protects against replay attacks.

Replay attacks involve an attacker who copies a packet and sends it out of sequence to confuse communicating devices. The remaining four parts of the ESP are all encrypted during transmission across the network. Those parts are as

follows:

?The Payload Data is the actual data that is carried by the packet.

?The Padding, from 0 to 255 bytes of data, allows certain types of encryption algorithms to require the data to be a multiple of a certain number of bytes. The padding also ensures that the text of a message terminates on a four-byte boundary

(an architectural requirement within IP).

?The Pad Length field specifies how much of the payload is padding rather than data.

?The Next Header field, like a standard IP Next Header field, identifies the type of data carried and the protocol.

The ESP is added after a standard IP header. Because the packet has a standard IP header, the network can route it with standard IP devices. As a result, IPsec is backwards-compatible with IP routers and other equipment even if that

equipment isn\\'t designed to use IPsec. ESP can support any number of encryption protocols. It\\'s up to the user to decide which ones to use. Different protocols can be used for every person a user communicates with. However, IPsec

specifies a basic DES-Cipher Block Chaining mode (CBC) cipher as the default to ensure minimal interoperability among IPsec networks. ESP\\'s encryption capability is designed for symmetric encryption algorithms. IPsec employs

asymmetric algorithms for such specialized purposes as negotiating keys for symmetric encryption.

Tunneling with ESP

Tunneling takes an original IP packet header and encapsulates it within the ESP. Then, it adds a new IP header containing the address of a gateway device to the packet. Tunneling allows a user to send illegal IP addresses through a public

network (like the Internet) that otherwise would not accept them. Tunneling with ESP offers the advantage of hiding original source and destination addresses from users on the public network. Hiding these addresses reduces the power of

traffic analysis attacks. A traffic analysis attack employs network monitoring techniques to determine how much data and what type of data is being communicated between two users.