



# 400-251<sup>Q&As</sup>

CCIE Security Written

## Pass Cisco 400-251 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/400-251.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco  
Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers





### QUESTION 1

Which two statements about AMP Threat Grid are true? (Choose two)

- A. It can transmit suspected malware to the public AMP threat Grid cloud for deeper analysis
- B. It provides two separate on premises appliances to support powerful malware analysis and threat intelligence features.
- C. It provides dynamic analysis reports and generates threat scores
- D. It supports real time threat and behavioral analysis
- E. It can be installed on individual endpoints to inspect local files for malware
- F. It can act as an anonymized proxy to transport endpoint prevent data to the public AMP Threat Grid cloud for threat detection

Correct Answer: BC

---

### QUESTION 2

Which statement about securing TLS connections on the ESA is true?

- A. The pre-configured demonstration certificate installed on the ESA can establish a secure, verifiable TLS connection
- B. If you apply a certificate to an ESA in cluster mode, it is automatically propagated to the other ESAs in the cluster
- C. Self-signed certificates and CA certificates can provide a verifiable connection. The ESA supports certificates in PKCS#7 and PKCS#12 format
- D. Certificates that are imported to secure RLS connections can also be used by other services on the ESA including LDAP and HTTPS
- E. The ESA encrypts all messages with a certificate before sending them over a TLS connection.
- F. After a certificate is applied to an ESA Cluster using centralized management, new devices added to the cluster automatically adopt the existing certificate.

Correct Answer: A

---

### QUESTION 3

Which are three similarities between containers and virtual machines? (Choose three)

- A. private space for processing



- B. public interface
- C. can not mount file systems
- D. share host system kernel
- E. private network interface and IP address
- F. allow custom routes

Correct Answer: AEF

---

#### QUESTION 4

Which two characteristic of a IoT network are true? (Choose two)

- A. IoT network must be designed for low-powered devices
- B. The transmission rate in an IoT network is consistent
- C. IoT networks are 100% reliable
- D. IoT networks use IS-IS for routing
- E. IoT networks are bandwidth constrained

Correct Answer: AE

---

#### QUESTION 5

Which two functionalities does the Threat Grid for the Cisco Meraki MX use of Sandbox technology allow?

- A. Deploy decoys for the malware to target
- B. Know what changes the malware is making
- C. Locate where the malware originated from
- D. To encrypt packet without an agent
- E. To decrypt packet without an agent
- F. Understanding of which processes the malware is affecting

Correct Answer: DF

---

#### QUESTION 6



Which statement is true about Remote Triggered Black Hole Filtering feature (RTBH)?

- A. It drops malicious traffic at the customer edge router by forwarding it to a Null0 interface
- B. In RTBH filtering, the trigger device redistributes static route to the iBGP peers
- C. The Null0 interface used for filtering able to receive the traffic but never forwards it
- D. It works in conjunction with QoS to drop the traffic that has a less priority
- E. It helps mitigate DDoS attack based only on source address
- F. In RTBH filtering the trigger device is always an ISP edge router

Correct Answer: B

---

#### QUESTION 7

Which three VSA attributes are present in a RADIUS WLAN Access-Accept packet? (Choose three)

- A. Tunnel-Private-Group-ID
- B. Tunnel-Type
- C. SSID
- D. EAP-Message
- E. LEAP Session-Key
- F. Authorization-Algorithm-Type

Correct Answer: CEF

---

#### QUESTION 8

Refer to the exhibit. One of the Windows machines in your network is experiencing a Dot1x authentication failure. Windows machines are setup to acquire an IP address from the DHCP server configured on the switch, which is supposed to hand over IP addresses from the 50.1.1.0/24 network, and forward AAA requests to the radius server at

161.1.7.14 using shared key "cisco". Knowing that interface Gi0/2 on switch may receive authentication requests from other devices and looking at the provided switch configuration, what could be the possible cause of this failure?

```
aaa new model
aaa authentication login NO_AUTH none
aaa authentication login vty local
aaa authentication dot1x default group radius
aaa authentication network default group radius
aaa accounting dot1x default start-stop group radius
! username cisco privilege 15 password 0 cisco
dot1x system-auth-control
! interface GigabitEthernet0/2
switchport mode access
ip access-group Pre-Auth in
authentication host-mode multi-auth
authentication open
authentication port-control auto
dot1x pae authenticator
! vlan 50
interface Vlan50
ip address 50.1.1.1 255.255.255.0
! ip dhcp excluded-address 50.1.1.1
ip dhcp pool pc-pool
network 50.1.1.0 255.255.255.0
default-router 50.1.1.1
! ip access-list extended Pre-Auth
permit udp any eq bootpc any eq bootps
deny ip any any
! radius server ccie address ipv4 161.1.7.14
auth-port 1645 acct-port 1646
key cisco
! line con 0
login authentication NO_AUTH
line vty 0 4
login
```



authentication vty

- A. an incorrect dhcp pool is configured
- B. aaa network authorization is not configured
- C. an incorrect pre-authentication acl is configured
- D. authentication port-control is not set on interface gi0/2
- E. an incorrect radius server addresss is defined
- F. aaa login authentication is not configured
- G. authentication is not enabled on interface gi0/2

Correct Answer: B

---

#### QUESTION 9

Which requirement for the FTD high availability setup is true?

- A. Units must be in different domains in FMC
- B. Units must have DHCP configured for the Interfaces
- C. Units must not have the same major, minor, and maintenance software version running on them
- D. Units can have any uncommitted changes on FMC and need not be fully deployed
- E. Units must be synchronized using the same NTP source.
- F. Units must be configured in routed mode
- G. Units must be configured in transparent mode

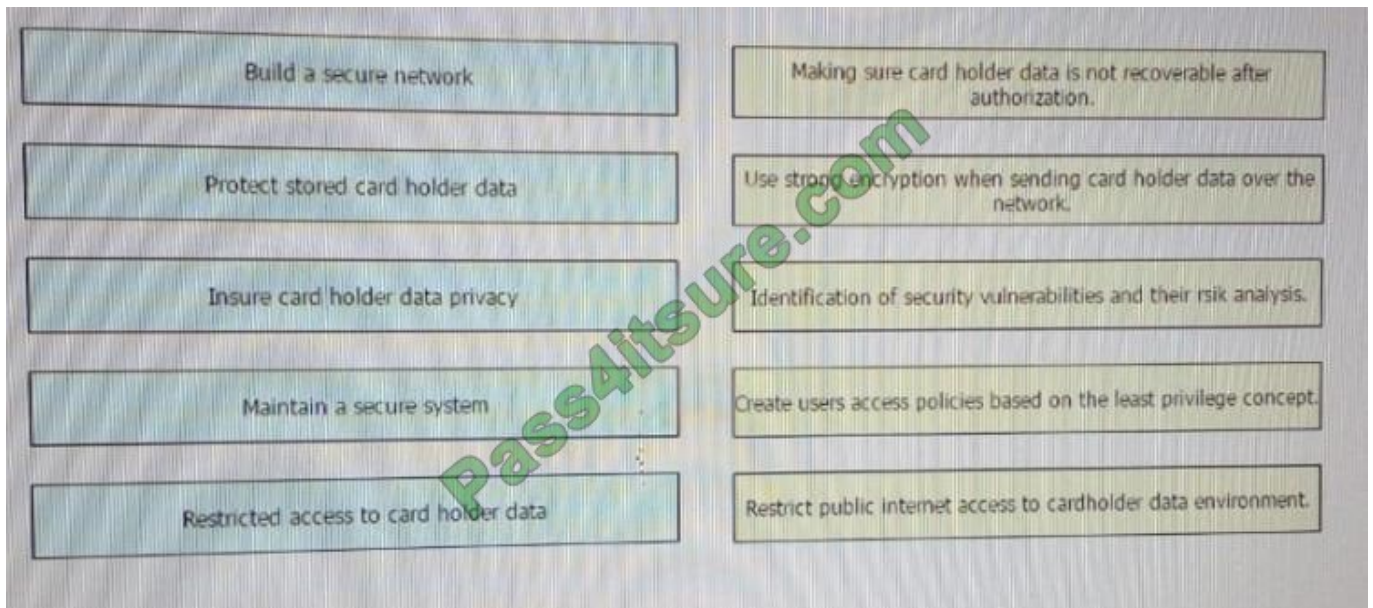
Correct Answer: E

---

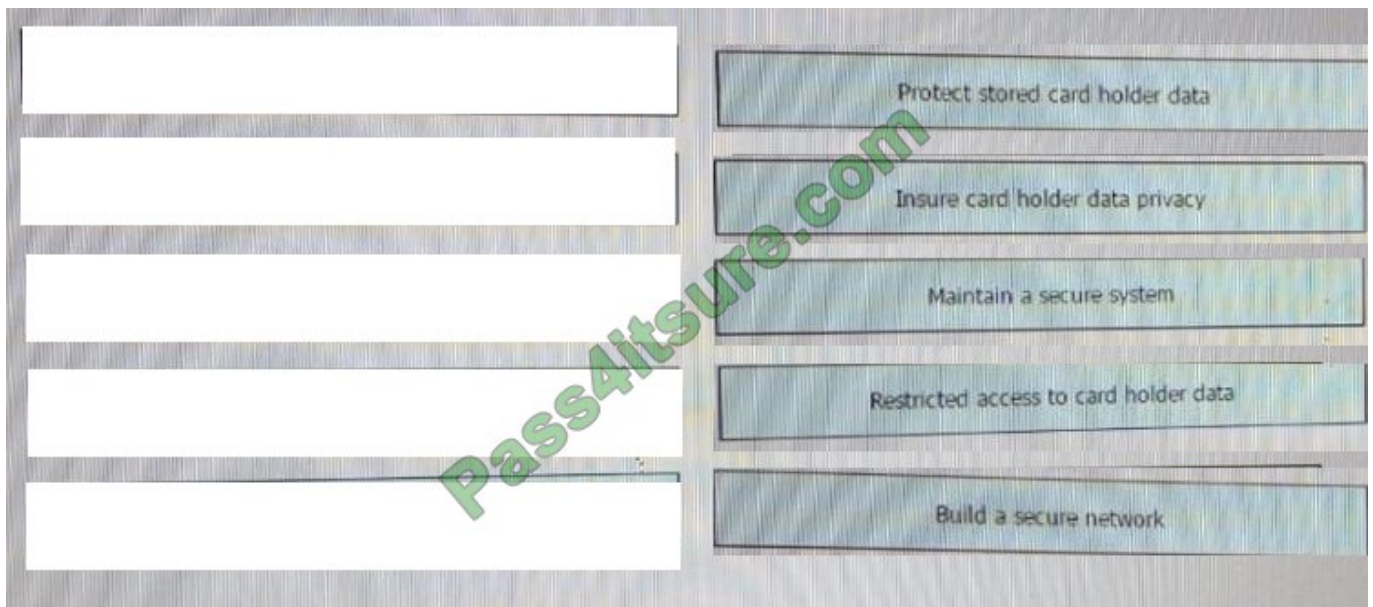
#### QUESTION 10

Drag the PCI-DSS requirements on the left to its security controls on the right

Select and Place:



Correct Answer:



#### QUESTION 11

Refer to the exhibit. One of the Windows machines in your network is having connectivity issues using 802.1x. Windows machines are setup to acquire an IP address from the DHCP server configured on the switch, which is supposed to hand over IP addresses from the 50.1.1.0/24 network, and forward AAA requests to the radius server at 161.1.7.14 using shared key "cisco". Knowing that interface Gi0/2 on SW1 may receive authentication requests from other devices and looking at the provided switch configuration, what could be the possible cause of this failure?

```
aaa new model
aaa authentication login default group radius
aaa authentication login NO_AUTH none
aaa authentication login vty local
aaa authentication dot1x default group radius
aaa authentication network default group radius
aaa accounting dot1x default start-stop group radius
!
username cisco privilege 15 password 0 cisco
!
interface GigabitEthernet0/2
switchport mode access
ip access-group Pre-Auth in
authentication host-mode multi-auth
authentication open
authentication port-control auto
!
vlan 50
interface Vlan50
ip address 50.1.1.1 255.255.255.0
!
ip
```





dhcp excluded-address 50.1.1.1 ip dhcp pool pc-pool network 50.1.1.0 255.255.255.0 default-router 50.1.1.1 ! ip access-list extended Pre-Auth permit udp any eq bootpc any eq bootps deny ip any any ! radius server ccie address ipv4 161.1.7.4 auth-port 1645 acct-port 1646 key cisco ! line con 0 login authentication NO\_AUTH line vty 0 4 login authentication vty

- A. 802.1x authentication is not enabled on interface Gi0/2
- B. an incorrect default route is pushed on supplicant from SW1
- C. an incorrect ip address is configured for SVI 50
- D. aaa network authorization is not configured
- E. There is a RADIUS key mismatch
- F. 802.1X is disabled on the switch
- G. authentication for multiple hosts is not configured on interface Gi0/2

Correct Answer: A

## QUESTION 12

Which statement is true regarding TLS security protocol?

- A. It only supports data authentication for the client-server session using a browser
- B. TLS and SSL versions can interoperate in the client-server handshake
- C. There is no difference between TLS and SSL versions 2 and 3
- D. TLS version 1.0 is more secure than SSL version 3.0
- E. It is always recommended to disable TLS version 1.0 in the browser so that it only supports SSL for better security
- F. You need to replace SSL certificate with TLS certificate for successful TLS operation

Correct Answer: D

[Latest 400-251 Dumps](#)

[400-251 Study Guide](#)

[400-251 Braindumps](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

## Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

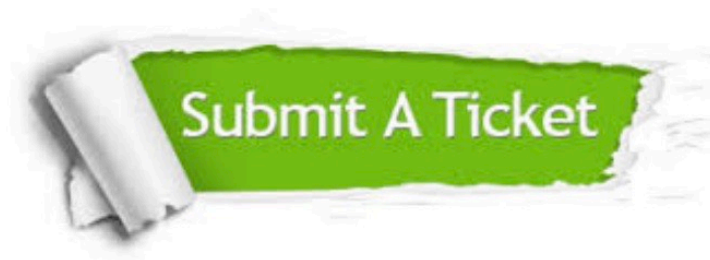
We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.pass4itsure.com/allproducts>

## Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <b>One Year Free Update</b> <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <b>Money Back Guarantee</b> <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <b>Security &amp; Privacy</b> <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © pass4itsure, All Rights Reserved.