Vendor: Cisco

Exam Code: 210-260

Exam Name: Implementing Cisco Network Security

QUESTION 1
Which three ESP fields can be encrypted during transmission? (Choose three.)

A. Security Parameter Index
B. Sequence Number
C. MAC Address
D. Padding
E. Pad Length
F. Next Header

Correct Answer: DEF
Explanation

QUESTION 2
What mechanism does asymmetric cryptography use to secure data?

A. a public/private key pair
B. shared secret keys
C. an RSA nonce
D. an MD5 hash

Correct Answer: A
Explanation

QUESTION 3
Whit which type of Leyer 2 attack can you "do something" for one host:

A. MAC spoofing
B. CAM overflow....

Correct Answer: A
Explanation

QUESTION 4
Refer to the exhibit.

```
R1#show snmp
Chassis: FTX123456789
0 SNMP packets input
   6 Bad SNMP version errors
   3 Unknown community name
   9 Illegal operation for community name supplied
   4 Encoding errors
   2 Number of requested variables
   0 Number of altered variables
   98 Get-request PDUs
   12 Get-next PDUs
   2 Set-request PDUs
   0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
   0 Too big errors (Maximum packet size 1500)
   0 No such name errors
   0 Bad values errors
   0 General errors
   31 Response PDUs
   1 Trap PDUs
```

How many times was a read-only string used to attempt a write operation?

A. 9
B. 6
C. 4
D. 3
E. 2

Correct Answer: A
Explanation

QUESTION 5
Which feature allows a dynamic PAT pool to select the next address in the PAT pool instead of the next port of an existing address?

A. next IP
B. round robin
C. dynamic rotation
D. NAT address rotation

Correct Answer: B
Explanation

QUESTION 6
Which label is given to a person who uses existing computer scripts to hack into computers lacking the expertise to write their own?

A. white hat hacker
B. hacktivist
C. phreaker
D. script kiddy

Correct Answer: D
Explanation

QUESTION 7
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
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080 8bc994.shtml

Zone-Based Policy Firewall Actions
ZFW provides three actions for traffic that traverses from one zone to another:
Drop -- This is the default action for all traffic, as applied by the "class class-default" that terminates every inspect-type policy-map. Other class-maps within a policy-map can also be configured to drop unwanted traffic.
Traffic that is handled by the drop action is "silently" dropped (i.e., no notification of the drop is sent to the relevant end-host) by the ZFW, as opposed to an ACL's behavior of sending an ICMP "host unreachable" message to the host that sent the denied traffic. Currently, there is not an option to change the "silent drop" behavior. The log option can be added with drop for syslog notification that traffic was dropped by the firewall.

Pass -- This action allows the router to forward traffic from one zone to another. The pass action does not track the state of connections or sessions within the traffic. Pass only allows the traffic in one direction. A corresponding policy must be applied to allow return traffic to pass in the opposite direction. The pass action is useful for protocols such as IPSec ESP, IPSec AH, ISAKMP, and other inherently secure protocols with predictable behavior. However, most application traffic is better handled in the ZFW with the inspect action.

Inspect--The inspect action offers state-based traffic control. For example, if traffic from the private zone to the Internet zone in the earlier example network is inspected, the router maintains connection or session information for TCP and User Datagram Protocol (UDP) traffic. Therefore, the router permits return traffic sent from Internet-zone hosts in reply to private zone connection requests. Also, inspect can provide application inspection and control for certain service protocols that might carry vulnerable or sensitive application traffic.

Audit-trail can be applied with a parameter-map to record connection/session start, stop, duration, the data volume transferred, and source and destination addresses.

QUESTION 8
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
Explanation

QUESTION 9
Which statement about a PVLAN isolated port configured on a switch is true?

A. The isolated port can communicate only with the promiscuous port.
B. The isolated port can communicate with other isolated ports and the promiscuous port.
C. The isolated port can communicate only with community ports.
D. The isolated port can communicate only with other isolated ports.

Correct Answer: A
Explanation

QUESTION 10
Which statement about Cisco ACS authentication and authorization is true?

A. ACS servers can be clustered to provide scalability.
B. ACS can query multiple Active Directory domains.
C. ACS uses TACACS to proxy other authentication servers.
D. ACS can use only one authorization profile to allow or deny requests.

Correct Answer: A
Explanation

QUESTION 11
Refer to the exhibit.

```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mab dotlx webauth
authentication priority dotlx mab
authentication port-control auto
dotlx pae authenticator
```

If a supplicant supplies incorrect credentials for all authentication methods configured on the switch, how will the switch respond?

A. The supplicant will fail to advance beyond the webauth method.
B. The switch will cycle through the configured authentication methods indefinitely.
C. The authentication attempt will time out and the switch will place the port into the unauthorized state.
D. The authentication attempt will time out and the switch will place the port into VLAN 101.

Correct Answer: A
Explanation

QUESTION 12
What configure mode you used for the command ip ospf authentication-key c1$c0?

A. global
B. privileged
C. in-line
D. Interface

Correct Answer: D
Explanation

Explanation/Reference:
Explanation: ip ospf authentication-key is used under interface configuration mode, so it's in interface level, under global configuration mode. If it asks about interface level then choose that.
interface Serial0
ip address 192.16.64.1 255.255.25

QUESTION 13
Which two features are commonly used CoPP and CPPr to protect the control plane? (Choose two.)

A. QoS
B. traffic classification
C. access lists
D. policy maps
E. class maps
F. Cisco Express Forwarding

Correct Answer: AB
Explanation

QUESTION 14
What is one requirement for locking a wired or wireless device from ISE?

A. The ISE agent must be installed on the device.
B. The device must be connected to the network when the lock command is executed.
C. The user must approve the locking action.
D. The organization must implement an acceptable use policy allowing device locking.

Correct Answer: A
Explanation

QUESTION 15
Which three statements are characteristics of DHCP Spoofing? (choose three)

A. Arp Poisoning
B. Modify Traffic in transit
C. Used to perform man-in-the-middle attack
D. Physically modify the network gateway
E. Protect the identity of the attacker by masking the DHCP address
F. can access most network devices

Correct Answer: ABC
Explanation

QUESTION 16
Which statement correctly describes the function of a private VLAN?

A. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains
B. A private VLAN partitions the Layer 3 broadcast domain of a VLAN into subdomains
C. A private VLAN enables the creation of multiple VLANs using one broadcast domain
D. A private VLAN combines the Layer 2 broadcast domains of many VLANs into one major broadcast domain

Correct Answer: A

Explanation

QUESTION 17
which feature allow from dynamic NAT pool to choose next IP address and not a port on a used IP address?

A. next IP
B. round robin
C. Dynamic rotation
D. Dynamic PAT rotation

Correct Answer: B
Explanation

QUESTION 18
Which type of encryption technology has the broadcast platform support?

A. Middleware
B. Hardware
C. Software
D. File-level

Correct Answer: C
Explanation

QUESTION 19
When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?

A. Deny the connection inline.
B. Perform a Layer 6 reset.
C. Deploy an antimalware system.
D. Enable bypass mode.

Correct Answer: A
Explanation

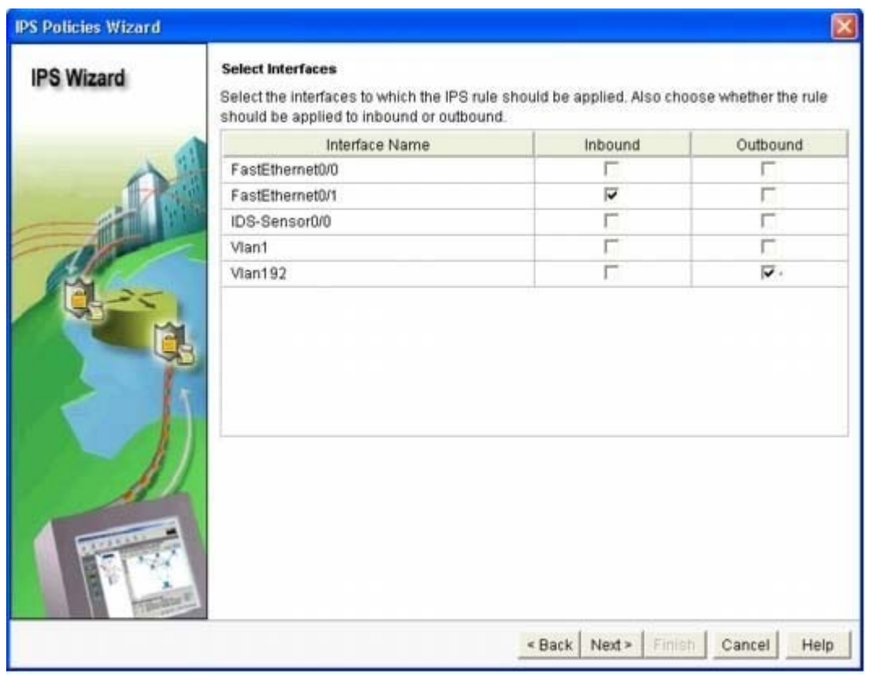
QUESTION 20
Which four tasks are required when you configure Cisco IOS IPS using the Cisco Configuration Professional IPS wizard? (Choose four.)

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
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_pa per0900aecd8066d265.html

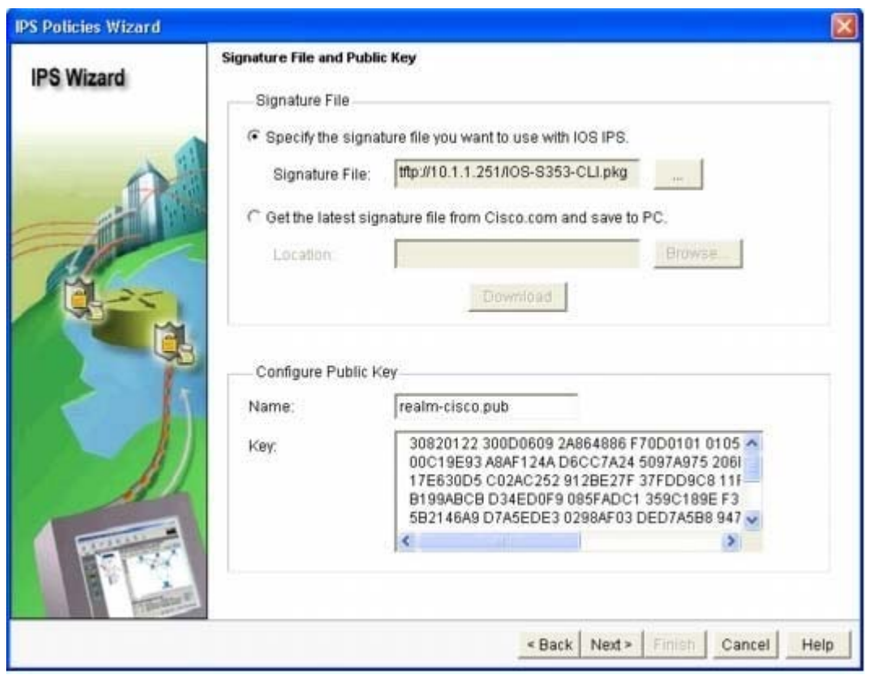
Step 11. At the `Select Interfaces' screen, select the interface and the direction that IOS IPS will be applied to, then click `Next' to continue.



Step 12. At the `IPS Policies Wizard' screen, in the `Signature File' section, select the first radio button "Specify the signature file you want to use with IOS IPS", then click the "..." button to bring up a dialog box to specify the location of the signature package file, which will be the directory specified in Step 6. In this example, we use tftp to download the signature package to the router.

Step 13. In the `Configure Public Key' section, enter `realm-cisco.pub' in the `Name' text field, then copy and paste the following public key's key-string in the `Key' text field. This public key can be downloaded from

Cisco.com at: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup. Click `Next' to continue.
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101 00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16 17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7
DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35 FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001



QUESTION 21
Which ports need to be active for AAA server and a Microsoft server to permit Active Directory authentication?

A. 445 and 389
B. 888 and 3389
C. 636 and 4445
D. 363 and 983

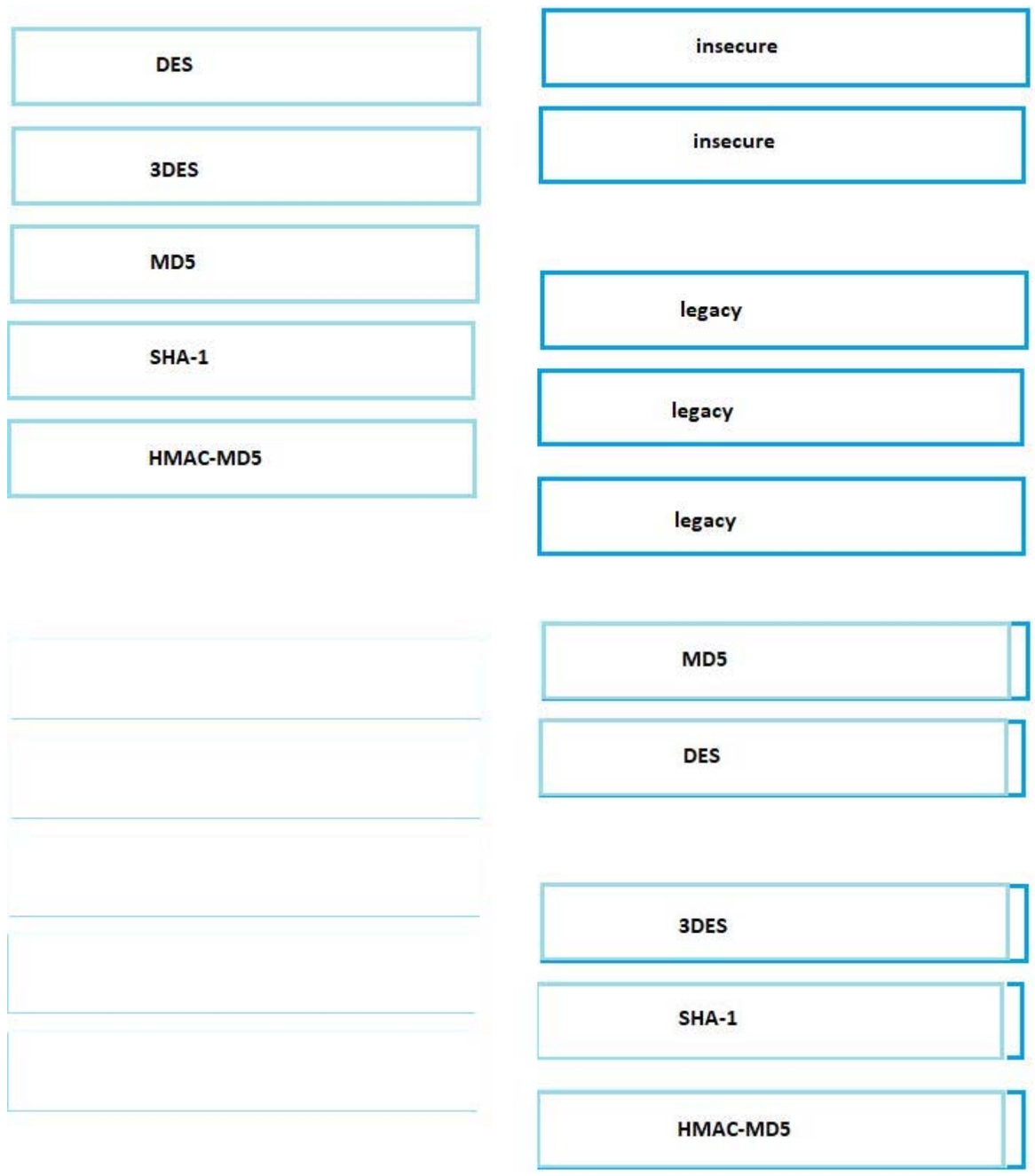
Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 22
DRAG DROP

Drag the hash or algorithm from the left column to its appropriate category on the right.

Select and Place:



Correct Answer:

Explanation

Explanation/Reference:

QUESTION 23
If a switch receives a superior BPDU and goes directly into a blocked state, what mechanism must be in use?

A. root guard
B. EtherChannel guard
C. loop guard
D. BPDU guard

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 24
Which two are valid types of VLANs using PVLANs? (Choose two.)

A. Backup VLAN
B. Secondary VLAN
C. Promiscuous VLAN
D. Community VLAN
E. Isolated VLAN

Correct Answer: DE
Explanation

Explanation/Reference:

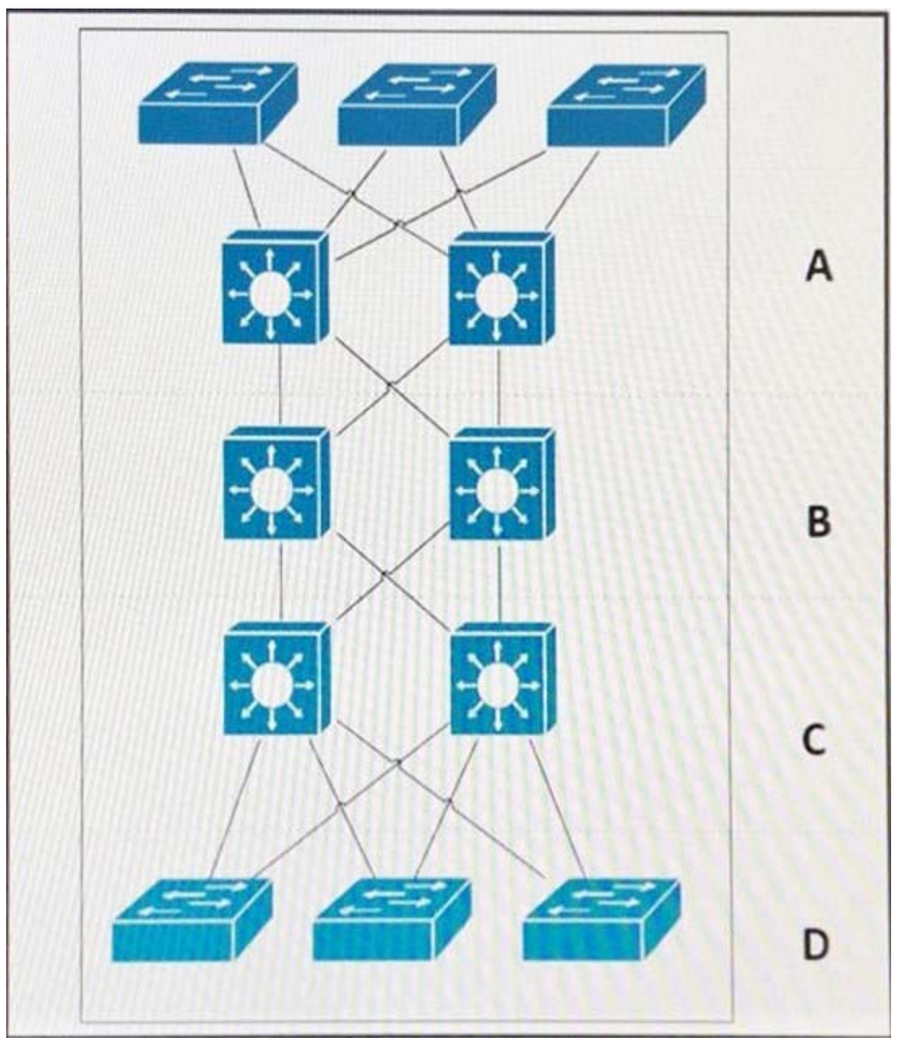
QUESTION 25
Which two are the default settings for port security? (Choose two.)

A. Violation is Protect
B. Maximum number of MAC addresses is 1
C. Violation is Restrict
D. Violation is Shutdown
E. Maximum number of MAC addresses is 2

Correct Answer: BD
Explanation

Explanation/Reference:

QUESTION 26
Refer to the exhibit.



Which area represents the data center?

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

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 27
Refer to the exhibit.

```
ASA#show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic LOCALUSERS GLBPOOL
        translate_hits=3218, untranslate_hits=0
2 (inside) to (outside) source static REAL_SERVER GLB_SERVER
        translate_hits=0, untranslate_hits= 108764

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static SSL_SERVER 88.1.115.1
        translate_hits=0, untranslate_hits=0

Manual NAT Policies (Section 3)
1 (inside) to (outside) source dynamic NEW_USERS GLBPOOL2
        translate_hits=0, untranslate_hits=0
```

A network security administrator checks the ASA firewall NAT policy table with the **show nat** command.
Which statement is false?

A. First policy in the Section 1 is dynamic nat entry defined in the object configuration.
B. There are only reverse translation matches for the REAL_SERVER object.
C. NAT policy in Section 2 is a static entry defined in the object configuration.
D. Translation in Section 3 is used when a connection does not match any entries in first two sections.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 28
Which two are characteristics of RADIUS? (Choose two.)

A. Uses TCP ports 1812/1813

B. Uses UDP port 49
C. Encrypts only the password between user and server
D. Uses TCP port 49
E. Uses UDP ports 1812/1813

Correct Answer: CE
Explanation

Explanation/Reference:

QUESTION 29
Which two types of firewalls work at layer 4 and above? (Choose two.)

A. Application level firewall
B. Circuit-level gateway
C. Static packet filter
D. Network Address Translation
E. Stateful inspection

Correct Answer: AB
Explanation

Explanation/Reference:

QUESTION 30
When setting up a site-to-site VPN with PSK authentication on a Cisco router, which two elements must be configured under crypto map? (Choose two.)

A. nat
B. peer
C. pfs
D. reverse-route
E. transform-set

Correct Answer: BE
Explanation

Explanation/Reference:

QUESTION 31
Which two commands are used to implement Resilient IOS Configuration? (Choose two.)

A. copy flash:/ios.bin tftp
B. copy running-config tftp
C. copy running-config startup-config
D. secure boot-image
E. secure boot-config

Correct Answer: DE
Explanation

Explanation/Reference:

QUESTION 32
Which two events would cause the state table of a stateful firewall to be updated? (Choose two.)

A. when a connection’s timer has expired within the state table
B. when a connection is created
C. when rate-limiting is applied
D. when a packet is evaluated against the outbound access list and is denied
E. when an outbound packet is forwarded to the outbound interface

Correct Answer: AB
Explanation

Explanation/Reference:

QUESTION 33
Which IPSec mode is used to encrypt traffic directly between a client and a server VPN endpoint?

A. transport mode
B. tunnel mode
C. aggressive mode
D. quick mode

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 34
On an ASA, the policy that indicates that traffic should not be translated is often referred to as which of the following?

A. NAT zero
B. NAT forward
C. NAT null
D. NAT allow

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 35
What is true of an ASA in transparent mode?

A. It requires a management IP address
B. It allows the use of dynamic NAT
C. It requires an IP address for each interface
D. It supports OSPF

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 36
Which component offers a variety of security solutions, including firewall, IPS, VPN, antispyware, antivirus, and antiphishing features?

A. Cisco IOS router
B. Cisco ASA 5500-X Series Next Gen. Security appliance
C. Cisco 4200 series IPS appliance
D. Cisco ASA 5500 series security appliance

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 37
How does a zone pair handle traffic if the policy definition of the zone pair is missing?

A. It permits all traffic without logging.
B. It drops all traffic.
C. It inspects all traffic.
D. It permits and logs all traffic.

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 38
Which command do you enter to configure your firewall to conceal internal addresses?

A. no ip logging facility
B. no ip directed-broadcast
C. no ip inspect
D. no proxy-arp
E. no ip source-route
F. no ip inspect audit-trail

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 39
Which IOS command do you enter to test authentication against a AAA server?

A. aaa authentication enable default test group tacacs+
B. dialer aaa suffix <suffix> password <password>
C. ppp authentication chap pap test
D. test aaa-server authentication dialergroup username <user> password <password>

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 40
Which technology can block a non-malicious program that is run from a local computer that has been disconnected from the network?

A. antivirus software
B. firewall
C. host IPS
D. network IPS

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 41
Which protocol offers data Integrity, encryption, authentication, and anti-replay functions for IPSec VPN?

A. AH protocol
B. IKEv2 Protocol
C. IKEv1 Protocol
D. ESP protocol

Correct Answer: D
Explanation

Explanation/Reference:

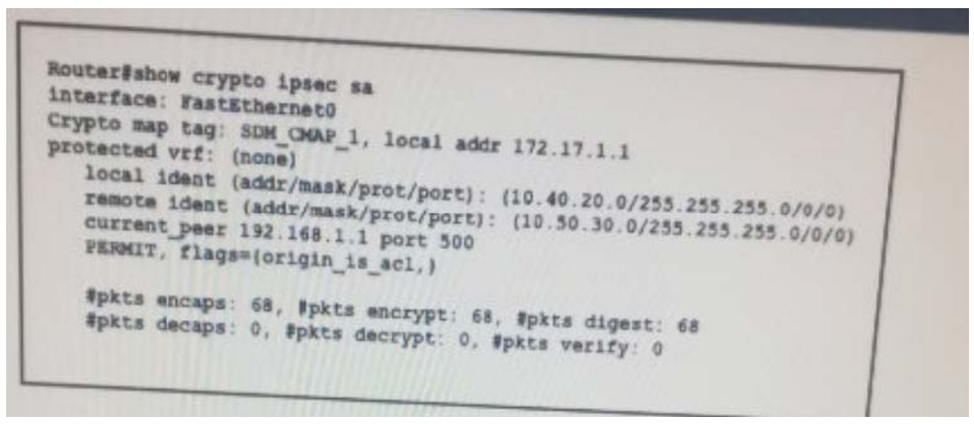
QUESTION 42
By default, how does a zone-based firewall handle traffic to and from the self zone?

A. It permits all traffic without inspection.
B. It inspects all traffic to determine how it is handled.
C. It permits all traffic after inspection.
D. It drops all traffic.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 43
Refer to the exhibit.



For which reason is the tunnel unable to pass traffic?

A. UDP port 500 is blocked.
B. The IP address of the remote peer is incorrect.
C. The tunnel is failing to receive traffic from the remote peer.
D. The local peer is unable to encrypt the traffic.

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 44
Which two statements about the self zone on a Cisco zone-based policy firewall are true? (Choose Two)

A. Multiple interfaces can be assigned to the self zone.
B. Traffic entering the self zone must match a rule.
C. Zone pairs that include the self zone apply to traffic transiting the device.
D. It can be either the source zone or the destination zone.
E. It supports stateful inspection for multicast traffic.

Correct Answer: DE
Explanation

Explanation/Reference:

QUESTION 45
What does the command crypto isakmp nat-traversal do?

A. Enables udp port 4500 on all IPsec enabled interfaces
B. rebooting the ASA the global command

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 46
Which quantifiable item should you consider when your organization adopts new technologies?

A. threats
B. vulnerability
C. risk
D. exploits

Correct Answer: C
Explanation

Explanation/Reference:

QUESTION 47
Which IPS mode is less secure than other options but allows optimal network throughput?

A. Promiscuous mode
B. inline mode
C. transparent mode
D. inline-bypass mode

Correct Answer: A
Explanation

Explanation/Reference:

QUESTION 48
Which option is a key security component of an MDM deployment?

A. Using MS-CHAPv2 as the primary EAP method.
B. Using self-signed certificates to validate the server.
C. Using network-specific installer packages
D. Using an application tunnel by default.

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 49
Which command should be used to enable AAA authentication to determine if a user can access the privilege command level?

A. aaa authentication enable level
B. aaa authentication enable default local
C. aaa authentication enable method default
D. aaa authentication enable local

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 50
Which type of firewall can serve as the intermediary between a client and a server?

A. Application firewall
B. Stateless firewall
C. Personal firewall
D. Proxy firewall

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 51
Which two characteristics of a PVLAN are true?

A. Isolated ports cannot communicate with other ports on the same VLAN.
B. They require VTP to be enabled in server mode.
C. Promiscuous ports can communicate with PVLAN ports.
D. PVLAN ports can be configured as EtherChannel ports.
E. Community ports have to be a part of the trunk.

Correct Answer: CE
Explanation

Explanation/Reference:

QUESTION 52
Which two features are supported in a VRF-aware software infrastructure before VRF-lite? (Choose two)

A. priority queuing
B. EIGRP
C. multicast
D. WCCP
E. fair queuing

Correct Answer: BC
Explanation

Explanation/Reference:

QUESTION 53
Which two primary security concerns can you mitigate with a BYOD solution? (Choose two)

A. Schedule for patching the device.
B. **C**ompliance with applicable policies.
C. Device lagging and inventory.
D. Connections to public Wi-Fi networks.
E. Securing access to a trusted corporate network.

Correct Answer: BE

Explanation

Explanation/Reference:

QUESTION 54
Which IDS/IPS solution can monitor system processes and resources?

A. IDS
B. HIPS
C. PROXY
D. IPS

Correct Answer: B
Explanation

Explanation/Reference:

QUESTION 55
Which type of attack can exploit design flaws in the implementation of an application without going noticed?

A. Volume-based DDoS attacks.
B. Application DDoS flood attacks.
C. DHCP starvation attacks.
D. Low-rate DoS attacks.

Correct Answer: D
Explanation

Explanation/Reference:

QUESTION 56
Which type of address translation supports the initiation of communications bidirectionally?

A. multi-session PAT
B. static NAT
C. dynamic PAT
D. dynamic NAT

Correct Answer: D
Explanation

Explanation/Reference: