

## Implementing Cisco IOS Network Security (IINS v2.0)

Number: 640-554  
Passing Score: 800  
Time Limit: 120 min  
File Version: 1.0



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



**Frankly Sudan**

**Vendor: Cisco**

**Exam Code: 640-554**

**Exam Name: Implementing Cisco IOS Network Security (IINS v2.0)**

**Version: 1.0**

### **Sections**

1. Drag and Drop
2. Security Fundamentals
3. Access list Questions
4. LabSim
5. Modern Network Security Threats
6. Securing Network Devices
7. Authentication Authorization & Accounting
8. Implementing Firewall Technologies
9. IPsec Questions

10. Cisco Configuration Professional CCP
11. Implementing Intrusion Prevention
12. Securing Local Area Networks
13. Storage Area Network SAN
14. Cryptographic Systems
15. Implementing Virtual Private Networks
16. Managing a Secure Network

## Exam A

### QUESTION 1

Which statement describes a best practice when configuring trunking on a switch port?

- A. Disable double tagging by enabling DTP on the trunk port.
- B. Enable encryption on the trunk port.
- C. Enable authentication and encryption on the trunk port.
- D. Limit the allowed VLAN(s) on the trunk to the native VLAN only.
- E. Configure an unused VLAN as the native VLAN.

**Correct Answer:** E

**Section:** (none)

**Explanation**

### QUESTION 2

Which type of Layer 2 attack causes a switch to flood all incoming traffic to all ports?

- A. MAC spoofing attack
- B. CAM overflow attack
- C. VLAN hopping attack
- D. STP attack

**Correct Answer:** B

**Section:** (none)

**Explanation**

### QUESTION 3

What is the best way to prevent a VLAN hopping attack?

- A. Encapsulate trunk ports with IEEE 802.1Q.
- B. Physically secure data closets.
- C. Disable DTP negotiations.
- D. Enable BPDU guard.

**Correct Answer:** C

**Section:** (none)

**Explanation**

### QUESTION 4

Which statement about PVLAN Edge is true?

- A. PVLAN Edge can be configured to restrict the number of MAC addresses that appear on a single port.
- B. The switch does not forward any traffic from one protected port to any other protected port.
- C. By default, when a port policy error occurs, the switchport shuts down.
- D. The switch only forwards traffic to ports within the same VLAN Edge.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



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

#### QUESTION 5

If you are implementing VLAN trunking, which additional configuration parameter should be added to the trunking configuration?

- A. no switchport mode access
- B. no switchport trunk native VLAN 1
- C. switchport mode DTP
- D. switchport nonnegotiate

**Correct Answer:** D

**Section:** (none)

**Explanation**

#### QUESTION 6

When Cisco IOS zone-based policy firewall is configured, which three actions can be applied to a traffic class? (Choose three.)

- A. pass
- B. police
- C. inspect
- D. drop
- E. queue
- F. shape

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

#### QUESTION 7

With Cisco IOS zone-based policy firewall, by default, which three types of traffic are permitted by the router when some of the router interfaces are assigned to a zone? (Choose three.)

- A. traffic flowing between a zone member interface and any interface that is not a zone member
- B. traffic flowing to and from the router interfaces (the self zone)
- C. traffic flowing among the interfaces that are members of the same zone
- D. traffic flowing among the interfaces that are not assigned to any zone
- E. traffic flowing between a zone member interface and another interface that belongs in a different zone
- F. traffic flowing to the zone member interface that is returned traffic

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**QUESTION 8**

Which option is a key difference between Cisco IOS interface ACL configurations and Cisco ASA appliance interface ACL configurations?

- A. The Cisco IOS interface ACL has an implicit permit-all rule at the end of each interface ACL.
- B. Cisco IOS supports interface ACL and also global ACL. Global ACL is applied to all interfaces.
- C. The Cisco ASA appliance interface ACL configurations use netmasks instead of wildcard masks.
- D. The Cisco ASA appliance interface ACL also applies to traffic directed to the IP addresses of the Cisco ASA appliance interfaces.
- E. The Cisco ASA appliance does not support standard ACL. The Cisco ASA appliance only support extended ACL.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**QUESTION 9**

Which two options are advantages of an application layer firewall? (Choose two.)

- A. provides high-performance filtering
- B. makes DoS attacks difficult
- C. supports a large number of applications
- D. authenticates devices
- E. authenticates individuals

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**QUESTION 10**

On Cisco ISR routers, for what purpose is the realm-cisco.pub public encryption key used?

- A. used for SSH server/client authentication and encryption
- B. used to verify the digital signature of the IPS signature file
- C. used to generate a persistent self-signed identity certificate for the ISR so administrators can authenticate the ISR when accessing it using Cisco Configuration Professional
- D. used to enable asymmetric encryption on IPsec and SSL VPNs
- E. used during the DH exchanges on IPsec VPNs

**Correct Answer:** B

**Section:** (none)

**Explanation**

**QUESTION 11**

Which four tasks are required when you configure Cisco IOS IPS using the Cisco Configuration Professional IPS wizard? (Choose four.)

- A. Select the interface(s) to apply the IPS rule.
- B. Select the traffic flow direction that should be applied by the IPS rule.
- C. Add or remove IPS alerts actions based on the risk rating.
- D. Specify the signature file and the Cisco public key.

- E. Select the IPS bypass mode (fail-open or fail-close).
- F. Specify the configuration location and select the category of signatures to be applied to the selected interface(s).

**Correct Answer:** ABDF

**Section:** (none)

**Explanation**

#### **QUESTION 12**

Which statement is a benefit of using Cisco IOS IPS?

- A. It uses the underlying routing infrastructure to provide an additional layer of security.
- B. It works in passive mode so as not to impact traffic flow.
- C. It supports the complete signature database as a Cisco IPS sensor appliance.
- D. The signature database is tied closely with the Cisco IOS image.

**Correct Answer:** A

**Section:** (none)

**Explanation**

#### **QUESTION 13**

Which description of the Diffie-Hellman protocol is true?

- A. It uses symmetrical encryption to provide data confidentiality over an unsecured communications channel.
- B. It uses asymmetrical encryption to provide authentication over an unsecured communications channel.
- C. It is used within the IKE Phase 1 exchange to provide peer authentication.
- D. It provides a way for two peers to establish a shared-secret key, which only they will know, even though they are communicating over an unsecured channel.
- E. It is a data integrity algorithm that is used within the IKE exchanges to guarantee the integrity of the message of the IKE exchanges.

**Correct Answer:** D

**Section:** (none)

**Explanation**

#### **QUESTION 14**

Which IPsec transform set provides the strongest protection?

- A. crypto ipsec transform-set 1 esp-3des esp-sha-hmac
- B. crypto ipsec transform-set 2 esp-3des esp-md5-hmac
- C. crypto ipsec transform-set 3 esp-aes 256 esp-sha-hmac
- D. crypto ipsec transform-set 4 esp-aes esp-md5-hmac
- E. crypto ipsec transform-set 5 esp-des esp-sha-hmac
- F. crypto ipsec transform-set 6 esp-des esp-md5-hmac

**Correct Answer:** C

**Section:** (none)

**Explanation**

#### **QUESTION 15**

Which two options are characteristics of the Cisco Configuration Professional Security Audit wizard? (Choose

two.)

- A. displays a screen with fix-it check boxes to let you choose which potential security-related configuration changes to implement
- B. has two modes of operation: interactive and non-interactive
- C. automatically enables Cisco IOS firewall and Cisco IOS IPS to secure the router
- D. uses interactive dialogs and prompts to implement role-based CLI
- E. requires users to first identify which router interfaces connect to the inside network and which connect to the outside network

**Correct Answer:** AE

**Section:** (none)

**Explanation**

#### **QUESTION 16**

Which statement describes a result of securing the Cisco IOS image using the Cisco IOS image resilience feature?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### **QUESTION 17**

Which aaa accounting command is used to enable logging of the start and stop records for user terminal sessions on the router?

- A. aaa accounting network start-stop tacacs+
- B. aaa accounting system start-stop tacacs+
- C. aaa accounting exec start-stop tacacs+
- D. aaa accounting connection start-stop tacacs+
- E. aaa accounting commands 15 start-stop tacacs+

**Correct Answer:** C

**Section:** (none)

**Explanation**

#### **QUESTION 18**

Which access list permits HTTP traffic sourced from host 10.1.129.100 port 3030 destined to host 192.168.1.10?

- A. access-list 101 permit tcp any eq 3030
- B. access-list 101 permit tcp 10.1.128.0 0.0.1.255 eq 3030 192.168.1.0 0.0.0.15 eq www
- C. access-list 101 permit tcp 10.1.129.0 0.0.0.255 eq www 192.168.1.10 0.0.0.0 eq www
- D. access-list 101 permit tcp host 192.168.1.10 eq 80 10.1.0.0 0.0.255.255 eq 3030
- E. access-list 101 permit tcp 192.168.1.10 0.0.0.0 eq 80 10.1.0.0 0.0.255.255

F. access-list 101 permit ip host 10.1.129.100 eq 3030 host 192.168.1.100 eq 80

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### **QUESTION 19**

Which location is recommended for extended or extended named ACLs?

- A. an intermediate location to filter as much traffic as possible
- B. a location as close to the destination traffic as possible
- C. when using the established keyword, a location close to the destination point to ensure that return traffic is allowed
- D. a location as close to the source traffic as possible

**Correct Answer:** D

**Section:** (none)

**Explanation**

#### **QUESTION 20**

Which statement about asymmetric encryption algorithms is true?

- A. They use the same key for encryption and decryption of data.
- B. They use the same key for decryption but different keys for encryption of data.
- C. They use different keys for encryption and decryption of data.
- D. They use different keys for decryption but the same key for encryption of data.

**Correct Answer:** C

**Section:** (none)

**Explanation**

#### **QUESTION 21**

Which option can be used to authenticate the IPsec peers during IKE Phase 1?

- A. Diffie-Hellman Nonce
- B. pre-shared key
- C. XAUTH
- D. integrity check value
- E. ACS
- F. AH

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### **QUESTION 22**

Which single Cisco IOS ACL entry permits IP addresses from 172.16.80.0 to 172.16.87.255?

- A. permit 172.16.80.0 0.0.3.255
- B. permit 172.16.80.0 0.0.7.255



- C. permit 172.16.80.0 0.0.248.255
- D. permit 176.16.80.0 255.255.252.0
- E. permit 172.16.80.0 255.255.248.0
- F. permit 172.16.80.0 255.255.240.0

**Correct Answer:** B

**Section:** (none)

**Explanation**

### QUESTION 23

You want to use the Cisco Configuration Professional site-to-site VPN wizard to implement a site- to-site IPsec VPN using pre-shared key.

Which four configurations are required (with no defaults)? (Choose four.)

- A. the interface for the VPN connection
- B. the VPN peer IP address
- C. the IPsec transform-set
- D. the IKE policy
- E. the interesting traffic (the traffic to be protected)
- F. the pre-shared key

**Correct Answer:** ABEF

**Section:** (none)

**Explanation**

### QUESTION 24

Which two options represent a threat to the physical installation of an enterprise network? (Choose two.)

- A. surveillance camera
- B. security guards
- C. electrical power
- D. computer room access
- E. change control

**Correct Answer:** CD

**Section:** (none)

**Explanation**

### QUESTION 25

Which option represents a step that should be taken when a security policy is developed?

- A. Perform penetration testing.
- B. Determine device risk scores.
- C. Implement a security monitoring system.
- D. Perform quantitative risk analysis.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**QUESTION 26**

Which type of network masking is used when Cisco IOS access control lists are configured?

- A. extended subnet masking
- B. standard subnet masking
- C. priority masking
- D. wildcard masking

**Correct Answer:** D

**Section:** (none)

**Explanation**

**QUESTION 27**

How are Cisco IOS access control lists processed?

- A. Standard ACLs are processed first.
- B. The best match ACL is matched first.
- C. Permit ACL entries are matched first before the deny ACL entries.
- D. ACLs are matched from top down.
- E. The global ACL is matched first before the interface ACL.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**QUESTION 28**

Which type of management reporting is defined by separating management traffic from production traffic?

- A. IPsec encrypted
- B. in-band
- C. out-of-band
- D. SSH

**Correct Answer:** C

**Section:** (none)

**Explanation**

**QUESTION 29**

Which syslog level is associated with LOG\_WARNING?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5
- F. 6

**Correct Answer:** D

**Section:** (none)

**Explanation**

**QUESTION 30**

In which type of Layer 2 attack does an attacker broadcast BDPUs with a lower switch priority?

- A. MAC spoofing attack
- B. CAM overflow attack
- C. VLAN hopping attack
- D. STP attack

**Correct Answer: D**

**Section: (none)**

**Explanation**

**QUESTION 31**

Which security measure must you take for native VLANs on a trunk port?

- A. Native VLANs for trunk ports should never be used anywhere else on the switch.
- B. The native VLAN for trunk ports should be VLAN 1.
- C. Native VLANs for trunk ports should match access VLANs to ensure that cross-VLAN traffic from multiple switches can be delivered to physically disparate switches.
- D. Native VLANs for trunk ports should be tagged with 802.1Q.

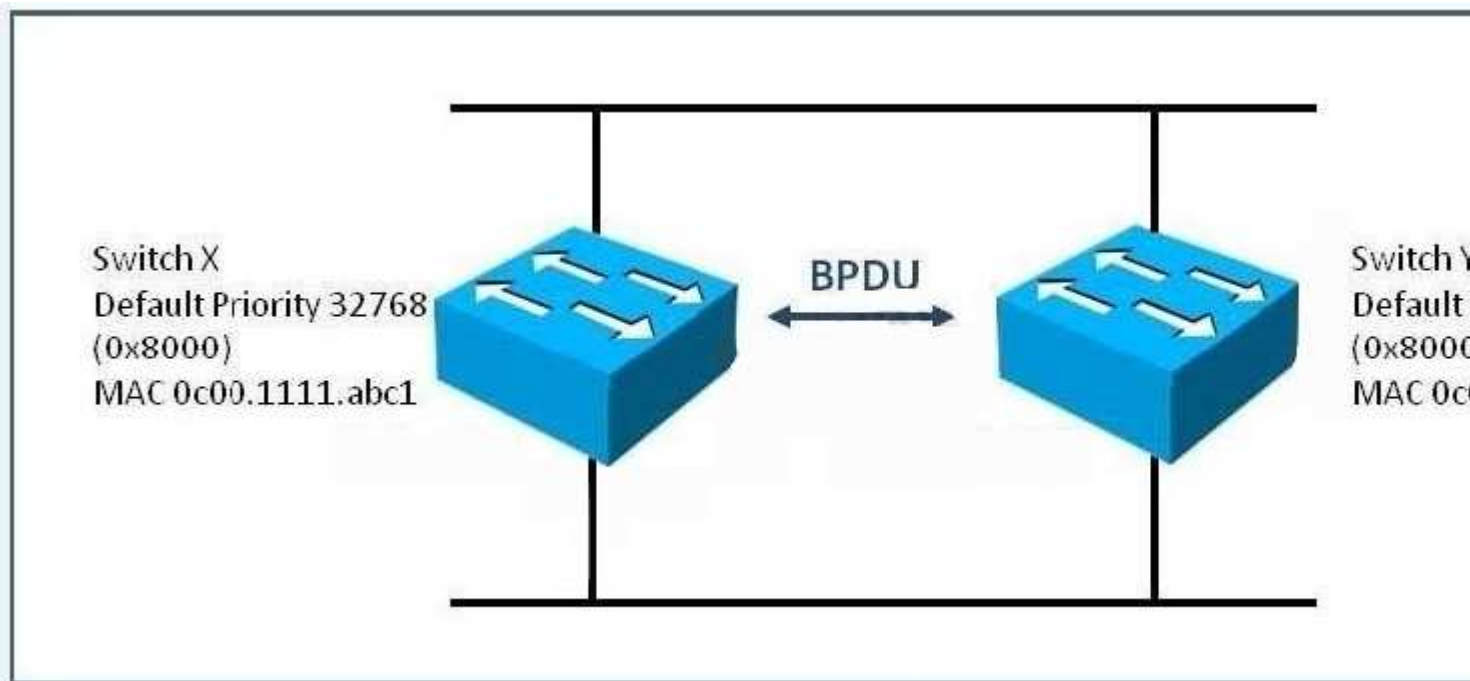
**Correct Answer: A**

**Section: (none)**

**Explanation**

**QUESTION 32**

Refer to the exhibit. Which switch is designated as the root bridge in this topology?



- A. It depends on which switch came on line first.

- B. Neither switch would assume the role of root bridge because they have the same default priority.
- C. switch X
- D. switch Y

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 33**

Which type of firewall technology is considered the versatile and commonly used firewall technology?

- A. static packet filter firewall
- B. application layer firewall
- C. stateful packet filter firewall
- D. proxy firewall
- E. adaptive layer firewall

**Correct Answer:** C

**Section:** (none)

**Explanation**

### **QUESTION 34**

Which type of NAT is used where you translate multiple internal IP addresses to a single global, routable IP address?

- A. policy NAT
- B. dynamic PAT
- C. static NAT
- D. dynamic NAT
- E. policy PAT

**Correct Answer:** B

**Section:** (none)

**Explanation**

### **QUESTION 35**

Which Cisco IPS product offers an inline, deep-packet inspection feature that is available in integrated services routers?

- A. Cisco iSDM
- B. Cisco AIM
- C. Cisco IOS IPS
- D. Cisco AIP-SSM

**Correct Answer:** C

**Section:** (none)

**Explanation**

### **QUESTION 36**

Which three modes of access can be delivered by SSL VPN? (Choose three.)

- A. full tunnel client
- B. IPsec SSL
- C. TLS transport mode
- D. thin client
- E. clientless
- F. TLS tunnel mode

**Correct Answer:** ADE

**Section:** (none)

**Explanation**

#### **QUESTION 37**

During role-based CLI configuration, what must be enabled before any user views can be created?

- A. multiple privilege levels
- B. usernames and passwords
- C. aaa new-model command
- D. secret password for the root user
- E. HTTP and/or HTTPS server
- F. TACACS server group

**Correct Answer:** C

**Section:** (none)

**Explanation**

#### **QUESTION 38**

Which three statements about applying access control lists to a Cisco router are true? (Choose three.)

- A. Place more specific ACL entries at the top of the ACL.
- B. Place generic ACL entries at the top of the ACL to filter general traffic and thereby reduce "noise" on the network.
- C. ACLs always search for the most specific entry before taking any filtering action.
- D. Router-generated packets cannot be filtered by ACLs on the router.
- E. If an access list is applied but it is not configured, all traffic passes.

**Correct Answer:** ADE

**Section:** (none)

**Explanation**

#### **QUESTION 39**

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

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

**Correct Answer:** B

**Section: (none)**  
**Explanation**

**QUESTION 40**

Which three statements about the Cisco ASA appliance are true? (Choose three.)

- A. The DMZ interface(s) on the Cisco ASA appliance most typically use a security level between 1 and 99.
- B. The Cisco ASA appliance supports Active/Active or Active/Standby failover.
- C. The Cisco ASA appliance has no default MPF configurations.
- D. The Cisco ASA appliance uses security contexts to virtually partition the ASA into multiple virtual firewalls.
- E. The Cisco ASA appliance supports user-based access control using 802.1x.
- F. An SSM is required on the Cisco ASA appliance to support Botnet Traffic Filtering.

**Correct Answer:** ABD

**Section: (none)**

**Explanation**

**QUESTION 41**

Refer to the exhibit. This Cisco IOS access list has been configured on the FA0/0 interface in the inbound direction.

Which four TCP packets sourced from 10.1.1.1 port 1030 and routed to the FA0/0 interface are permitted? (Choose four.)

```
access-list 102 permit tcp any 192.168.15.32 0.0.0.31 eq www
access-list 102 deny ip any 192.168.15.32 0.0.0.31
access-list 102 permit ip any any
```

```
Current configuration : 156 bytes
!
interface FastEthernet0
 ip address 192.168.32.13 255.255.255.0
 ip access-group IOS in
 ip flow ingress
 ip flow egress
 duplex auto
 speed auto
!
end

Router(config-ext-nacl)#do show access-1 IOS
Extended IP access list IOS
 10 permit tcp host 10.1.1.1 eq 1030 host 192.168.15.80 eq telnet
 20 permit tcp host 10.1.1.1 eq 1030 host 192.168.15.66 eq 8080
 30 permit tcp host 10.1.1.1 eq 1030 host 192.168.15.36 eq www
 40 permit tcp host 10.1.1.1 eq 1030 host 192.168.15.63 eq www
Router(config-ext-nacl)#
```

- A. destination ip address: 192.168.15.37 destination port: 22
- B. destination ip address: 192.168.15.80 destination port: 23
- C. destination ip address: 192.168.15.66 destination port: 8080

- D. destination ip address: 192.168.15.36 destination port: 80
- E. destination ip address: 192.168.15.63 destination port: 80
- F. destination ip address: 192.168.15.40 destination port: 21

**Correct Answer:** BCDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 42**

You use Cisco Configuration Professional to enable Cisco IOS IPS. Which state must a signature be in before any actions can be taken when an attack matches that signature?

- A. enabled
- B. unretired
- C. successfully complied
- D. successfully complied and unretired
- E. successfully complied and enabled
- F. unretired and enabled
- G. enabled, unretired, and successfully complied

**Correct Answer:** G

**Section:** (none)

**Explanation**

#### **QUESTION 43**

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:** B

**Section:** (none)

**Explanation**

#### **QUESTION 44**

Refer to the exhibit. Which three statements about these three show outputs are true? (Choose three.)

```

router#show crypto isakmp policy
Protection suite of priority 1
  encryption algorithm: 3DES -Data encryption Standard (168 bit keys)
  hash algorithm: Secure Hash Standard
  authentication method: preshared Key
  Diffie-Hellman Group: #2 (1024 bit)
  lifetime: 86400 seconds, no volume limit
Protection suite priority 2
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm: Secure Hash Standard
  authentication method: preshared Key
  Diffie-Hellman Group: #2 (1024 bit)
  lifetime: 86400 seconds, no volume limit
Default protection suite
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm: Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group: #1 (768 bit)
  lifetime: 86400 seconds, no volume limit

Router#show crypto ipsec transform-set
transform set mine; { esp-128-aes esp-sha-hmac } will negotiate = { Tunnel, }

Router#show crypto map
Crypto Map "mymap" 10 ipsec-isakmp
  Peer = 172.16.1.2
  Extended IP access list 110
  access-list 110 permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255
  Current peer: 17.16.1.2
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets=mine, }

```

- A. Traffic matched by ACL 110 is encrypted.
- B. The IPsec transform set uses SHA for data confidentiality.
- C. The crypto map shown is for an IPsec site-to-site VPN tunnel.
- D. The default ISAKMP policy uses a digital certificate to authenticate the IPsec peer.
- E. The IPsec transform set specifies the use of GRE over IPsec tunnel mode.
- F. The default ISAKMP policy has higher priority than the other two ISAKMP policies with a priority of 1 and 2

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 45

Which type of security control is defense in depth?

- A. threat mitigation
- B. risk analysis
- C. botnet mitigation



D. overt and covert channels

**Correct Answer:** A

**Section:** (none)

**Explanation**

**QUESTION 46**

Which two options are two of the built-in features of IPv6? (Choose two.)

- A. VLSM
- B. native IPsec
- C. controlled broadcasts
- D. mobile IP
- E. NAT

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**QUESTION 47**

Which option is a characteristic of the RADIUS protocol?

- A. uses TCP
- B. offers multiprotocol support
- C. combines authentication and authorization in one process
- D. supports bi-directional challenge

**Correct Answer:** C

**Section:** (none)

**Explanation**

**QUESTION 48**

When STP mitigation features are configured, where should the root guard feature be deployed?

- A. toward ports that connect to switches that should not be the root bridge
- B. on all switch ports
- C. toward user-facing ports
- D. Root guard should be configured globally on the switch.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**QUESTION 49**

Refer to the exhibit. Which statement about this debug output is true?

Router# debug tacacs

```
14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15 (AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15 (AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15 (AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

- A. The requesting authentication request came from username GETUSER.
- B. The TACACS+ authentication request came from a valid user.
- C. The TACACS+ authentication request passed, but for some reason the user's connection was closed immediately.
- D. The initiating connection request was being spoofed by a different source address.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 50

Which option is a characteristic of a stateful firewall?

- A. can analyze traffic at the application layer
- B. allows modification of security rule sets in real time to allow return traffic
- C. will allow outbound communication, but return traffic must be explicitly permitted
- D. supports user authentication

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### QUESTION 51

Which type of NAT would you configure if a host on the external network required access to an internal host?

- A. outside global NAT
- B. NAT overload
- C. dynamic outside NAT
- D. static NAT

**Correct Answer:** D

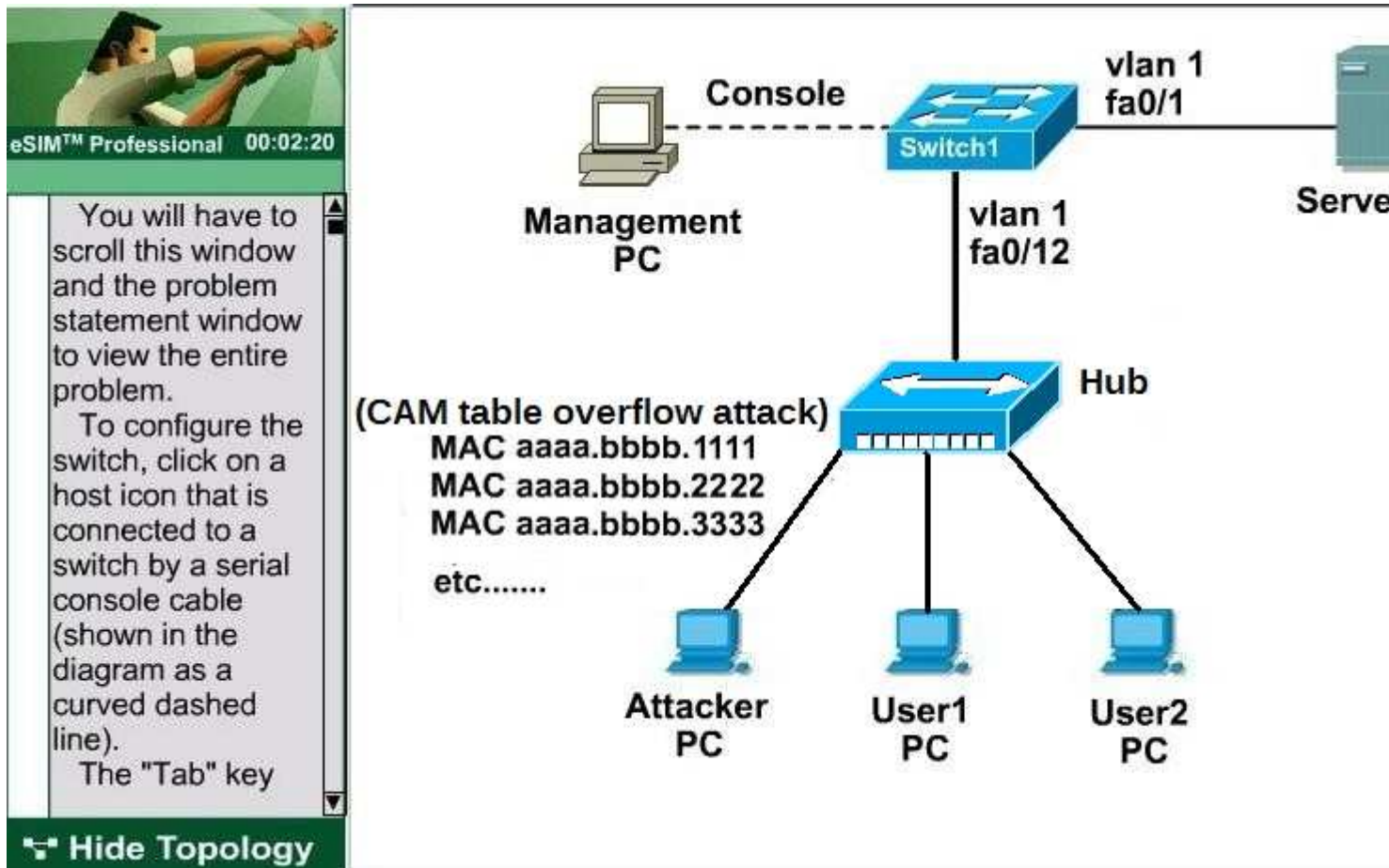
Section: (none)  
Explanation

**QUESTION 52**  
Lab Simulation

You are the network security administrator for Big Money Bank Co . You are informed that an attacker is performing a CAM table overflow attack by sending spoofed MAC addresses on one of the switch ports. The attacker has been identified and escorted out of the campus. You now need to take action to configure the switch to protect against this kind of attack in the future.

For purposes of this test, the attacker was connected via a hub to the Fa0/12 interface of the switch. The attacker was provided for your use. The enable password of the switch is **cisco**. Your task is to configure the Fa0/12 interface of the switch to limit the maximum number of MAC addresses that are allowed to access the port to two and to shutdown the interface when there is a violation.

Enable password: **cisco**



---

```
---S#show run
Building configuration...
Current configuration :
!
version 12.1
no service pad
Service timestamps debug uptime
Service timestamps log uptime
No service password-encryption
!
Hostname    -S
!
!
Enable secret 5 $1$0/yw#toqA0XRiCtY8gh7pM06fS0
!
Ip subnet-zero
!
Ip ssh time-out 120
Ip ssh authentication-retries 3
!
Spanning-tree mode pvst
No spanning-tree optimize bpdu transmission
Spanning-tree extend system-id
!
.....
!
Interface FastEthernet0/22
!
Interface FastEthernet0/23
!
Interface FastEthernet0/24
  switchport mode trunk
!
Interface GigabitEthernet0/1
!
Interface GigabitEthernet0/2
!
Interface vlan1
  ip address 172.26.26.202 255.255.255.0
  no ip route-cache
!
Ip http server
!
!
!
!
Line con 0
Line aux 0

Line vty 5 15
  password cisco
Login
!
End
-S#
```

---

```
A. Switch1>enable
Switch1#config t
Switch1(config)#interface fa0/12
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport port-security maximum 2
Switch1(config-if)#switchport port-security violation shutdown
Switch1(config-if)#no shut
Switch1(config-if)#end
Switch1#copy run start
```

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 53

Which two functions are required for IPsec operation? (Choose two.)

- A. using SHA for encryption
- B. using PKI for pre-shared-key authentication
- C. using IKE to negotiate the SA
- D. using AH protocols for encryption and authentication
- E. using Diffie-Hellman to establish a shared-secret key

**Correct Answer:** CE

**Section:** (none)

**Explanation**

### QUESTION 54

Which two features are supported by Cisco IronPort Security Gateway? (Choose two.)

- A. spam protection
- B. outbreak intelligence
- C. HTTP and HTTPS scanning
- D. email encryption
- E. DDoS protection

**Correct Answer:** AD

**Section:** (none)

**Explanation**

### QUESTION 55

Which option is a feature of Cisco ScanSafe technology?

- A. spam protection
- B. consistent cloud-based policy
- C. DDoS protection
- D. RSA Email DLP

**Correct Answer:** B

**Section: (none)**  
**Explanation**

**QUESTION 56**

Which two characteristics represent a blended threat? (Choose two.)

- A. man-in-the-middle attack
- B. trojan horse attack
- C. pharming attack
- D. denial of service attack
- E. day zero attack

**Correct Answer: BE**

**Section: (none)**

**Explanation**

**QUESTION 57**

Under which higher-level policy is a VPN security policy categorized?

- A. application policy
- B. DLP policy
- C. remote access policy
- D. compliance policy
- E. corporate WAN policy

**Correct Answer: C**

**Section: (none)**

**Explanation**

**QUESTION 58**

Refer to the exhibit. What does the option secret 5 in the username global configuration mode command indicate about the user password?

```
Router# show run | include username
Username test secret 5 $1$knm. $GOGQBIL8TK77POLWxvX400
```

- A. It is hashed using SHA.
- B. It is encrypted using DH group 5.
- C. It is hashed using MD5.
- D. It is encrypted using the service password-encryption command.
- E. It is hashed using a proprietary Cisco hashing algorithm.
- F. It is encrypted using a proprietary Cisco encryption algorithm.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 59**

What does level 5 in this enable secret global configuration mode command indicate?

- A. router#enable secret level 5 password
- B. The enable secret password is hashed using MD5.
- C. The enable secret password is hashed using SHA.
- D. The enable secret password is encrypted using Cisco proprietary level 5 encryption.
- E. Set the enable secret command to privilege level 5.
- F. The enable secret password is for accessing exec privilege level 5.

**Correct Answer:** E

**Section:** (none)

**Explanation**

**QUESTION 60**

Which Cisco management tool provides the ability to centrally provision all aspects of device configuration across the Cisco family of security products?

- A. Cisco Configuration Professional
- B. Security Device Manager
- C. Cisco Security Manager
- D. Cisco Secure Management Server

**Correct Answer:** C

**Section:** (none)

**Explanation**

**QUESTION 61**

Which option is the correct representation of the IPv6 address 2001:0000:150C:0000:0000:41B1:45A3:041D?

- A. 2001::150c::41b1:45a3:041d
- B. 2001:0:150c:0::41b1:45a3:04d1
- C. 2001:150c::41b1:45a3::41d
- D. 2001:0:150c::41b1:45a3:41d

**Correct Answer:** D

**Section:** (none)

**Explanation**

**QUESTION 62**

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

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

**Correct Answer:** ABF

**Section: (none)**  
**Explanation**

**QUESTION 63**

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**

**Section: (none)**

**Explanation**

**QUESTION 64**

Which two characteristics of the TACACS+ protocol are true? (Choose two.)

- A. uses UDP ports 1645 or 1812
- B. separates AAA functions
- C. encrypts the body of every packet
- D. offers extensive accounting capabilities
- E. is an open RFC standard protocol

**Correct Answer: BC**

**Section: (none)**

**Explanation**

**QUESTION 65**

Refer to the exhibit. Which statement about this output is true?



```

Oct13 19:46:06.170: AAA/MEMORY: create_user (0x4C5E1F60) user='tecteam'
ruser='NULL' ds0=0 port='tty515' rem_addr='10.0.2.13' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
Oct13 19:46:06.170: AAA/AUTHEN/START(2600878790): port='tty515' list=""
action=LOGIN service=ENABLE
Oct13 19:46:06.170: AAA/AUTHEN/START(2600878790): console enable - default to
enable password (if any)
Oct13 19:46:06.170: AAA/AUTHEN/START(2600878790): Method=ENABLE
Oct13 19:46:06.170: AAA/AUTHFN (2600878790): status = GETPASS
Oct13 19:46:07.266: AAA/AUTHEN/CONT(2600878790): continue_login
(user='{undef}')
Oct13 19:46:07.266: AAA/AUTHFN (2600878790): status = GETPASS
Oct13 19:46:07.266: AAA/AUTHEN/CONT(2600878790): Method=ENABLE
Oct13 19:46:07.266: AAA/AUTHEN(2600878790): password incorrect
Oct13 19:46:07.266: AAA/AUTHEN (2600878790): status = FAIL
Oct13 19:46:07.266: AAA/MEMORY: free_user (0x4C5E1F60) user='NULL'
ruser='NULL' port='tty515' rem_addr='10.0.2.13' authen_type=ASCII service=ENABLE
priv=15 vrf= (id=0)

```

- A. The user logged into the router with the incorrect username and password.
- B. The login failed because there was no default enable password.
- C. The login failed because the password entered was incorrect.
- D. The user logged in and was given privilege level 15.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 66

Refer to the exhibit. Which traffic is permitted by this ACL?

```

access-list 100 permit tcp 172.26.26.16 0.0.0.7 host 192.168.1.2 eq 443
access-list 100 permit tcp 172.26.26.16 0.0.0.7 host 192.168.1.2 eq 80
access-list 100 deny tcp any host 192.168.1.2 eq telnet
access-list 100 deny tcp any host 192.168.1.2 eq www
access-list 100 permit ip any any

```

- A. TCP traffic sourced from any host in the 172.26.26.8/29 subnet on any port to host 192.168.1.2 port 80 or

443

- B. TCP traffic sourced from host 172.26.26.21 on port 80 or 443 to host 192.168.1.2 on any port
- C. any TCP traffic sourced from host 172.26.26.30 destined to host 192.168.1.1
- D. any TCP traffic sourced from host 172.26.26.20 to host 192.168.1.2

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 67

Refer to the exhibit. Which statement about this partial CLI configuration of an access control list is true?

```
access-list 2 permit 10.10.0.10
access-list 2 deny 10.10.0.0 0.0.255.255
access-list 2 permit 10.10.0.0 0.0.255.255

interface fastEthernet0/0
 ip access-group 2 in
```

- 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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 68

Which type of Cisco ASA access list entry can be configured to match multiple entries in a single statement?

- A. nested object-class
- B. class-map
- C. extended wildcard matching
- D. object groups

**Correct Answer:** D

**Section:** (none)

**Explanation**

#### QUESTION 69

Which statement about an access control list that is applied to a router interface is true?

- A. It only filters traffic that passes through the router.
- B. It filters pass-through and router-generated traffic.
- C. An empty ACL blocks all traffic.
- D. It filters traffic in the inbound and outbound directions.

**Correct Answer:** A

**Section:** (none)

**Explanation**

#### **QUESTION 70**

You have been tasked by your manager to implement syslog in your network. Which option is an important factor to consider in your implementation?

- A. Use SSH to access your syslog information.
- B. Enable the highest level of syslog function available to ensure that all possible event messages are logged.
- C. Log all messages to the system buffer so that they can be displayed when accessing the router.
- D. Synchronize clocks on the network with a protocol such as Network Time Protocol.

**Correct Answer:** D

**Section:** (none)

**Explanation**

#### **QUESTION 71**

Which protocol secures router management session traffic?

- A. SSTP
- B. POP
- C. Telnet
- D. SSH

**Correct Answer:** D

**Section:** (none)

**Explanation**

#### **QUESTION 72**

Which two considerations about secure network management are important? (Choose two.)

- A. log tampering
- B. encryption algorithm strength
- C. accurate time stamping
- D. off-site storage
- E. Use RADIUS for router commands authorization.
- F. Do not use a loopback interface for device management access.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

#### **QUESTION 73**

Which command enables Cisco IOS image resilience?

- A. secure boot-<IOS image filename>
- B. secure boot-running-config
- C. secure boot-start
- D. secure boot-image

**Correct Answer:** D

**Section:** (none)

**Explanation**

#### **QUESTION 74**

Which router management feature provides for the ability to configure multiple administrative views?

- A. role-based CLI
- B. virtual routing and forwarding
- C. secure config privilege {level}
- D. parser view view name

**Correct Answer:** A

**Section:** (none)

**Explanation**

#### **QUESTION 75**

You suspect that an attacker in your network has configured a rogue Layer 2 device to intercept traffic from multiple VLANs, which allows the attacker to capture potentially sensitive data. Which two methods will help to mitigate this type of activity? (Choose two.)

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

**Correct Answer:** BD

**Section:** (none)

**Explanation**

#### **QUESTION 76**

You are the security administrator for a large enterprise network with many remote locations. You have been given the assignment to deploy a Cisco IPS solution. Where in the network would be the best place to deploy Cisco IOS IPS?

- A. inside the firewall of the corporate headquarters Internet connection
- B. at the entry point into the data center
- C. outside the firewall of the corporate headquarters Internet connection
- D. at remote branch offices

**Correct Answer:** D

**Section:** (none)

**Explanation**

**QUESTION 77**

Which IPS technique commonly is used to improve accuracy and context awareness, aiming to detect and respond to relevant incidents only and therefore, reduce noise?

- A. attack relevancy
- B. target asset value
- C. signature accuracy
- D. risk rating

**Correct Answer:** D

**Section:** (none)

**Explanation**

**QUESTION 78**

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

**Section:** (none)

**Explanation**

**QUESTION 79**

Which option describes the purpose of Diffie-Hellman?

- A. used between the initiator and the responder to establish a basic security policy
- B. used to verify the identity of the peer
- C. used for asymmetric public key encryption
- D. used to establish a symmetric shared key via a public key exchange process

**Correct Answer:** D

**Section:** (none)

**Explanation**

**QUESTION 80**

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

**Section:** (none)

## Explanation

### QUESTION 81

When configuring SSL VPN on the Cisco ASA appliance, which configuration step is required only for Cisco AnyConnect full tunnel SSL VPN access and not required for clientless SSL VPN?

- A. user authentication
- B. group policy
- C. IP address pool
- D. SSL VPN interface
- E. connection profile

**Correct Answer:** C

**Section:** (none)

**Explanation**

### QUESTION 82

For what purpose is the Cisco ASA appliance web launch SSL VPN feature used?

- A. to enable split tunneling when using clientless SSL VPN access
- B. to enable users to login to a web portal to download and launch the AnyConnect client
- C. to enable smart tunnel access for applications that are not web-based
- D. to optimize the SSL VPN connections using DTLS
- E. to enable single-sign-on so the SSL VPN users need only log in once

**Correct Answer:** B

**Section:** (none)

**Explanation**

### QUESTION 83

Which statement describes how VPN traffic is encrypted to provide confidentiality when using asymmetric encryption?

- A. The sender encrypts the data using the sender's private key, and the receiver decrypts the data using the sender's public key.
- B. The sender encrypts the data using the sender's public key, and the receiver decrypts the data using the sender's private key.
- C. The sender encrypts the data using the sender's public key, and the receiver decrypts the data using the receiver's public key.
- D. The sender encrypts the data using the receiver's private key, and the receiver decrypts the data using the receiver's public key.
- E. The sender encrypts the data using the receiver's public key, and the receiver decrypts the data using the receiver's private key.
- F. The sender encrypts the data using the receiver's private key, and the receiver decrypts the data using the sender's public key.

**Correct Answer:** E

**Section:** (none)

**Explanation**

### QUESTION 84

Which four types of VPN are supported using Cisco ISRs and Cisco ASA appliances? (Choose four.)

- A. SSL clientless remote-access VPNs
- B. SSL full-tunnel client remote-access VPNs
- C. SSL site-to-site VPNs
- D. IPsec site-to-site VPNs
- E. IPsec client remote-access VPNs
- F. IPsec clientless remote-access VPNs

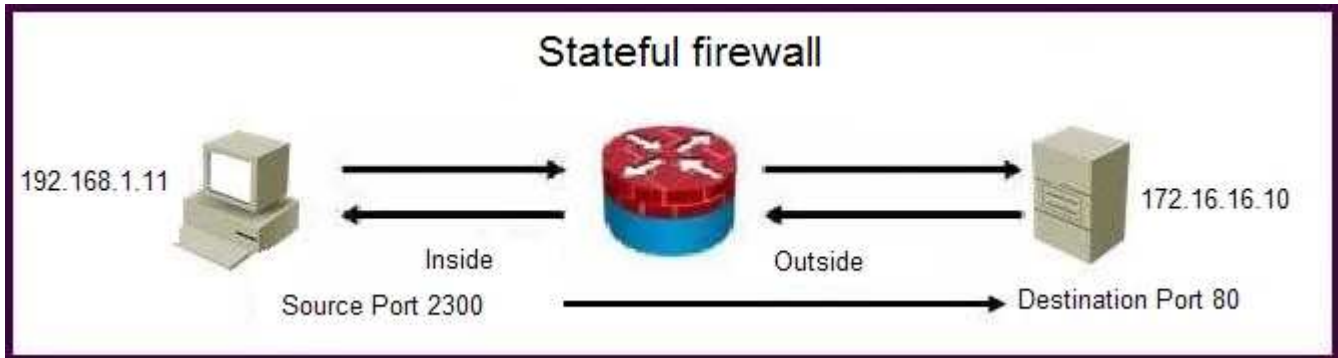
**Correct Answer:** ABDE

**Section:** (none)

**Explanation**

**QUESTION 85**

Refer to the exhibit. Using a stateful packet firewall and given an inside ACL entry of permit ip 192.16.1.0 0.0.0.255 any, what would be the resulting dynamically configured ACL for the return traffic on the outside ACL?



- A. permit tcp host 172.16.16.10 eq 80 host 192.168.1.11 eq 2300
- B. permit ip 172.16.16.10 eq 80 192.168.1.0 0.0.0.255 eq 2300
- C. permit tcp any eq 80 host 192.168.1.11 eq 2300
- D. permit ip host 172.16.16.10 eq 80 host 192.168.1.0 0.0.0.255 eq 2300

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 86**

Which option is the resulting action in a zone-based policy firewall configuration with these conditions?

Source: Zone 1  
Destination: Zone 2  
Zone pair exists?: Yes  
Policy exists?: No

- A. no impact to zoning or policy
- B. no policy lookup (pass)
- C. drop
- D. apply default policy

**Correct Answer:** C

**Section:** (none)

**Explanation**

**QUESTION 87**

A Cisco ASA appliance has three interfaces configured. The first interface is the inside interface with a security level of 100. The second interface is the DMZ interface with a security level of 50. The third interface is the outside interface with a security level of 0. By default, without any access list configured, which five types of traffic are permitted? (Choose five.)

- A. outbound traffic initiated from the inside to the DMZ
- B. outbound traffic initiated from the DMZ to the outside
- C. outbound traffic initiated from the inside to the outside
- D. inbound traffic initiated from the outside to the DMZ
- E. inbound traffic initiated from the outside to the inside
- F. inbound traffic initiated from the DMZ to the inside
- G. HTTP return traffic originating from the inside network and returning via the outside interface
- H. HTTP return traffic originating from the inside network and returning via the DMZ interface
- I. HTTP return traffic originating from the DMZ network and returning via the inside interface
- J. HTTP return traffic originating from the outside network and returning via the inside interface

**Correct Answer:** ABCGH

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Answer: ABCGH

**QUESTION 88**

Which two protocols enable Cisco Configuration Professional to pull IPS alerts from a Cisco ISR router? (Choose two.)

- A. syslog
- B. SDEE
- C. FTP
- D. TFTP
- E. SSH
- F. HTTPS

**Correct Answer:** BF

**Section:** (none)

**Explanation**

**QUESTION 89**

Which two functions are required for IPsec operation? (Choose two.)

- A. using SHA for encryption
- B. using PKI for pre-shared key authentication
- C. using IKE to negotiate the SA
- D. using AH protocols for encryption and authentication
- E. using Diffie-Hellman to establish a shared-secret key



**Correct Answer:** CE  
**Section:** (none)  
**Explanation**

**QUESTION 90**

Which statement about disabled signatures when using Cisco IOS IPS is true?

- A. They do not take any actions, but do produce alerts.
- B. They are not scanned or processed.
- C. They still consume router resources.
- D. They are considered to be "retired" signatures.

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**QUESTION 91**

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  
**Section:** (none)  
**Explanation**

**QUESTION 92**

Which two services are provided by IPsec? (Choose two.)

- A. Confidentiality
- B. Encapsulating Security Payload
- C. Data Integrity
- D. Authentication Header
- E. Internet Key Exchange

**Correct Answer:** AC  
**Section:** (none)  
**Explanation**

**QUESTION 93**

Which type of Cisco IOS access control list is identified by 100 to 199 and 2000 to 2699?

- A. standard
- B. extended
- C. named
- D. IPv4 for 100 to 199 and IPv6 for 2000 to 2699

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**QUESTION 94**

Which priority is most important when you plan out access control lists?

- A. Build ACLs based upon your security policy.
- B. Always put the ACL closest to the source of origination.
- C. Place deny statements near the top of the ACL to prevent unwanted traffic from passing through the router.
- D. Always test ACLs in a small, controlled production environment before you roll it out into the larger production network.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**QUESTION 95**

Which step is important to take when implementing secure network management?

- A. Implement in-band management whenever possible.
- B. Implement telnet for encrypted device management access.
- C. Implement SNMP with read/write access for troubleshooting purposes.
- D. Synchronize clocks on hosts and devices.
- E. Implement management plane protection using routing protocol authentication.

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**QUESTION 96**

Which statement best represents the characteristics of a VLAN?

- A. Ports in a VLAN will not share broadcasts amongst physically separate switches.
- B. A VLAN can only connect across a LAN within the same building.
- C. A VLAN is a logical broadcast domain that can span multiple physical LAN segments.
- D. A VLAN provides individual port security.

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**QUESTION 97**

Which Layer 2 protocol provides loop resolution by managing the physical paths to given network segments?

- A. root guard
- B. port fast
- C. HSRP
- D. STP

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**



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

#### QUESTION 98

Which statement is true when you have generated RSA keys on your Cisco router to prepare for secure device management?

- A. You must then zeroize the keys to reset secure shell before configuring other parameters.
- B. The SSH protocol is automatically enabled.
- C. You must then specify the general-purpose key size used for authentication with the crypto key generate rsa general-keys modulus command.
- D. All vty ports are automatically enabled for SSH to provide secure management.

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

#### QUESTION 99

What is the key difference between host-based and network-based intrusion prevention?

- A. Network-based IPS is better suited for inspection of SSL and TLS encrypted data flows.
- B. Network-based IPS provides better protection against OS kernel-level attacks against hosts and servers.
- C. Network-based IPS can provide protection to desktops and servers without the need of installing specialized software on the end hosts and servers.
- D. Host-based IPS can work in promiscuous mode or inline mode.
- E. Host-based IPS is more scalable than network-based IPS.
- F. Host-based IPS deployment requires less planning than network-based IPS.

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

#### QUESTION 100

Refer to the exhibit. You are a network manager for your organization. You are looking at your Syslog server reports. Based on the Syslog message shown, which two statements are true? (Choose two.)

```
Feb 1 10:12:08 PST: %SYS-5-CONFIG_1: Configured from console by vty0 (10.2.2.6)
```

- A. Service timestamps have been globally enabled.
- B. This is a normal system-generated information message and does not require further investigation.

- C. This message is unimportant and can be ignored.
- D. This message is a level 5 notification message.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 101

Refer to the exhibit. Which statement is correct based on the show login command output shown?

**Router# show login**

```
A default login delay of 1 seconds is applied.  
No Quiet-Mode access list has been configured.  
All successful login is logged and generate SNMP traps.  
All failed login is logged and generate SNMP traps.  
Router enabled to watch for login Attacks.  
If more than 2 login failures occur in 100 seconds or less, logins will be disabled  
for 100 seconds.  
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.  
Denying logins from all sources.
```

- A. When the router goes into quiet mode, any host is permitted to access the router via Telnet, SSH, and HTTP, since the quiet-mode access list has not been configured.
- B. The login block-for command is configured to block login hosts for 93 seconds.
- C. All logins from any sources are blocked for another 193 seconds.
- D. Three or more login requests have failed within the last 100 seconds.

**Correct Answer:** D

**Section:** Implementing Intrusion Prevention

**Explanation**

**Explanation/Reference:**

#### QUESTION 102

Which four methods are used by hackers? (Choose four.)

- A. footprint analysis attack
- B. privilege escalation attack
- C. buffer Unicode attack
- D. front door attacks
- E. social engineering attack
- F. Trojan horse attack

**Correct Answer:** ABEF

**Section:** (none)

**Explanation**

**QUESTION 103**

Which statement about Cisco IOS IPS on Cisco IOS Release 12.4(11)T and later is true?

- A. uses Cisco IPS 5.x signature format
- B. requires the Basic or Advanced Signature Definition File
- C. supports both inline and promiscuous mode
- D. requires IEV for monitoring Cisco IPS alerts
- E. uses the built-in signatures that come with the Cisco IOS image as backup
- F. supports SDEE, SYSLOG, and SNMP for sending Cisco IPS alerts

**Correct Answer:** A

**Section:** (none)

**Explanation**

**QUESTION 104**

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

**Section:** (none)

**Explanation**

**QUESTION 105**

Which kind of table do most firewalls use today to keep track of the connections through the firewall?

- A. dynamic ACL
- B. reflexive ACL
- C. netflow
- D. queuing
- E. state
- F. express forwarding

**Correct Answer:** E

**Section:** (none)

**Explanation**

**QUESTION 106**

Which Cisco IOS command is used to verify that either the Cisco IOS image, the configuration files, or both have been properly backed up and secured?

- A. show archive
- B. show secure bootset
- C. show flash
- D. show file systems
- E. dir

F. dir archive

**Correct Answer: B**

**Section: (none)**

**Explanation**

#### QUESTION 107

What does the secure boot-config global configuration accomplish?

- A. enables Cisco IOS image resilience
- B. backs up the Cisco IOS image from flash to a TFTP server
- C. takes a snapshot of the router running configuration and securely archives it in persistent storage
- D. backs up the router running configuration to a TFTP server
- E. stores a secured copy of the Cisco IOS image in its persistent storage

**Correct Answer: C**

**Section: (none)**

**Explanation**

#### QUESTION 108

Refer to the exhibit. Based on the show policy-map type inspect zone-pair session command output shown, what can be determined about this Cisco IOS zone based firewall policy?

```
Class-map: TEST-Class (match-all)
Match: access-group 110
Match: protocol http
Inspect
Established Sessions
Session 643BCF88 (10.0.2.12:3364) =>(172.26.26.51:80) http SIS_OPEN
Created 00:00:10, Last heard 00:00:00
Bytes sent (initiator, responder) [1268:64324]
Session 643BB9C8 (10.0.2.12:3361) =>(172.26.26.51:80) http SIS_OPEN
Created 00:00:16, Last heard 00:00:06
Bytes sent (initiator, responder) [2734:38447]
Session 643BD240 (10.0.2.12:3362) =>(172.26.26.51:80) http SIS_OPEN
Created 00:00:14, Last heard 00:00:07
Bytes sent (initiator, responder) [2219:39813]
Session 643BBF38 (10.0.2.12:3363) =>(172.26.26.51:80) http SIS_OPEN
Created 00:00:14, Last heard 00:00:06
Bytes sent (initiator, responder) [2106:19895]
Class-map: class-default (match-any)
Match: any
Drop (default action)
58 packets, 2104 bytes
```

- A. All packets will be dropped since the class-default traffic class is matching all traffic.
- B. This is an inbound policy (applied to traffic sourced from the less secured zone destined to the more secured zone).
- C. This is an outbound policy (applied to traffic sourced from the more secured zone destined to the less secured zone).

- D. Stateful packet inspection will be applied only to HTTP packets that also match ACL 110.
- E. All non-HTTP traffic will be permitted to pass as long as it matches ACL 110.
- F. All non-HTTP traffic will be inspected.

**Correct Answer:** D

**Section:** Implementing Firewall Technologies

**Explanation**

**Explanation/Reference:**

#### **QUESTION 109**

When using a stateful firewall, which information is stored in the stateful session flow table?

- A. the outbound and inbound access rules (ACL entries)
- B. the source and destination IP addresses, port numbers, TCP sequencing information, and additional flags for each TCP or UDP connection associated with a particular session
- C. all TCP and UDP header information only
- D. all TCP SYN packets and the associated return ACK packets only
- E. the inside private IP address and the translated inside global IP address

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### **QUESTION 110**

Which statement is true about configuring access control lists to control Telnet traffic destined to the router itself?

- A. The ACL is applied to the Telnet port with the ip access-group command.
- B. The ACL should be applied to all vty lines in the in direction to prevent an unwanted user from connecting to an unsecured port.
- C. The ACL applied to the vty lines has no in or out option like ACL being applied to an interface.
- D. The ACL must be applied to each vty line individually.

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### **QUESTION 111**

When configuring role-based CLI on a Cisco router, which step is performed first?

- A. Log in to the router as the root user.
- B. Create a parser view called "root view."
- C. Enable role-based CLI globally on the router using the privileged EXEC mode Cisco IOS command.
- D. Enable the root view on the router.
- E. Enable AAA authentication and authorization using the local database.
- F. Create a root local user in the local database.

**Correct Answer:** D

**Section:** (none)

**Explanation**

### QUESTION 112

Refer to the exhibit. Which statement about the aaa configurations is true?

```
R(config)# username admin privilege level 15 secret hardtOcRackPw
R(config)# aaa new-model
R(config)# aaa authentication login default tacacs+
R(config)# aaa authentication login test tacacs+ local
R(config)# line vty 0 4
R(config-line)# login authentication test
R(config-line)# line con 0
R(config-line)# end
```

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 113

Which characteristic is a potential security weakness of a traditional stateful firewall?

- A. It cannot support UDP flows.
- B. It cannot detect application-layer attacks.
- C. It cannot ensure each TCP connection follows a legitimate TCP three-way handshake.
- D. It works only in promiscuous mode.
- E. The status of TCP sessions is retained in the state table after the sessions terminate.
- F. It has low performance due to the use of syn-cookies.

**Correct Answer:** B

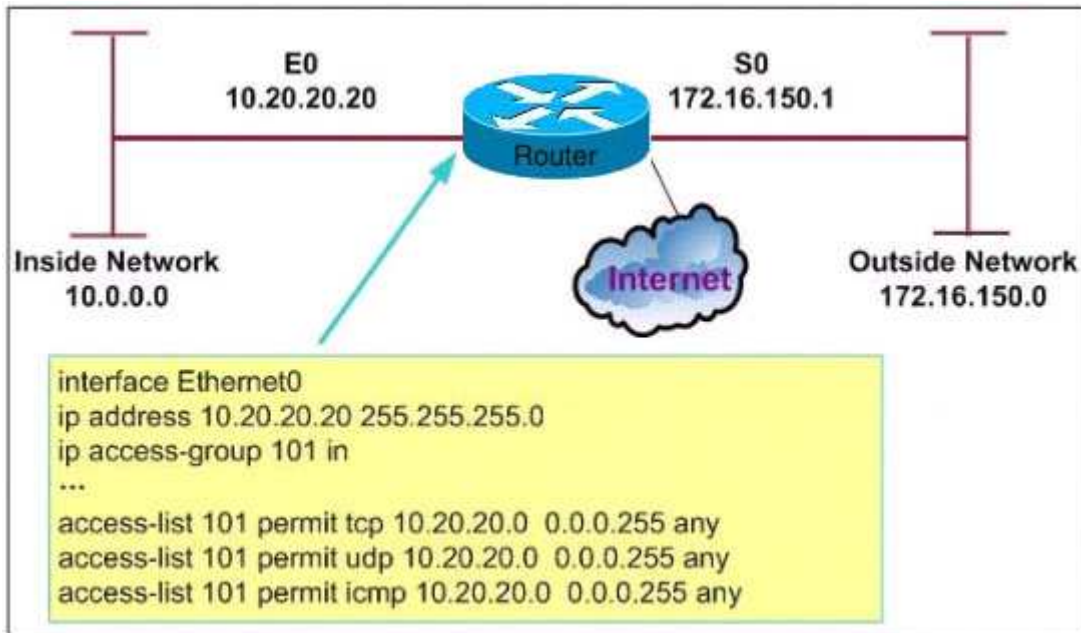
**Section:** (none)

**Explanation**

### QUESTION 114

Refer to the exhibit and partial configuration. Which statement is true?





- A. All traffic destined for network 172.16.150.0 will be denied due to the implicit deny all.
- B. All traffic from network 10.0.0.0 will be permitted.
- C. Access-list 101 will prevent address spoofing from interface E0.
- D. This is a misconfigured ACL resulting in traffic not being allowed into the router in interface S0.
- E. This ACL will prevent any host on the Internet from spoofing the inside network address as the source address for packets coming into the router from the Internet.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 115

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

- A. changes to the config-register setting
- B. ROMMON
- C. password encryption service
- D. aaa new-model global configuration command
- E. the xmodem privilege EXEC mode command to recover the Cisco IOS image

**Correct Answer: B**

**Section: (none)**

**Explanation**

#### QUESTION 116

What does the MD5 algorithm do?

- A. takes a message less than 2<sup>64</sup> bits as input and produces a 160-bit message digest
- B. takes a variable-length message and produces a 168-bit message digest

- C. takes a variable-length message and produces a 128-bit message digest
- D. takes a fixed-length message and produces a 128-bit message digest

**Correct Answer:** C

**Section:** (none)

**Explanation**

### QUESTION 117

You have configured a standard access control list on a router and applied it to interface Serial 0 in an outbound direction. No ACL is applied to Interface Serial 1 on the same router. What happens when traffic being filtered by the access list does not match the configured ACL statements for Serial 0?

- 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 1.
- D. The traffic is dropped.

**Correct Answer:** D

**Section:** (none)

**Explanation**

### QUESTION 118

Hotspot Questions

Scenario:

You are the security admin for a small company. This morning your manager has supplied you with a list of Cisco ISR and CCP configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your business question.

The screenshot displays a Cisco exam interface. On the left, a vertical progress bar is labeled 'Questions' at the top and '0% Complete' at the bottom. Below the bar are five numbered buttons (1-5) and a green arrow pointing up, and another green arrow pointing down. The main area is divided into two sections: 'Instructions' and 'Scenario'. The 'Instructions' section contains the text: 'You can click on the grey buttons below to view the different windows. Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it'. The 'Scenario' section contains the text: 'You are the security admin for a small company. This morning your manager has supplied you with a list of Cisco configuration questions. Using CCP, your job is to navigate the pre-configured CCP in order to find answers to your business questions. Not all screens are active for this exercise.' At the bottom right, the Cisco logo is visible.

Select Community Member:

(No devices discovered)

Home > Community View

- Router
- Switching
- Switching Module
- Security
- Traffic Monitoring

Utilities

- Flash File Management
- Software Upgrade
- Configuration Editor
- Save Configuration to PC
- Write to Startup Configuration
- Telnet

Cisco Configuration Professional News

Date	Title
22-Jul-2010	<a href="#">Provide CCP Feedback</a>

Community Information

Selected community: **Demo Community** . Select a device from the table below.

Filter

IP address / Hostname	Router Hostname	Connection Type
CISCO-887-1		Non secure
CISCO-1861-W		Non secure
CISCO-2921-1		Non secure

Manage Devices Delete Discover Discovery Details



Home



Configure



Monitor



Select Community Member:

CISCO-2921-1



Configure > Interface Management > Interface and Connections



- Interface Management
  - Interface and Connections
  - Module Configuration
- Router
  - Router Options
  - Time
    - Date and Time
    - NTP and SNTP
  - Router Access
    - User Accounts/View
    - VTY
    - Management Access
    - SSH
  - DHCP
  - DNS
    - DNS
    - Dynamic DNS
  - Static and Dynamic Routing
  - AAA
    - AAA Summary
    - AAA Servers and Groups
    - Authentication Policies

Utilities



## Interfaces and Connections

Create Connection

Edit Interface/Connection

Edit Controllers/Connection

Create New Connection

Select a connection and click Create New Connection

- Ethernet LAN
- Ethernet (PPPoE or Unencapsulated Routing)
- G.SHDSL (PPPoE or RFC 1483 Routing or PPPoA)
- Cable Modem
- Analog Modem (PPP)

Information

Configure Ethernet LAN interface for straight routing and 802.1q trunking

Create New Connection

How do I:

How Do I Configure an Unsupported WAN Interface?

Question 1

What NAT address will be assigned by ACL 1?

- 192.168.1.0/25
- GigabitEthernet0/0 interface address
- 172.25.223.0/24
- 10.0.10.0/24

**Answer:**

Question 1

What NAT address will be assigned by ACL 1?

- 192.168.1.0/25
- GigabitEthernet0/0 interface address
- 172.25.223.0/24
- 10.0.10.0/24

**Explanation:**

Select Community Member:

CISCO-2921-1

**Configure > Router > ACL > NAT Rules**

- Interface Management
- Router**
  - Router Options
  - Time
  - Router Access
  - DHCP
  - DNS
  - Static and Dynamic Routing
  - AAA
  - ACL**
    - Object Groups
    - ACL Summary
    - ACL Editor
    - NAT Rules**
    - IPSec Rules
    - NAC Rules
    - Firewall Rules
    - QoS Rules
    - Unsupported Rules
    - Externally-defined Rules
    - NAT
    - QoS
  - Performance Routing
  - Router Provisioning
  - SDP

Utilities

- Flash File Management
- Configuration Editor
- Save Configuration to PC
- Write to Startup Configuration
- Telnet
- Reload Device
- Ping and Traceroute
- View

Additional Tasks

NAT Rules

Name/Number	Used by
1	NAT

Action	Source	Log
✓ Permit	192.168.1.0/0.0.0.127	

Question 2

Which four protocols are included in the Inspection Class Map OUT\_SERVICE? (Choose four)

- FTP
- HTTP
- HTTPS
- SMTP
- P2P
- ICMP

**Answer:**

Question 2

Which four protocols are included in the Inspection Class Map OUT\_SERVICE? (Choose four)

- FTP
- HTTP
- HTTPS
- SMTP
- P2P
- ICMP

**Explanation:**



Home



Configure



Monitor



Select Community Member:

CISCO-2921-1

Interface Management

Router

Security

Firewall

Firewall

Firewall Components

Zone Pairs

Zones

VPN

Public Key Infrastructure

NAC

Web Filter Configuration

Intrusion Prevention

802.1x

Port to Application Mappings

C3PL

Policy Map

Class Map

Parameter Map

Security Audit

Unified Communications

Utilities

Flash File Management

Configuration Editor

Save Configuration to PC

Write to Startup Configuration

Telnet

Reload Device

Ping and Traceroute

View

Configure > Security > Firewall > Firewall

Firewall

Create Firewall

Edit Firewall Policy

Add Edit... Delete Move

Traffic Classification		
ID	Source	Destination
ccp-permit-dmzservice ( in-zone to dmz-zone , out		
1	any	10.1.1.1
2	Unmatched Traffic	
ccp-permit ( out-zone to self)		
1	any	any
2	any	any
3	Unmatched Traffic	
ccp-permit-icmpreply ( self to out-zone)		
1	any	any
2	any	any
3	any	any
4	Unmatched Traffic	
ccp-inspect ( in-zone to out-zone)		
1	100	
	● 255.255.255.255 -> any	
	● 127.0.0.0/0.255.255.255 -> any	
	● 10.2.0.0/0.0.0.255 -> any	
	● 10.3.0.0/0.0.0.255 -> any	
2	any	any
3	any	any
4	any	any
5	any	any
6	Unmatched Traffic	







### Question 3

Which Class Map is used by the INBOUND Rule?

- SERVICE\_IN
- Class-map ccp-cls-2
- Ccp-cls-2
- Class-map SERVICE\_IN

**Answer:**

### Question 3

Which Class Map is used by the INBOUND Rule?

- SERVICE\_IN
- Class-map ccp-cls-2
- Ccp-cls-2
- Class-map SERVICE\_IN

**Explanation:**



Home



Configure



Monitor



Select Community Member:

CISCO-2921-1

Interface Management

Router

Security

Firewall

Firewall

Firewall Components

Zone Pairs

Zones

VPN

Public Key Infrastructure

NAC

Web Filter Configuration

Intrusion Prevention

802.1x

Port to Application Mappings

C3PL

Policy Map

Class Map

QoS Class Map

Inspection

Deep Packet Inspection

Parameter Map

Security Audit

Unified Communications

Utilities

Flash File Management

Configuration Editor

Save Configuration to PC

Write to Startup Configuration

Telnet

Reload Device

Ping and Traceroute

View

Configure > Security > Firewall > Firewall



Firewall

Create Firewall

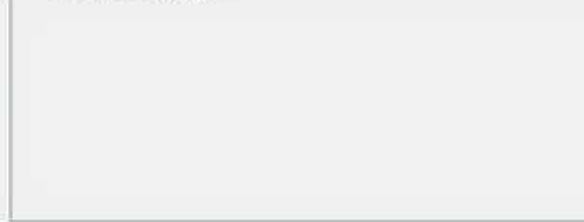
Edit Firewall Policy

Add Edit... Delete Move

Traffic Classification		
ID	Source	Destination
ccp-permit-icmpreply ( self to out-zone)		
1	any	any
2	any	any
3	any	any
4	Unmatched Traffic	
ccp-inspect ( in-zone to out-zone)		
1	100	
	● 255.255.255.255 -> any	
	● 172.0.0.0/0.255.255.255 -> any	
	● 10.3.0.0/0.0.0.255 -> any	
2	any	any
3	any	any
4	any	any
5	any	any
ccp-permit ( out-zone to self)		
1	any	any
2	any	any
3	Unmatched Traffic	

255.255.255.255  
172.0.0.0/0.255.255.255  
10.3.0.0/0.0.0.255

Rule Flow Diagram



#### Question 4

What is included in the Network Object Group INSIDE? (Choose two.)

- Network 192.168.1.0/24
- Network 172.25.133.0/24
- Network 10.0.10.0/24
- Network 10.0.0.0/8
- Network 192.168.1.0/8

**Answer:**

#### Question 4

What is included in the Network Object Group INSIDE? (Choose two.)

- Network 192.168.1.0/24
- Network 172.25.133.0/24
- Network 10.0.10.0/24
- Network 10.0.0.0/8
- Network 192.168.1.0/8

#### Question 5

Which policy is assigned to Zone Pair sdm-zp-OUT-IN?

- sdm-cls-http
- OUT\_SERVICE
- ccp-policy-ccp-cls-1
- ccp-policy-ccp-cls-2

**Answer:**

### Question 5

Which policy is assigned to Zone Pair sdm-zp-OUT-IN?

- sdm-cls-http
- OUT\_SERVICE
- ccp-policy-ccp-cls-1
- ccp-policy-ccp-cls-2

**Explanation:**

Select Community Member:

CISCO-2921-1

Configure > Security > Firewall > Firewall C

**Additional Tasks**

Zone Pairs

Zone Pair	Source
sdm-zip-OUT-IN	out-zone
ccp-zp-self-out	self
ccp-zp-in-out	in-zone
ccp-zp-in-dmz	in-zone
ccp-zp-out-dmz	out-zone
ccp-zp-out-self	out-zone

Search:

- ▶ Interface Management
- ▶ Router
- ▼ **Security**
  - ▼ Firewall
    - Firewall
    - ▼ **Firewall Components**
      - ▼ **Zone Pairs**
      - Zones
  - ▶ VPN
  - ▶ Public Key Infrastructure
  - ▶ NAC
  - Web Filter Configuration
  - Intrusion Prevention
  - 802.1x
  - Port to Application Mappings
  - ▼ C3PL
    - ▼ Policy Map
      - QoS Policy Map
      - Protocol Inspection
      - ▶ Application Inspection
    - ▼ Class Map
      - QoS Class Map
      - Inspection
      - ▶ Deep Packet Inspection
    - ▶ Parameter Map

**Utilities**

- Flash File Management
- Configuration Editor
- Save Configuration to PC
- Write to Startup Configuration
- Telnet
- Reload Device
- Ping and Traceroute
- ▶ View

- A.
- B.
- C.
- D.

**Correct Answer:**  
**Section: LabSim**  
**Explanation**

**Explanation/Reference:**

**QUESTION 119**

Lab Simulation

**Instruction**

This item contains a simulation task. Refer to the scenario and topology before starting. Open the Topology window and click the required icon to open a virtual terminal. Check your configuration from the client system in the topology.

---

**Scenario**

You are the security administrator for a small company. You need to modify an existing configuration of a Cisco Integrated Services Router. Using Cisco Configuration Professional (CCP), you will need to add the following configurations to the router to meet security policy requirements.

- Configure Network Time Protocol (NTP)
  - Preferred NTP Server IP 192.168.4.2
  - Source Interface FastEthernet 0/1
  - Authentication key of 1 with a key value of cisco
- Create a new Access Rule
  - Name Inbound
  - Type Extended Rule
- Create and add a new Rule Entry to the Access Rule
  - Permit any source and any destination for protocol eigrp
- Add an additional Rule Entry to the Access Rule
  - Permit any source to the 10.0.2.0/24 network for protocol 80
- Associate this new Access Rule to the **OUTSIDE** interface in the **INBOUND** direction

NOTE: Allow CCP to add an entry rule to allow NTP traffic

---

**TOPOLOGY**

Scenario topology

The diagram shows a network topology. At the top, there is an NTP Server represented by a server icon with the IP address 192.168.4.4. A line connects the NTP Server to a cloud icon representing a network. The cloud is labeled with the IP address 192.168.2.0/24. A line connects the cloud to a Cisco ISR router, represented by a red and blue router icon. The router is labeled with the IP address .2. The text 'Cisco ISR' is written below the router icon.

**Instruction** | **Scenario** | **TOPOLOGY**



Application Help



Home



Configure



Monitor



Cisco Configuration

Select Community Member:

10.0.2.1

<< Home >>

Community View

Community View

### Cisco Configuration Professional News

Date	Title
22-Jul-2010	<a href="#">Provide CCP Feedback</a>

### Community Information

Selected community: **New Community** . Select a device from the table below. Use the

Filter

IP address / Hostname	Router Hostname	Connection Type
10.0.2.1	pod-2-isr	Secure

Manage Devices

Delete

Discover

Discovery Details

### Utilities

- Flash File Management
- Software Upgrade
- Configuration Editor
- Save Configuration to PC
- Write to Startup Configuration
- Telnet

http://127.0.0.1:8600/Counterpoint/CPMain.html?rand=9185 - Windows Internet Explorer provided by Cisco

Application Help

Home Configure Monitor

Select Community Member: 10.0.2.1

Configure > Router > DHCP DHCP Bindings

Additional Tasks

DHCP Bindings

Binding Name	Host IP/Mask	MAC address	Type	Client

Community View

- Interface Management
- Router
- Security
- Unified Communications

Instruction Scenario **TOPOLOGY**

A. For the NTP portion:

Click on Router - Time - NTP and SNTP on left hand pane. Then click the Add button. Enter the Server IP address and source interface and key information as specified. Also be sure to click the Prefer button.

For the access rule portion:

Click on Router - ACL - ACL Editor. Click Add button. Then enter Inbound for the name and make sure rule is extended. Then click Add at the rule entry. Then ensure that permit is selected and that source and destination boxes both say Any IP Address (They should already).

Under Protocol and Service select EIGRP. Hit OK.

Then click add button again. Leave the source as any and click the destination box as "A network" and type in 10.0.2.0 and select the wildcard mask as 0.0.0.255. Click on the TCP protocol button and select "www" Hit OK.

Finally, click on edit for this rule and click on the Associate button. Select the outside interface and select the inbound direction.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 120**

Drag the IPS detection approaches from the left and drop on the correct IPS detection technology categories on the right

Detects attacks based on known attacks fingerprints	policy-based
Detects unexpected traffic spikes	anomaly-based
Only allows HTTPS traffic to the web server	signature-based
Detects events based on correlations with a blacklist downloaded from a dynamically updated database	reputation-based

**Select and Place:**

Drag the IPS detection approaches from the left and drop on the correct IPS detection technology categories on the right

Detects attacks based on known attacks fingerprints	policy-based
Detects unexpected traffic spikes	anomaly-based
Only allows HTTPS traffic to the web server	signature-based
Detects events based on correlations with a blacklist downloaded from a dynamically updated database	reputation-based

**Correct Answer:**

Drag the IPS detection approaches from the left and drop on the correct IPS detection technology categories on the right



Only allows HTTPS traffic to the web server

Detects unexpected traffic spikes

Detects attacks based on known attacks fingerprints

Detects events based on correlations with a blacklist downloaded from a dynamically updated database

Section: Drag and Drop  
Explanation

Explanation/Reference:

#### QUESTION 121

Drag the correct IPv6 unicast types from the left and drop them on the boxes on the right. Not all types are used

global

6to4

link-local

reserved

site-local

solicited node

Target

Target

Target

Target

Select and Place:

Drag the correct IPv6 unicast types from the left and drop them on the boxes on the right. Not all types are used

global

6to4

link-local

reserved

site-local

solicited node

Target

Target

Target

Target

Correct Answer:

Drag the correct IPv6 unicast types from the left and drop them on the boxes on the right. Not all types are used

global

6to4

link-local

reserved

site-local

solicited node

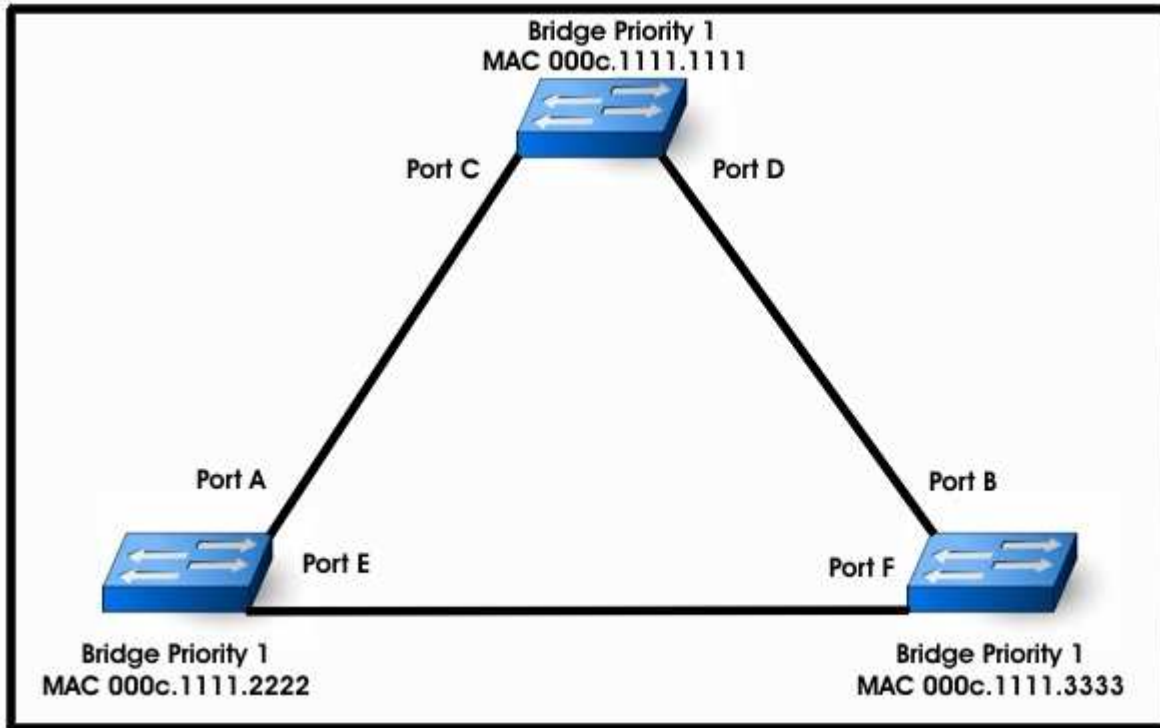
Section: Drag and Drop

**Explanation**

**Explanation/Reference:**

**QUESTION 122**

Refer to the exhibit. Drag the port(s) from the left and drop them on the correct STP roles on the right. Not all options on the left are used.



Port E

Port F

Ports A and B

Ports C and D

Ports C, D, and E

Ports A, B, and F

Ports A, B, and E

Ports A, B, C, and D

root port(s)

designated port(s)

non-designated port(s)

Select and Place:

Port E

Port F

Ports A and B

Ports C and D

Ports C, D, and E

Ports A, B, and F

Ports A, B, and E

Ports A, B, C, and D

root port(s)

designated port(s)

non-designated port(s)

Correct Answer:



Port E

Ports C and D

Ports A, B, and F

Ports A, B, and E

Ports A, B, C, and D

Ports A and B

Ports C, D, and E

Port F

Section: Drag and Drop  
Explanation

Explanation/Reference:

QUESTION 123

Match The descriptions on the left with the IKE phases on the right.

Perform a Diffie-Hellman exchange

Establish IPsec SAs

Negotiate IPsec security policies

Negotiate IKE policy sets authenticate peers

Perform an optional Diffie-Hellman exchange

IKE Phase 1

IKE Phase 2

Select and Place:

Match The descriptions on the left with the IKE phases on the right.

Perform a Diffie-Hellman exchange

Establish IPsec SAs

Negotiate IPsec security policies

Negotiate IKE policy sets authenticate peers

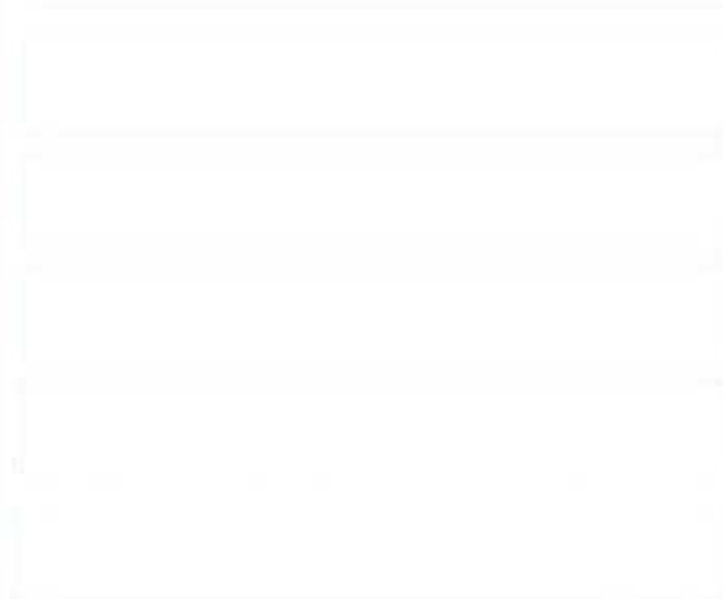
Perform an optional Diffie-Hellman exchange

IKE Phase 1

IKE Phase 2

Correct Answer:

Match The descriptions on the left with the IKE phases on the right.



IKE Phase 1

Negotiate IKE policy sets authenticate peers

Perform a Diffie-Hellman exchange

IKE Phase 2

Negotiate IPsec security policies

Establish IPsec SAs

Perform an optional Diffie-Hellman exchange

Section: Drag and Drop  
Explanation

Explanation/Reference:

QUESTION 124

Drag the characteristics from the left and drop the the correct categories on the right.

Can stop the attack trigger packet

No network impact if there is a sensor overload

Allows malicious traffic to pass before it can respond

Deployed in promiscuous mode

Can use stream normalization techniques

More vulnerable to network evasion techniques

Has some impact on network latency and jitter

Deployed in inline mode

IPS

Target

Target

Target

Target

IDS

Target

Target

Target

Target

Select and Place:

Drag the characteristics from the left and drop the the correct categories on the right.

- Can stop the attack trigger packet
- No network impact if there is a sensor overload
- Allows malicious traffic to pass before it can respond
- Deployed in promiscuous mode
- Can use stream normalization techniques
- More vulnerable to network evasion techniques
- Has some impact on network latency and jitter
- Deployed in inline mode

IPS

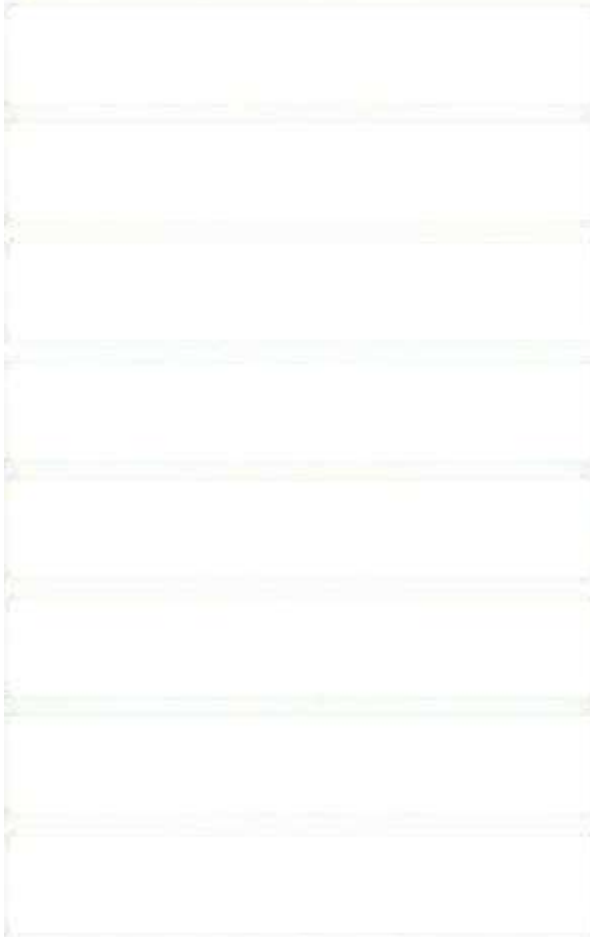
- Target
- Target
- Target
- Target

IDS

- Target
- Target
- Target
- Target

Correct Answer:

Drag the characteristics from the left and drop the the correct categories on the right.



**IPS**

Can stop the attack trigger packet

Has some impact on network latency and jitter

Deployed in inline mode

Can use stream normalization techniques

**IDS**

No network impact if there is a sensor overload

Allows malicious traffic to pass before it can respond

Deployed in promiscuous mode

More vulnerable to network evasion techniques

Section: Drag and Drop  
Explanation

Explanation/Reference:

QUESTION 125

Drag the characteristics of a static packet filter firewall rule and drop them on the right. Not all characteristics are used.

Can permit or deny traffic based on IP address

Target

Maintains connect state

Target

Can permit or deny traffic based on protocol

Target

Can permit or deny based on source and destination port

Can dynamically filter traffic based on port negotiations

Can permit or deny traffic based on fragmented packets

Select and Place:

Drag the characteristics of a static packet filter firewall rule and drop them on the right. Not all characteristics are used.

Can permit or deny traffic based on IP address

Target

Maintains connect state

Target

Can permit or deny traffic based on protocol

Target

Can permit or deny based on source and destination port

Can dynamically filter traffic based on port negotiations

Can permit or deny traffic based on fragmented packets

Correct Answer:



Drag the characteristics of a static packet filter firewall rule and drop them on the right. Not all characteristics are used.

Maintains connect state

Can permit or deny traffic based on IP address

Can permit or deny traffic based on protocol

Can permit or deny based on source and destination port

Can dynamically filter traffic based on port negotiations

Can permit or deny traffic based on fragmented packets

Section: Drag and Drop  
Explanation

Explanation/Reference:

QUESTION 126

Drag the protocol characteristics from the left and drop them on the correct protocols on the right. Not all the options on the left used

Uses TCP

Uses UDP

Uses IP protocol number 49

Separates the authentication, authorization, and accounting functions

Combinations the authentication and authorization functions

Encrypts the entire body of the packet

Encrypts the password only

Supports authorization of router commands on a per-user or per-group basis

Uses a trusted third party called the key distribution center

Uses a peer-to-peer architecture

TACACS+

RADIUS

Select and Place:

Drag the protocol characteristics from the left and drop them on the correct protocols on the right. Not all the options on the left used

Uses TCP

Uses UDP

Uses IP protocol number 49

Separates the authentication, authorization, and accounting functions

Combinations the authentication and authorization functions

Encrypts the entire body of the packet

Encrypts the password only

Supports authorization of router commands on a per-user or per-group basis

Uses a trusted third party called the key distribution center

Uses a peer-to-peer architecture

TACACS+

RADIUS

Correct Answer:

Drag the protocol characteristics from the left and drop them on the correct protocols on the right. Not all the options on the left used

Uses IP protocol number 49

Uses a trusted third party called the key distribution center

Uses a peer-to-peer architecture

#### TACACS+

Uses TCP

Separates the authentication, authorization, and accounting functions

Encrypts the entire body of the packet

Supports authorization of router commands on a per-user or per-group basis

#### RADIUS

Uses UDP

Combines the authentication and authorization functions

Encrypts the password only

Section: Drag and Drop  
Explanation

Explanation/Reference:

QUESTION 127

Match the cryptographis algorithms on the left with the type of algorithms on the right.

3DES

RSA

Diffie-Hellman

AES

IDEA

Elliptical Curve

Symmetric

Asymmetric

Select and Place:

Match the cryptographis algorithms on the left with the type of algorithms on the right.

3DES

RSA

Diffie-Hellman

AES

IDEA

Elipical Curve

Symmetric

Asymmetric

Correct Answer:

Match the cryptographis algorithms on the left with the type of algorithms on the right.


Symmetric
3DES
AES
IDEA

Asymmetric
RSA
Eliptical Curve
Diffie-Hellman

Section: Drag and Drop  
Explanation

Explanation/Reference:

### QUESTION 128

Drag the item on the left and drop them on their function on the right

Control plane

secures transit traffic through the router

Data plane

secures router access

Management plane

secures traffic destined to the router itself

Select and Place:

Drag the item on the left and drop them on their function on the right

Control plane

secures transit traffic through the router

Data plane

secures router access

Management plane

secures traffic destined to the router itself

Correct Answer:

Drag the item on the left and drop them on their function on the right

Data plane

Management plane

Control plane

Section: Drag and Drop  
Explanation

Explanation/Reference:

QUESTION 129



Drag the items from the left and drop them on their functions on the right.

False positive

A signature is not fired when non-offending traffic is captured and analyzed

False negative

A signature is not fired when offending traffic is detected

True positive

An alarm is triggered by normal traffic or a benign action

True negative

Generates an alarm when offending traffic is detected

Select and Place:

Drag the items from the left and drop them on their functions on the right.

False positive

A signature is not fired when non-offending traffic is captured and analyzed

False negative

A signature is not fired when offending traffic is detected

True positive

An alarm is triggered by normal traffic or a benign action

True negative

Generates an alarm when offending traffic is detected

Correct Answer:

Drag the items from the left and drop them on their functions on the right.


True negative

False negative

False positive

True positive

Section: Drag and Drop

Explanation

Explanation/Reference:

### QUESTION 130

Drag each AAA function on the left to the protocol that it corresponds to.

Has no option to authorize router commands

Encrypts the entire packet

Combines authentication and authorization functions

Uses TCP port 49

TACACS+

RADIUS

Select and Place:

Drag each AAA function on the left to the protocol that is corresponds to.

Has no option to authorize router commands

Encrypts the entire packet

Combines authentication and authorization functions

Uses TCP port 49

TACACS+

RADIUS

Correct Answer:

Drag each AAA function on the left to the protocol that is corresponds to.

TACACS+

Uses TCP port 49

Encrypts the entire packet

RADIUS

Combines authentication and authorization functions

Has no option to authorize router commands

Section: Drag and Drop  
Explanation

Explanation/Reference:

**QUESTION 131**

Drag each AAA function from the left and drop it on the protocol that it corresponds to on the right.

- has no option to authorize router commands
- encrypts the entire packet
- combines authentication and authorization functions
- uses TCP port 49

TACACS+

RADIUS

**Select and Place:**

Drag each AAA function from the left and drop it on the protocol that it corresponds to on the right.

- has no option to authorize router commands
- encrypts the entire packet
- combines authentication and authorization functions
- uses TCP port 49

TACACS+

RADIUS

**Correct Answer:**

Drag each AAA function from the left and drop it on the protocol that it corresponds to on the right.


### TACACS+

uses TCP port 49

encrypts the entire packet

### RADIUS

combines authentication and authorization

has no option to authorize router configuration

## Section: Drag and Drop Explanation

Explanation/Reference:

### QUESTION 132

Drag the IKE steps or modes from the left and drop them on the correct categories on the right.

quick mode

supports main or aggressive mode

negotiates the IKE policy

establishes the IPsec SAs

authenticates the peer using PSK or digital certificate

negotiates the IPsec security parameters

uses DH during the second message exchanges

can optionally perform additional DH exchanges

### IKEv1 Phase 1

Target

Target

Target

Target

### IKEv1 Phase 2

Target

Target

Target

Target

**Select and Place:**

Drag the IKE steps or modes from the left and drop them on the correct categories on the right.

- quick mode
- supports main or aggressive mode
- negotiates the IKE policy
- establishes the IPsec SAs
- authenticates the peer using PSK or digital certificate
- negotiates the IPsec security parameters
- uses DH during the second message exchanges
- can optionally perform additional DH exchanges

**IKEv1 Phase 1**

- Target
- Target
- Target
- Target

**IKEv1 Phase 2**

- Target
- Target
- Target
- Target

**Correct Answer:**

Drag the IKE steps or modes from the left and drop them on the correct categories on the right.


<b>IKEv1 Phase 1</b>
supports main or aggressive mode
negotiates the IKE policy
authenticates the peer using PSK or digital signatures
uses DH during the second message exchange
<b>IKEv1 Phase 2</b>
quick mode
establishes the IPsec SAs
negotiates the IPsec security parameters
can optionally perform additional DH exchanges

**Section: Drag and Drop**  
**Explanation**

**Explanation/Reference:**

**QUESTION 133**

Drag the items from the left that are part of a secure network lifecycle and drop them in the spaces on the right. Not all items are used.

- initiation
- implementation
- acquisition and development
- disposition
- staff roles and responsibilities
- operations and management
- incident response policy

- Target
- Target
- Target
- Target
- Target

**Select and Place:**

Drag the items from the left that are part of a secure network lifecycle and drop them in the spaces on the right. Not all items are used.

- initiation
- implementation
- acquisition and development
- disposition
- staff roles and responsibilities
- operations and management
- incident response policy

- Target
- Target
- Target
- Target
- Target

**Correct Answer:**



Drag the items from the left that are part of a secure network lifecycle and drop them in the spaces on the right. Not all items are used.

staff roles and responsibilities
incident response policy

initiation
implementation
acquisition and development
disposition
operations and management

**Section: Drag and Drop**  
**Explanation**

**Explanation/Reference:**

**QUESTION 134**

Drag the CLI Configuration to implement a zone-based policy firewall from the left and drop them in the correct order on the right.

policy map
service policy
class map


**Select and Place:**

Drag the CLI Configuration to implement a zone-based policy firewall from the left and drop them in the correct order on the right.

policy map
service policy
class map


**Correct Answer:**

Drag the CLI Configuration to implement a zone-based policy firewall from the left and drop them in the correct order on the right.


**Section: Drag and Drop**  
**Explanation**

**Explanation/Reference:**

**QUESTION 135**

Drag the disaster recovery concepts from the left and drop them on their definitions on the right.

recovery point objective	the age of the data you want the ability to recover in event of a system outage
maximum tolerable downtime	the amount of downtime accepted for a system
recovery time objective	the amount of downtime accepted for a business process outage

**Select and Place:**

Drag the disaster recovery concepts from the left and drop them on their definitions on the right.

recovery point objective	the age of the data you want the ability to recover in event of a system outage
maximum tolerable downtime	the amount of downtime accepted for a system
recovery time objective	the amount of downtime accepted for a business process outage

**Correct Answer:**

Drag the disaster recovery concepts from the left and drop them on their definitions on the right.


recovery point objective
recovery time objective
maximum tolerable downtime

**Section: Drag and Drop**  
**Explanation**

**Explanation/Reference:**

**QUESTION 136**

Drag the items from the left and drop them on their functions on the right.

control plane
data plane
management plane

secures transit traffic through the network
secures router access
secures traffic destined to the router

**Select and Place:**

Drag the items from the left and drop them on their functions on the right.

control plane
data plane
management plane

secures transit traffic through the network
secures router access
secures traffic destined to the router

**Correct Answer:**

Drag the items from the left and drop them on their functions on the right.


data plane
management plane
control plane

**Section: Drag and Drop**  
**Explanation**

**Explanation/Reference:**

**QUESTION 137**

Drag the characteristics of a static packet filter firewall rule and drop them on the right. Not all characteristics are used.

- can permit or deny traffic based on IP address
- maintains connection state
- can permit or deny traffic based on protocol
- can permit or deny traffic based on source and destination ports
- can dynamically filter traffic based on port negotiations
- can permit or deny traffic based on fragmented packets

- Target
- Target
- Target

**Select and Place:**

Drag the characteristics of a static packet filter firewall rule and drop them on the right. Not all characteristics are used.

- can permit or deny traffic based on IP address
- maintains connection state
- can permit or deny traffic based on protocol
- can permit or deny traffic based on source and destination ports
- can dynamically filter traffic based on port negotiations
- can permit or deny traffic based on fragmented packets

- Target
- Target
- Target

**Correct Answer:**

Drag the characteristics of a static packet filter firewall rule and drop them on the right. Not all characteristics are used.

maintains connection state

can dynamically filter traffic based on port negotiations

can permit or deny traffic based on fragmented packets

can permit or deny traffic based on

can permit or deny traffic based on source a

can permit or deny traffic based o

**Section: Drag and Drop**  
**Explanation**

**Explanation/Reference:**

**QUESTION 138**

Drag the signature engines from the left and drop them on their characteristics on the right. Not all engines are used.

other

string

atomic

multi-string

service

inspects and analyzes things such as HTTP

examines simple packets

uses regular expression-based patte

**Select and Place:**

Drag the signature engines from the left and drop them on their characteristics on the right. Not all engines are used.

- other
- string
- atomic
- multi-string
- service

- inspects and analyzes things such as HTTP
- examines simple packets
- uses regular expression-based patterns

**Correct Answer:**

Drag the signature engines from the left and drop them on their characteristics on the right. Not all engines are used.

- other
- 
- 
- multi-string
- 

- service
- atomic
- string

**Section: Drag and Drop**  
**Explanation**

**Explanation/Reference:**



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