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.pass4itsure.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

When AAA login authentication is configured on Cisco routers, which two authentication methods should be used as the final method to ensure that the administrator can still log in to the router in case the external AAA server fails? (Choose two.)

A. group RADIUS

B. group TACACS+

C. local

D. krb5

E. enable

F. if-authenticated

Correct Answer: CE

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scftplus.html

TACACS+ Authentication Examples The following example shows how to configure TACACS+ as the security protocol for PPP authentication: aaa new-model aaa authentication ppp test group tacacs+ local tacacs-server host 10.1.2.3 tacacs-server key goaway interface serial 0 ppp authentication chap pap test The lines in the preceding sample configuration are defined as follows:

•

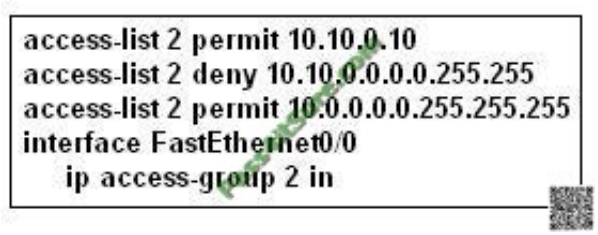
The aaa new-model command enables the AAA security services.

•

The aaa authentication command defines a method list, "test," to be used on serial interfaces running PPP. The keyword group tacacs+ means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword local indicates that authentication will be attempted using the local database on the network access server.
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800946a3.shtml Authentication Start to configure TAC+ on the router. Enter enable mode and type configure terminal before the command set. This command syntax ensures that you are not locked out of the router initially, providing the tac_plus_executable is not running: !--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable

QUESTION 2

Refer to the exhibit.



Which statement about this partial CLI configuration of an access control list is true?

A. The access list accepts all traffic on the 10.0.0.0 subnets.

B. All traffic from the 10.10.0.0 subnets is denied.

C. Only traffic from 10.10.0.10 is allowed.

D. This configuration is invalid. It should be configured as an extended ACL to permit the associated wildcard mask.

E. From the 10.10.0.0 subnet, only traffic sourced from 10.10.0.10 is allowed; traffic sourced from the other 10.0.0.0 subnets also is allowed.

F. The access list permits traffic destined to the 10.10.0.10 host on FastEthernet0/0 from any source.

Correct Answer: E

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-2mt/sec-acl-ov-gdl.html

The Order in Which You Enter Criteria Statements

Note that each additional criteria statement that you enter is appended to the end of the access list statements.

Also note that you cannot delete individual statements after they have been created. You can only delete an entire access list.

The order of access list statements is important! When the router is deciding whether to forward or block a packet, the Cisco IOS software tests the packet against each criteria statement in the order in which the statements were created.

After a match is found, no more criteria statements are checked.

If you create a criteria statement that explicitly permits all traffic, no statements added later will ever be checked. If you need additional statements, you must delete the access list and retype it with the new entries.

Apply an Access Control List to an Interface

With some protocols, you can apply up to two access lists to an interfacE. one inbound access list and one outbound access list. With other protocols, you apply only one access list that checks both inbound and outbound packets.

If the access list is inbound, when a device receives a packet, Cisco software checks the access list\\'s criteria statements for a match. If the packet is permitted, the software continues to process the packet. If the packet is denied, the software

discards the packet.

If the access list is outbound, after receiving and routing a packet to the outbound interface, Cisco software checks the access list\\'s criteria statements for a match. If the packet is permitted, the software transmits the packet. If the packet is

denied, the software discards the packet.

Note

Access lists that are applied to interfaces on a device do not filter traffic that originates from that device. The access list check is bypassed for locally generated packets, which are always outbound. By default, an access list that is applied to

an outbound interface for matching locally generated traffic will bypass the outbound access list check; but transit traffic is subjected to the outbound access list check.

QUESTION 3

Which type of intrusion prevention technology is the primary type used by the Cisco IPS security appliances?

A. profile-based

B. rule-based

C. protocol analysis-based

D. signature-based

E. NetFlow anomaly-based

Correct Answer: D

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_fwids.html

The Signature Definition File A Signature Definition file (SDF) has definitions for each signature it contains. After signatures are loaded and complied onto a router running Cisco IOS IPS, IPS can begin detecting the new signatures immediately. If customers do not use the default, built-in signatures that are shipped with the routers, users can choose to download one of two different types of SDFs: the attack-drop.sdf file (which is a static file) or a dynamic SDF (which is dynamically updated and accessed from Cisco.com). The attack-drop.sdf file is available in flash on all Cisco access routers that are shipped with Cisco IOS Release 12.3(8)T or later. The attack-drop.sdf file can then be loaded directly from flash into the Cisco IOS IPS system. If flash is erased, the attack-drop.sdf file may also be erased. Thus, if you are copying a Cisco IOS image to flash and are prompted to erase the contents of flash before copying the new image, you might risk erasing the attack-drop.sdf file. If this occurs, the router will refer to the built-in signatures within the Cisco IOS image. The attack-drop.sdf file can also be downloaded onto your router from Cisco.com. To help detect the latest vulnerabilities, Cisco provides signature updates on Cisco.com on a regular basis. Users can use SDM or VMS to download these signature updates, tune the signature parameters as necessary, and deploy the new SDF to a Cisco IOS IPS router.

QUESTION 4

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 5

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.