

ActualCollection

WELCOME TO ACTUALCOLLECTION

ActualCollection dumps, higher pass rate



ActualCollection is a website offering the latest and valid actual exam dump to make you go through the actual test with a high score.



Quality and Value

ActualCollection Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.



Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.



Easy to Pass

If you prepare for the exams using our ActualCollection testing engine, it is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.



Try Before Buy

ActualCollection offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

<http://www.actualcollection.com>

Actual dumps collection, higher pass rate

Exam : **400-251**

Title : CCIE Security Written Exam
(v5.0)

Vendor : Cisco

Version : DEMO

NO.1 Which statement is true for email processing pipeline in Cisco Email Security Appliance (ESA)?

- A. VOF (Virus Outbreak Filters) scanning is done before Graymail scanning
- B. Anti-Spam scanning is done before Anti-Virus scanning
- C. Content filters are used before Message filters in ESA pipeline
- D. VOF (Virus Outbreak Filters) scanning is done at very beginning of the work-queue part of email pipeline

Answer: B

NO.2 If a packet capture is taken between ISE and an endpoint to capture an EAP-TLS session, you will be able to see:

- A. Certificates from ISE and the endpoint
- B. Certificates from ISE only
- C. Certificate and associated private keys from endpoint only
- D. Certificate and associated private keys from ISE only

Answer: A

NO.3 Which attribute cannot be used in Mobile Device Management (MDM) Authorization policy?

- A. DaysSinceLastCheckin
- B. MDMServerName
- C. NetworkAccess:EAPChaningResult
- D. DeviceRegistrationStatus
- E. MDMServerReachable

Answer: C

NO.4 Which five next-generation features are available on the Cisco NGFWs compared to traditional stateful firewalls? (Choose five)

- A. Net Flow Analytics
- B. IPS
- C. Advanced Malware Protection
- D. TLS Decryption
- E. Security Intelligence
- F. Identity and Access Management
- G. URL Filtering

Answer: B,C,D,E,G

NO.5 Which Cisco NGFW interface mode can detect intrusion attempts inline but can't drop malicious traffic inline?

- A. Transparent
- B. inline Pair
- C. Inline Tap
- D. ERSPAN
- E. Passive

Answer: C

NO.6 ISE can be integrated with an MDM to ensure that only registered devices are allowed on the network, and use the MDM to push policies to the device. Devices can go in and out of compliance either due to policy changes on the MDM server, or another reason. Consider a device that has already authenticated on the network, and stays connected, but fails out of compliance. Which action can you take to ensure that a noncompliant device is checked periodically and re-assessed before allowing access to the network?

- A. Fire-AMP connector scan can be used to relay posture information to ISE via FireAMP cloud
- B. Enable Change of authorization on ISE
- C. The MDM agent automatically disconnects the device from the network when it is noncompliant
- D. Enable Period compliance checking on ISE
- E. The MDM agent periodically sends a packet with compliance info that the wireless controller can be used to limit network access
- F. Enable change of authorization on MDM

Answer: B

NO.7 Which of the following Policies belongs to cisco Web Security Appliance policy types?

- A. SSL Inspection Policy
- B. Routing Policy
- C. DNS Policy
- D. VOF Policy

Answer: B

NO.8 Which are three similarities between containers and virtual machines? (Choose three)

- A. private space for processing
- B. cannot mount file systems
- C. public interface
- D. private network interface and IP address
- E. share host system kernel
- F. allow custom routes

Answer: A,D,E

NO.9 Refer to the exhibit.

```
R3:
ip vrf mgmt
!
crypto keyring CCIE vrf mgmt
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
!
crypto isakmp policy 33
  encr 3des
  authentication pre-share
  group 2
  lifetime 600
!
crypto ipsec transform-set site_ab esp-aes 256 esp-sha-hmac
  mode tunnel
!
crypto ipsec profile site_a
  set security-association lifetime seconds 600
  set transform-set site_ab
!
crypto gdoi group group_a
  identity number 100
  server local
  rekey algorithm aes 256
```

```

rekey lifetime seconds 300
rekey retransmit 10 number 3
rekey authentication mypubkey rsa cciekey
rekey transport unicast
sa ipsec 1
  profile site_a
  match address ipv4 site_a
  replay counter window-size 64
  no tag
address ipv4 10.1.20.3

```

```

interface GigabitEthernet3
ip address 10.1.20.3 255.255.255.0

```

```

ip access-list extended site_a
permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255

```

R3 is the key server in a GETVPN VRF-Aware implementation. The group members for the site_a register with key server via interface address 10.1.20.3/24 in the management VRF "mgmt". The GROUP ID for the site_a is 100 to retrieve group policy and keys from the key server. The traffic to be encrypted by the site_a group members is between 192.186.4.0/24 and 192.186.5.0/24. The preshared key used by the group members to authenticate with the key server is "cisco". It has been reported that group members cannot perform encryption for the traffic defined in the group policy of site_a. Which two possible issues are true? (Choose two.)

- A. incorrect encryption in ISAKMP policy
- B. incorrect encryption traffic defined in the group policy
- C. The registration interface is not part of management VRF "mgmt"
- D. incorrect security-association time in the IPsec profile
- E. incorrect password in the keyring configuration
- F. The GDOI group has an incorrect local server address

Answer: B,C

NO.10 Which statement is correct about Cisco Web Security Appliance (WSA)?

- A. WSA policies can be configured using GUI interface only
- B. WSA can have only one routing table
- C. WSA can not decrypt HTTPS traffic
- D. WSA does not offer out-of-bound Management capability

Answer: A

NO.11 Which of the following statements is true about Cisco Email Security Appliance (ESA)?

- A. Private Listener has only RAT Table
- B. Private Listener has only HAT Table
- C. Cisco Email Security Appliance cant have Management and Data traffic bound to the same port (physical/ or virtual when we speak about vESA)
- D. Private Listener always has HAT and RAT tables

Answer: B

NO.12 Which tool or program is a version control system?

- A. Git
- B. Travis CI
- C. Logstash
- D. Jenkins
- E. SmartC

Answer: A