

Final Exam

Number: 640-554
Passing Score: 825
Time Limit: 120 min
File Version: 1.0



<http://www.gratisexam.com/>

Exame Teórico do CCNA Security

Exam A

QUESTION 1

When logging is enabled for an ACL entry, how does the router switch packets filtered by the ACL?

- A. topology-based switching
- B. autonomous switching
- C. process switching
- D. optimum switching

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

Which statement is true about the One-Step lockdown feature of the CCP Security Audit wizard?

- A. It enables the Secure Copy Protocol (SCP).
- B. It supports AAA configuration.
- C. It enables TCP intercepts.
- D. It sets an access class ACL on vty lines.
- E. It provides an option for configuring SNMPv3 on all routers.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

What are three common examples of AAA implementation on Cisco routers? (Choose three.)

- A. authenticating administrator access to the router console port, auxiliary port, and vty ports
- B. authenticating remote users who are accessing the corporate LAN through IPsec VPN connections
- C. implementing public key infrastructure to authenticate and authorize IPsec VPN peers using digital certificates
- D. implementing command authorization with TACACS+
- E. securing the router by locking down all unused services
- F. tracking Cisco Netflow accounting statistics

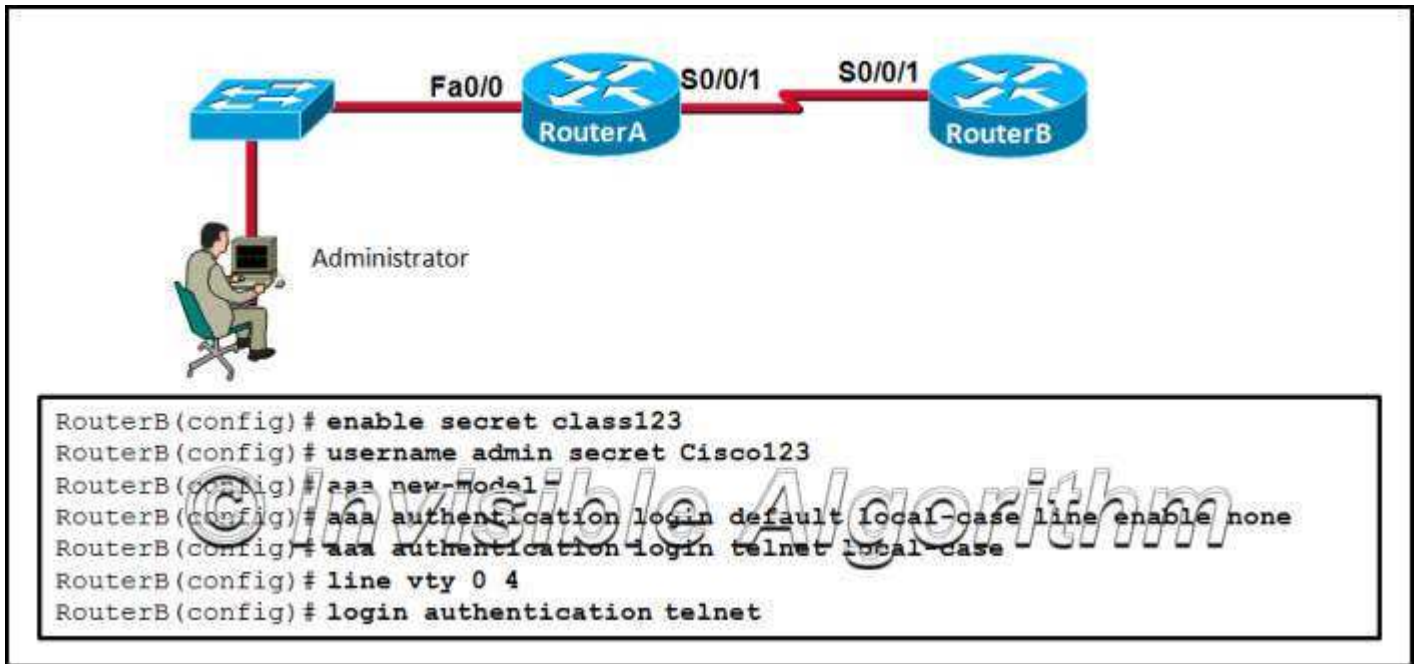
Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4



Refer to the exhibit. The administrator can ping the S0/0/1 interface of RouterB but is unable to gain Telnet access to the router using the password cisco123. What is a possible cause of the problem?

- A. The Telnet connection between RouterA and RouterB is not working correctly.
- B. The password cisco123 is wrong.
- C. The enable password and the Telnet password need to be the same.
- D. The administrator does not have enough rights on the PC that is being used.

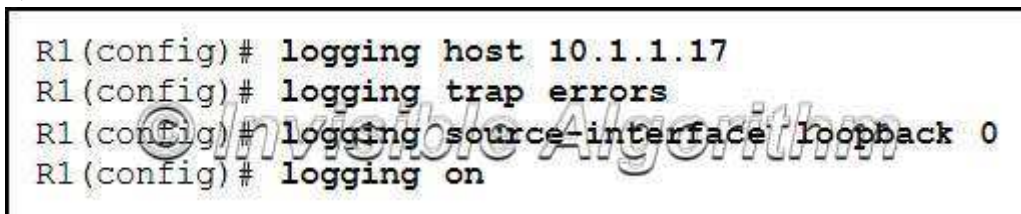
Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5



Refer to the exhibit. An administrator has entered the commands that are shown on router R1. At what trap level is the logging function set?

- A. 2
- B. 3
- C. 5
- D. 6

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

If a switch is configured with the storm-control command and the action shutdown and action trap parameters, which two actions does the switch take when a storm occurs on a port? (Choose two.)

- A. The port is disabled.
- B. The switch is rebooted.
- C. An SNMP log message is sent.
- D. The port is placed in a blocking state.
- E. The switch forwards control traffic only.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:



<http://www.gratisexam.com/>

QUESTION 7

Why does a worm poses a greater threat than a virus poses?

- A. Worms run within a host program.
- B. Worms are not detected by antivirus programs.
- C. Worms directly attack the network devices.
- D. Worms are more network-based than viruses are.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

When port security is enabled on a Cisco Catalyst switch, what is the default action when the maximum number of allowed MAC addresses is exceeded?

- A. The violation mode for the port is set to restrict.
- B. The MAC address table is cleared, and the new MAC address is entered into the table.
- C. The port remains enabled, but the bandwidth is throttled until the old MAC addresses are aged out.
- D. The port is shut down.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

Which type of encryption algorithm uses public and private keys to provide authentication, integrity, and confidentiality?

- A. IPsec
- B. symmetric
- C. asymmetric
- D. shared secret

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

Which three statements describe the IPsec protocol framework? (Choose three.)

- A. AH uses IP protocol 51.
- B. AH provides encryption and integrity.
- C. AH provides integrity and authentication.
- D. ESP uses UDP protocol 50.
- E. ESP requires both authentication and encryption.
- F. ESP provides encryption, authentication, and integrity.

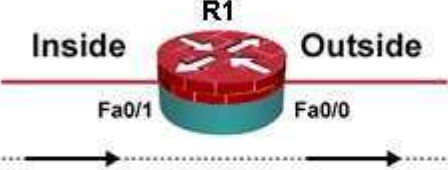
Correct Answer: ACF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11



```
R1# show running-config

<Output omitted>

ip inspect name OUTBOUND tcp
ip inspect name OUTBOUND udp
ip inspect name OUTBOUND icmp
!
ip access-list extended INSIDE
 permit tcp any any
 permit udp any any
 permit icmp any any
```

© Invisible Algorithm

Refer to the exhibit. Which interface configuration completes the CBAC configuration on router R1?

- A. R1(config)# interface fa0/0
R1(config-if)# ip inspect INSIDE in
R1(config-if)# ip access-group OUTBOUND in
- B. R1(config)# interface fa0/1
R1(config-if)# ip inspect INSIDE in
R1(config-if)# ip access-group OUTBOUND in
- C. R1(config)# interface fa0/1
R1(config-if)# ip inspect OUTBOUND in
R1(config-if)# ip access-group INSIDE out
- D. R1(config)# interface fa0/0
R1(config-if)# ip inspect OUTBOUND in
R1(config-if)# ip access-group INSIDE in
- E. R1(config)# interface fa0/1
R1(config-if)# ip inspect OUTBOUND in
R1(config-if)# ip access-group INSIDE in

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Which statement describes the operation of the IKE protocol?

- A. It uses IPsec to establish the key exchange process.
- B. It uses sophisticated hashing algorithms to transmit keys directly across a network.
- C. It calculates shared keys based on the exchange of a series of data packets.
- D. It uses TCP port 50 to exchange IKE information between the security gateways.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

Which two configuration requirements are needed for remote access VPNs using Cisco Easy VPN Server, but are not required for site-to-site VPNs? (Choose two.)

- A. group policy lookup
- B. IPsec translations
- C. virtual template interface
- D. IKE policies
- E. transform sets

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

What can be used as a VPN gateway when setting up a site-to-site VPN?

- A. Cisco Catalyst switch
- B. Cisco router
- C. Cisco Unified Communications Manager
- D. Cisco AnyConnect

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

Which type of Layer 2 attack makes a host appear as the root bridge for a LAN?

- A. LAN storm
- B. MAC address spoofing
- C. MAC address table overflow
- D. STP manipulation
- E. VLAN attack

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16



Refer to the exhibit. An administrator has configured a standard ACL on R1 and applied it to interface serial 0/0/0 in the outbound direction. What happens to traffic leaving interface serial 0/0/0 that does not match the configured ACL statements?

- A. The resulting action is determined by the destination IP address.
- B. The resulting action is determined by the destination IP address and port number.
- C. The source IP address is checked and, if a match is not found, traffic is routed out interface serial 0/0/1.
- D. The traffic is dropped.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

The use of 3DES within the IPsec framework is an example of which of the five IPsec building blocks?

- A. authentication
- B. confidentiality
- C. Diffie-Hellman
- D. integrity
- E. nonrepudiation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

```
S1# show storm-control
Interface  Filter State  Upper      Lower      Current
-----
Fa0/5     Forwarding    80.10%    80.10%    23.00%

S1# show storm-control multicast
Interface  Filter State  Upper      Lower      Current
-----
Fa0/6     Forwarding    2m pps    1m pps    0 pps
```

Refer to the exhibit. Which two statements are correct regarding the configuration on switch S1? (Choose two.)

- A. Port Fa0/5 storm control for broadcasts will be activated if traffic exceeds 80.1 percent of the total bandwidth.
- B. Port Fa0/6 storm control for multicasts and broadcasts will be activated if traffic exceeds 2,000,000 packets per second.
- C. Port Fa0/6 storm control for multicasts will be activated if traffic exceeds 2,000,000 packets per second.
- D. Port Fa0/5 storm control for multicasts will be activated if traffic exceeds 80.1 percent of the total bandwidth.
- E. Port Fa0/5 storm control for broadcasts and multicasts will be activated if traffic exceeds 80.1 percent of 2,000,000 packets per second.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

What is a characteristic of AAA accounting?

- A. Accounting can only be enabled for network connections.

- B. Users are not required to be authenticated before AAA accounting logs their activities on the network.
- C. Possible triggers for the aaa accounting exec default command include start-stop and stop-only.
- D. Accounting is concerned with allowing and disallowing authenticated users access to certain areas and programs on the network.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

A network technician is configuring SNMPv3 and has set a security level of auth. What is the effect of this setting?

- A. authenticates a packet using the SHA algorithm only
- B. authenticates a packet by a string match of the username or community string
- C. authenticates a packet by using either the HMAC with MD5 method or the SHA method
- D. authenticates a packet by using either the HMAC MD5 or HMAC SHA algorithms and encrypts the packet using either the DES, 3DES or AES algorithms

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

Which action best describes a MAC address spoofing attack?

- A. altering the MAC address of an attacking host to match that of a legitimate host
- B. bombarding a switch with fake source MAC addresses
- C. forcing the election of a rogue root bridge
- D. flooding the LAN with excessive traffic

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

When configuring a site-to-site IPsec VPN using the CLI, the authentication pre-share command is configured in the ISAKMP policy. Which additional peer authentication configuration is required?

- A. Configure the message encryption algorithm with the encryptiontype ISAKMP policy configuration command.
- B. Configure the DH group identifier with the groupnumber ISAKMP policy configuration command.
- C. Configure a hostname with the crypto isakmp identity hostname global configuration command.
- D. Configure a PSK with the crypto isakmp key global configuration command.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

Which three statements describe limitations in using privilege levels for assigning command authorization? (Choose three.)

- A. There is no access control to specific interfaces on a router.
- B. The root user must be assigned to each privilege level defined.
- C. Commands set on a higher privilege level are not available for lower privileged users.
- D. Views are required to define the CLI commands that each user can access.
- E. Creating a user account that needs access to most but not all commands can be a tedious process.
- F. It is required that all 16 privilege levels be defined, whether they are used or not.

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

Which set of Cisco IOS commands instructs the IPS to compile a signature category named ios_ips into memory and use it to scan traffic?

- A. R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired false
- B. R1(config)# ip ips signature-category
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
- C. R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# no retired false
- D. R1(config)# ip ips signature-category
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# no retired false

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Refer to the exhibit. Which three things occur if a user attempts to log in four times within 10 seconds using an incorrect password? (Choose three.)

- A. Subsequent virtual login attempts from the user are blocked for 60 seconds.
- B. During the quiet mode, an administrator can virtually log in from any host on network 172.16.1.0/24.
- C. Subsequent console login attempts are blocked for 60 seconds.
- D. A message is generated indicating the username and source IP address of the user.

- E. During the quiet mode, an administrator can log in from host 172.16.1.2.
- F. No user can log in virtually from any host for 60 seconds.

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

Which statement describes configuring ACLs to control Telnet traffic destined to the router itself?

- A. The ACL must be applied to each vty line individually.
- B. The ACL is applied to the Telnet port with the ip access-group command.
- C. Apply the ACL to the vty lines without the in or out option required when applying ACLs to interfaces.
- D. The ACL should be applied to all vty lines in the in direction to prevent an unwanted user from connecting to an unsecured port.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

What are three characteristics of the ASA routed mode? (Choose three.)

- A. This mode does not support VPNs, QoS, or DHCP Relay.
- B. The interfaces of the ASA separate Layer 3 networks and require different IP addresses in different subnets.
- C. It is the traditional firewall deployment mode.
- D. NAT can be implemented between connected networks.
- E. This mode is referred to as a "bump in the wire."
- F. In this mode, the ASA is invisible to an attacker.

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

Which authentication method is available when specifying a method list for group policy lookup using the CCP Easy VPN Server wizard?

- A. Active Directory
- B. Kerberos
- C. Certificate Authority
- D. RADIUS
- E. TACACS+

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

Which access list statement permits HTTP traffic that is sourced from host 10.1.129.100 port 4300 and destined to host 192.168.30.10?

- A. access-list 101 permit tcp any eq 4300
- B. access-list 101 permit tcp 192.168.30.10 0.0.0.0 eq 80 10.1.0.0 0.0.255.255
- C. access-list 101 permit tcp 10.1.129.0 0.0.0.255 eq www 192.168.30.10 0.0.0.0 eq www
- D. access-list 101 permit tcp 10.1.128.0 0.0.1.255 eq 4300 192.168.30.0 0.0.0.15 eq www
- E. access-list 101 permit tcp host 192.168.30.10 eq 80 10.1.0.0 0.0.255.255 eq 4300

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30



Refer to the exhibit. What conclusion can be drawn from the exhibited window when it is displayed on a remote user computer screen?

- A. The user has connected to a secure web server.
- B. The user has established a client-based VPN connection.

- C. The user has logged out of the AnyConnect VPN client.
- D. The user is installing the AnyConnect VPN client.
- E. The user is using a web browser to connect to a clientless SSL VPN.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31

What will be disabled as a result of the no service password-recovery command?

- A. aaa new-model global configuration command
- B. changes to the configuration register
- C. password encryption service
- D. ability to access ROMmon

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32

Which type of IPS signature detection is used to distract and confuse attackers?

- A. pattern-based detection
- B. anomaly-based detection
- C. policy-based detection
- D. honey pot-based detection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33

```
R1# config t
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# ip ips notify log
R1(config)# ip sdee events 500
R1(config)#
```

Refer to the exhibit. An administrator has configured router R1 as indicated. However, SDEE messages fail to log. Which solution corrects this problem?

- A. Issue the logging on command in global configuration.
- B. Issue the ip ips notify sdee command in global configuration.
- C. Issue the ip audit notify log command in global configuration.
- D. Issue the clear ip ips sdee events command to clear the SDEE buffer.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

Which attack allows the attacker to see all frames on a broadcast network by causing a switch to flood all incoming traffic?

- A. LAN storm
- B. VLAN hopping
- C. STP manipulation
- D. MAC table overflow
- E. 802.1q double tagging

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35



Refer to the exhibit. The indicated window has appeared in the web browser of a remote user. What is the cause of this message?

- A. The user has timed out of an AnyConnect SSL VPN installation.
- B. The user has logged out of a clientless SSL VPN session.
- C. The user has logged out of a Cisco VPN Client session.
- D. The user has logged out of an AnyConnect IPsec VPN session.
- E. The user has logged out of an AnyConnect SSL VPN session.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

An administrator has been asked to configure basic access security on a router, including creating secure passwords and disabling unattended connections. Which three actions accomplish this using recommended security practices? (Choose three.)

- A. Create passwords with only alphanumeric characters.
- B. Set the minimum password length to 10 characters.
- C. Set the executive timeout parameters on the console port to 120 and 0.
- D. Set the executive timeout parameters on the vty lines to 3 and 0.
- E. Enable the password encryption service for the router.
- F. Enable login using the Aux port with the executive timeout set to 0 and 0.

Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

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

- A. rule-based
- B. profile-based
- C. signature-based
- D. NetFlow anomaly-based
- E. protocol analysis-based

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

Which type of packets exiting the network of an organization should be blocked by an ACL?

- A. packets that are not encrypted
- B. packets that are not translated with NAT
- C. packets with source IP addresses outside of the organization's network address space
- D. packets with destination IP addresses outside of the organization's network address space

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

An administrator wants to prevent a rogue Layer 2 device from intercepting traffic from multiple VLANs on a network. Which two actions help mitigate this type of activity? (Choose two.)

- A. Disable DTP on ports that require trunking.
- B. Place unused active ports in an unused VLAN.
- C. Secure the native VLAN, VLAN 1, with encryption.
- D. Set the native VLAN on the trunk ports to an unused VLAN.
- E. Turn off trunking on all trunk ports and manually configure each VLAN as required on each port.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:



<http://www.gratisexam.com/>

QUESTION 40

Which command would an administrator use to clear generated crypto keys?

- A. Router(config)# crypto key decrypt
- B. Router(config-line)# transport input ssh clear
- C. Router(config)# crypto key rsa
- D. Router(config)# crypto key zeroize rsa

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

What occurs after RSA keys are generated on a Cisco router to prepare for secure device management?

- A. All vty ports are automatically configured for SSH to provide secure management.
- B. The general-purpose key size must be specified for authentication with the crypto key generate rsa general-keys moduluscommand.
- C. The keys must be zeroized to reset secure shell before configuring other parameters.
- D. The generated keys can be used by SSH.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42


```

CCNAS-ASA (config)# interface vlan 1
CCNAS-ASA (config-if) # nameif inside
INFO: Security level for "inside" set to 100 by default.
CCNAS-ASA (config-if) # security-level 100
CCNAS-ASA (config-if) # ip address 192.168.1.1 255.255.255.0
CCNAS-ASA (config-if) # no shut
CCNAS-ASA (config-if) # interface e0/1
CCNAS-ASA (config-if) # switchport access vlan 1
CCNAS-ASA (config-if) # exit
CCNAS-ASA (config)# interface vlan 2
CCNAS-ASA (config-if) # nameif outside
INFO: Security level for "outside" set to 0 by default.
CCNAS-ASA (config-if) # security-level 0
CCNAS-ASA (config-if) # no shut
CCNAS-ASA (config-if) # ip address 209.165.200.226 255.255.255.248
CCNAS-ASA (config-if) # interface e0/0
CCNAS-ASA (config-if) # switchport access vlan 2
CCNAS-ASA (config-if) # exit
CCNAS-ASA (config)#

```

Refer to the exhibit. An administrator has configured an ASA 5505 as indicated but is still unable to ping the inside interface from an inside host. What is the cause of this problem?

- A. An IP address should be configured on the Ethernet 0/0 and 0/1 interfaces.
- B. The no shutdown command should be entered on interface Ethernet 0/1.
- C. The security level of the inside interface should be 0 and the outside interface should be 100.
- D. VLAN 1 should be assigned to interface Ethernet 0/0 and VLAN 2 to Ethernet 0/1.
- E. VLAN 1 should be the outside interface and VLAN 2 should be the inside interface.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

```

Nov 30 11:00:24 EST: %SYS-5-CONFIG-I: Configured from console by vty0 (10.64.2.2)

```

Refer to the exhibit. An administrator is examining the message in a syslog server. What can be determined from the message?

- A. This is a notification message for a normal but significant condition.
- B. This is an alert message for which immediate action is needed.
- C. This is an error message for which warning conditions exist.
- D. This is an error message indicating the system is unusable.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

What is a result of securing the Cisco IOS image using the Cisco IOS Resilient Configuration feature?

- A. The Cisco IOS image file is not visible in the output of the show flash command.
- B. The Cisco IOS image is encrypted and then automatically backed up to a TFTP server.
- C. The Cisco IOS image is encrypted and then automatically backed up to the NVRAM.
- D. When the router boots up, the Cisco IOS image is loaded from a secured FTP location.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

Which two commands are needed on every IPv6 ACL to allow IPv6 neighbor discovery? (Choose two.)

- A. permit tcp any any ack
- B. permit icmp any any nd-na
- C. permit icmp any any echo-reply
- D. permit icmp any any nd-ns
- E. permit ipv6 any any fragments
- F. permit ipv6 any any routing

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

Which technology does CCP require for configuring remote access VPN support with the Easy VPN Server wizard?

- A. AutoSecure
- B. Role-Based CLI Access
- C. AAA
- D. port forwarding

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

What are three goals of a port scan attack? (Choose three.)

- A. disable used ports and services
- B. determine potential vulnerabilities
- C. identify active services

- D. identify peripheral configurations
- E. identify operating systems
- F. discover system passwords

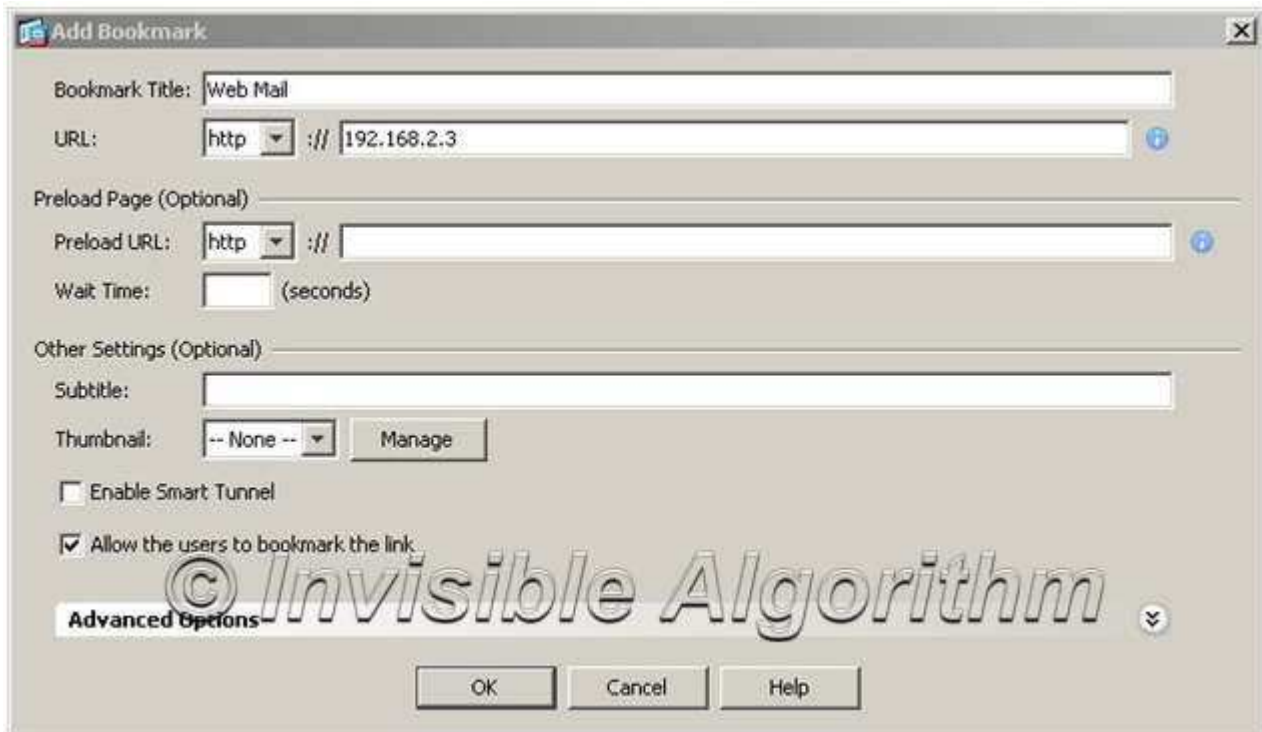
Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48



Refer to the exhibit. An administrator is implementing VPN support on an ASA 5505. What type of VPN support is being implemented?

- A. client-based IPsec VPN using Cisco VPN Client
- B. client-based IPsec VPN using AnyConnect
- C. client-based SSL VPN using AnyConnect
- D. clientless IPsec VPN
- E. clientless SSL VPN
- F. site-to-site IPsec VPN

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

Which type of VPN may require the Cisco VPN Client software?

- A. remote access VPN
- B. SSL VPN
- C. site-to-site VPN
- D. MPLS VPN

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

Sales representatives of an organization use computers in hotel business centers to occasionally access corporate e-mail and the inventory database. What would be the best VPN solution to implement on an ASA to support these users?

- A. client-based IPsec VPN using Cisco VPN Client
- B. client-based IPsec VPN using AnyConnect
- C. client-based SSL VPN using AnyConnect
- D. clientless IPsec VPN using a web browser
- E. clientless SSL VPN using a web browser
- F. site-to-site IPsec VPN

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

```
Router(config)# username ADMIN privilege level 15 secret T0ughPa55w0rd
Router(config)# aaa new-model
Router(config)# aaa authentication login default tacacs+
Router(config)# aaa authentication login ACCESS tacacs+ local
Router(config)# line vty 0 4
Router(config-line)# login authentication ACCESS
Router(config-line)# line con 0
Router(config-line)# end
```

Refer to the exhibit. What information can be obtained from the AAA configuration statements?

- A. The authentication method list used for Telnet is named ACCESS.
- B. The authentication method list used by the console port is named ACCESS.
- C. The local database is checked first when authenticating console and Telnet access to the router.
- D. If the TACACS+ AAA server is not available, no users can establish a Telnet session with the router.
- E. If the TACACS+ AAA server is not available, console access to the router can be authenticated using the local database.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

What must be configured before any Role-Based CLI views can be created?

- A. aaa new-model command
- B. multiple privilege levels
- C. secret password for the root user
- D. usernames and passwords

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

```
R1# show secure bootset
IOS resilience router id FTX1111WQQF

IOS image resilience version 12.4 activated at 11:07:05 UTC Fri
Apr 17 2009
Secure archive flash:c1841-advipservicesk9-mz.124-20.T1.bin
type is image (elf)
[]
file size is 37081324 bytes, run size is 37247008 bytes
Runnable image, entry point 0x8000F000, run from ram

IOS configuration resilience version 12.4 activated at 11:07:26
UTC Fri Apr 17 2009
Secure archive flash:.runcfg-20090417-110725.ar type is config
configuration archive size 1429 bytes
```

Refer to the exhibit. Based on the output from the show secure bootset command on router R1, which three conclusions can be drawn regarding Cisco IOS Resilience? (Choose three.)

- A. A copy of the Cisco IOS image file has been made.
- B. A copy of the router configuration file has been made.
- C. The Cisco IOS image file is hidden and cannot be copied, modified, or deleted.
- D. The Cisco IOS image filename will be listed when the show flash command is issued on R1.
- E. The copy tftp flash command was issued on R1.
- F. The secure boot-config command was issued on R1.

Correct Answer: BCF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

What are two disadvantages of using network IPS? (Choose two.)

- A. Network IPS has a difficult time reconstructing fragmented traffic to determine if an attack was successful.
- B. Network IPS is incapable of examining encrypted traffic.
- C. Network IPS is operating system-dependent and must be customized for each platform.
- D. Network IPS is unable to provide a clear indication of the extent to which the network is being attacked.
- E. Network IPS sensors are difficult to deploy when new networks are added.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

Which statement describes the CCP Security Audit wizard?

- A. After the wizard identifies the vulnerabilities, the CCP One-Step Lockdown feature must be used to make all security-related configuration changes.
- B. After the wizard identifies the vulnerabilities, it automatically makes all security-related configuration changes.
- C. The wizard autosenses the inside trusted and outside untrusted interfaces to determine possible security problems that might exist.
- D. The wizard is based on the Cisco IOS AutoSecure feature.
- E. The wizard is enabled by using the Intrusion Prevention task.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

Which three statements describe zone-based policy firewall rules that govern interface behavior and the traffic moving between zone member interfaces? (Choose three.)

- A. An interface can be assigned to multiple security zones.
- B. Interfaces can be assigned to a zone before the zone is created.
- C. Pass, inspect, and drop options can only be applied between two zones.
- D. If traffic is to flow between all interfaces in a router, each interface must be a member of a zone.
- E. Traffic is implicitly prevented from flowing by default among interfaces that are members of the same zone.
- F. To permit traffic to and from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone.

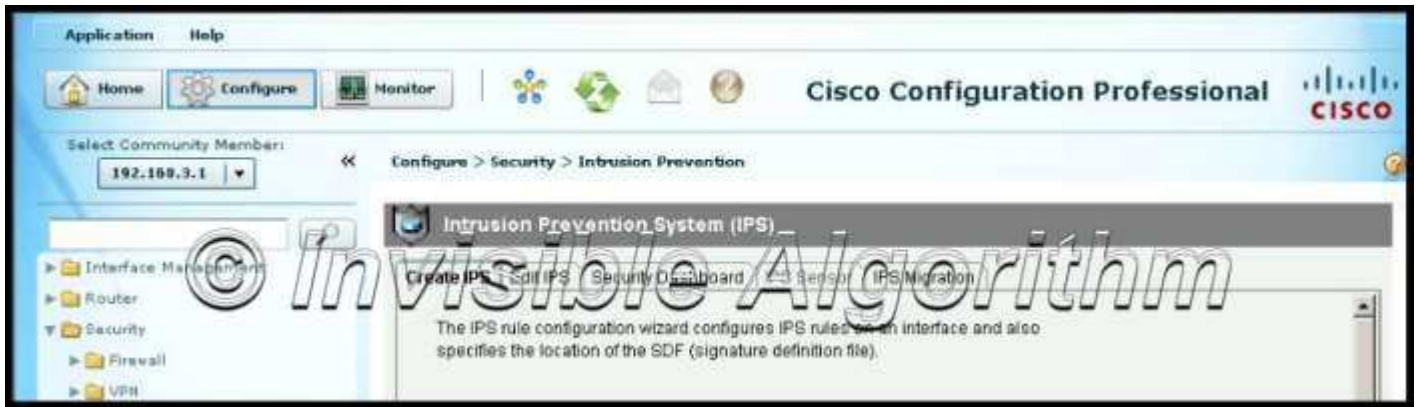
Correct Answer: CDF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57



Refer to the exhibit. Which option tab on the CCP screen is used to view the Top Threats table and deploy signatures associated with those threats?

- A. Create IPS
- B. Edit IPS
- C. Security Dashboard
- D. IPS Sensor
- E. IPS Migration

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 58

Which statement correctly describes a type of filtering firewall?

- A. A transparent firewall is typically implemented on a PC or server with firewall software running on it.
- B. A packet-filtering firewall expands the number of IP addresses available and hides network addressing design.
- C. An application gateway firewall (proxy firewall) is typically implemented on a router to filter Layer 3 and Layer 4 information.
- D. A stateful firewall monitors the state of connections, whether the connection is in an initiation, data transfer, or termination state.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59

Which component of AAA is used to determine which resources a user can access and which operations the user is allowed to perform?

- A. auditing
- B. accounting
- C. authorization

D. authentication

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

Which three statements should be considered when applying ACLs to a Cisco router? (Choose three.)

- A. Place generic ACL entries at the top of the ACL.
- B. Place more specific ACL entries at the top of the ACL.
- C. Router-generated packets pass through ACLs on the router without filtering.
- D. ACLs always search for the most specific entry before taking any filtering action.
- E. A maximum of three IP access lists can be assigned to an interface per direction (in or out).
- F. An access list applied to any interface without a configured ACL allows all traffic to pass.

Correct Answer: BCF

Section: (none)

Explanation

Explanation/Reference:



<http://www.gratisexam.com/>