# IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

**Exam : 400-251**

**Title : CCIE Security Written Exam (v5.0)**

**Version : DEMO**

1.In your ISE design, there are two TACACS profiles that are created for a device administration: Help Desk_Profile, and IOS_Admin_Profile. The Help Desk profile should login the user with privilege 1, with ability to change privilege level to 15. The Admin profile should login the user with privilege 15 by default.
Which two commands must the help Desk enter on the IOS device to access privilege level 15? (Choose two)
A. Enable secret
B. Enable 15
E. Enable
F, Enable lOS_Admin profile
G. Enable password
**Answer:** BE

2.Which criteria does ASA use for packet classification if multiple contexts share an ingress interface MAC address?
A, ASA ingress interface IP address
B. policy-based routing on ASA
D. destination MAC address
E. ASA ingress interface MAC address
G. ASA egress interface IP address
**Answer:** E

3.For your enterprise ISE deployment, you want to use certificate-based authentication for all your Windows machines you have already pushed the machine and user certificates out to all the machines using GPO. By default, certificate-based authentication does not check the certificate against Active Directory, or requires credentials from the user. This essentially means that no groups are returned as part of the authentication request.
In which way can the user be authorized based on Active Directory group membership?
A. The certificate must be configured with the appropriate attributes that contain appropriate group formation, which can be used in Authorization policies
B. Configure the Windows supplicant to used saved credentials as well as certificate based authentication
C. Enable Change of Authorization on the deployment to perform double authentication
D. Configure Network Access Device to bypass certificate-based authentication and push configured user credentials as a proxy to ISE
E. Use EAP authorization to retrieve group information from Active directory
F. Use ISE as the Certificate Authority which allows for automatic group retrieval from Active directory to perform the required authorization
**Answer:** A

4.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 bee 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. The registration interface is not part of management VRF "mgmt”

B. incorrect encryption traffic defined in the group policy

C. incorrect encryption in ISAKMP policy
D. incorrect password in the keyring configuration
E. The GDOI group has an incorrect local server address
F. incorrect security-association time in the IPsec profile
**Answer:** AB

5.Refer to the exhibit.
R15

```
crypto pki trustpoint ccier15
enrollment url http://172.16.100.17:8080
serial-number
ip-address 172.16.100.15
subject-name CN=r15 O=cisco.com
revocation-check none
source interface Loopback0
rsakeypair ccier15
!
crypto isakmp policy 1516
encr aes
hash md5
group 2
!
crypto ipsec transform-set ts1516 esp-aes esp-sha-hmac
mode tunnel
!
crypto map r15r16 1516 ipsec-isakmp
set peer 10.1.7.16
set transform-set ts1516
match address 110
!
interface Loopback0
ip address 172.16.100.15 255.255.255.255
!
interface Loopback1
ip address 192.168.15.15 255.255.255.0
!
interface GigabiEthernet1
ip address 20.1.6.15 255.255.255.0
netgotiation auto
crypto map r15r16
!
router bgp 6
bgp log-neighbor-changes
network 172.16.100.15 mask 255.255.255.255
```

```
neighbor 20.1.6.18 remote-as 678
neighbor 20.1.6.18 password cisco
!
ip route 192.168.16.0 255.255.255.0 20.1.7.16
access-list 110 permit ip 192.168.15.0 0.0.0.255 192.168.16.0 0.0.0.255
!
ntp authentication-key 11 md5 ccie
ntp authenticate
ntp trusted-key 12
ntp server 150.1.7.131 key 12
!
ip domain name cisco.com
```

R15 is building a Site-to-Site IPsec certificate-based VPN tunnel with the peer at 20.1.7.16. The CA is running at port 80 on address 172.16.100.18. R15 has a BGP peer at 20.6.1.18 doing an authenticated session to establish reachability with the VPN remote site.

The VPN tunnel secures traffic between 192.168.15.0/24 and 192.168.16.0/24 networks.

It has been reported that VPN tunnel is not coming up with remote site, what could be the issues? (Choose two)

A. Incorrect ACL defined for the traffic encryption
B. Incorrect static route
C. Incorrect crypto map configuration
D. Incorrect ISAKMP policy configuration
E. The crypto map is not applied on the correct interface
F. Incorrect truspoint configuration
G. Incorrect BGP peer Configuration
H. Incorrect transform set configuration

**Answer:** FG