Vendor: CISCO

Exam Code: 640-554

Exam Name: Implementing Cisco IOS Network Security
QUESTION 1
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

Answer: C

QUESTION 2
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

Answer: C

QUESTION 3
Refer to the exhibit.

Which traffic is permitted by this ACL?

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

Answer: C

QUESTION 4
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.

Answer: D

QUESTION 5
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 BDPU guard.

Answer: C

QUESTION 6
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

Answer: A

**QUESTION 7**
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.

Answer: AD

**QUESTION 8**
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+

**Answer:** C

**QUESTION 9**
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

**Answer:** C

**QUESTION 10**
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

**Answer:** C

**QUESTION 11**
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.

Answer: A

QUESTION 12
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

Answer: B

QUESTION 13
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

Answer: AC

QUESTION 14
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  

Answer: BD  

QUESTION 15  
Refer to the exhibit.  

```
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)#
```

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.)  

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

Answer: BCDE

QUESTION 16
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.

Answer: B

QUESTION 17
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

Answer: C

QUESTION 18
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

**Answer:** B

**QUESTION 19**
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

**Answer:** AE