

100% Money Back
Guarantee

Vendor:Cisco

Exam Code:400-251

Exam Name:CCIE Security Written

Version:Demo

QUESTION 1

Router(config)#crypto key zeroize pubkey-chain

Which effect of this command is true?

- A. The route immediately deletes its current public key from the cache and generates a new one.
- B. The public key of the remote peer is deleted from the router cache.
- C. The CA revokes the public key certificate of the router.
- D. The current public key of the router is deleted from the cache when the router reboots, and the router generates a new one.
- E. The router sends a request to the CA to delete the router certificate from its configuration.

Correct Answer: B

QUESTION 2

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 address from the 50.1.1.0/24 network, and forward AAA requests to the radius server at 161.1.7.14. Knowing that interface Gi0/2 on the 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 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 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
deny 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. An incorrect dhcp pool is configured.
- B. Authentication is not enabled on interface gi0/2.
- C. Aaa dot1x authentication is not configured.
- D. Authentication port-control is not set on interface gi0/2.
- E. An incorrect pre-authentication acl is configured.

Correct Answer: E

QUESTION 3

```
aaa new-model
aaa authentication username-prompt "Local Username: "
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
no aaa authorization config-commands
aaa authorization exec default group tacacs+ local if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
aaa authorization reverse-access default group tacacs+
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
```

Refer to the exhibit. Which two effects of this configuration are true? (Choose two)

- A. Configuration commands on the router are authorized without checking the TACACS+ server
- B. When a user logs in to privileged EXEC mode, the router will track all user activity
- C. Requests to establish a reverse AUX connection to the router will be authorized against the TACACS+ server
- D. When a user attempts to authenticate on the device, the TACACS+ server will prompt the user to enter the username stored in the router's database
- E. If a user attempts to log in as a level 15 user, the local database will be used for authentication and the TACACS+ will be used for authorization
- F. It configures the router's local database as the backup authentication method for all TTY, console, and aux logins

Correct Answer: AB

QUESTION 4

A customer has configured a single Policy Set to authenticate and authorize MAB and 802.1x requests on Cisco ISE. The 802.1x authorization rules are on the top of the list and check Active Directory group membership for a match. The MAB results are at the bottom of the list and check local Identity Groups for a match. When a MAB request comes to ISE:

- A. ISE will drop the request because 802.1x and MAB rules are not allowed in the same Policy Set.
- B. ISE will not try to find Active Directory group membership based on the 802.1x request.
- C. ISE will ignore the 802.1x authentication rules on the top.
- D. ISE will never match the MAB authorization rules at the bottom.
- E. ISE will try to find the Active Directory group membership based on the MAB request.

Correct Answer: E

QUESTION 5

What are two types of attacks against wireless networks that can be prevented by a WLC? (Choose two)

- A. DHCP rouge server attacks
- B. Layer 3 flooding attacks
- C. Inverse ARP attacks on specific ports
- D. IP spoofing attacks
- E. ARP sniffing attacks on specific ports

Correct Answer: AD

QUESTION 6

In your Corporate environment, you have various Active Directory groups based on the organizational structure and would like to ensure that users are only able to access certain resources depending on which groups(s) they belong to. This policy should apply across the network. You have ISE, ASA and WSA deployed, and would like to ensure the appropriate policies are present to ensure access is only based on the user's group membership. Additionally, you don't want the user to authenticate multiple times to get access. Which two policies are used to set this up? (Choose two)

- A. Deploy Cisco TrustSec Infrastructure, with ASA and WSA integrated with the ISE to transparently identify user based on SGT assignment. when the user authenticates to the network. The SGTs can then be used in access policies
- B. Deploy ISE, integrate it with Active Directory, and based on group membership authorize the user to specific VLANs. These VLANs (with specific subnets) should then be used in access policies on the ASA as well as the WSA.
- C. Deploy a Single Sign-On Infrastructure such as Ping, and Integrate ISE, ASA and WSA with it. Access policies will be applied based on the user's group membership retrieved from the authentication Infrastructure.
- D. Configure ISE as an SSO Service Provider, and integrate with ASA and WSA using pxGrid. ASA and WSA will be able to extract the relevant identity information from ISE to apply to the access policies once the user has authenticated to the network.
- E. Integrate ISE, ASA and WSA with Active Directory. Once user is authenticated to the network through ISE, the ASA and WSA will automatically extract the identity information from AD to apply the appropriate access policies.
- F. Configure ISE to relay learned SGTs for the authenticates sessions with the binded destination address using SXP or SXP speakers that will be used to apply access policies at the traffic ingress point for segmentation

Correct Answer: AC

QUESTION 7

Refer to the Exhibit. FMC with address 161.1.7.15 is not seeing AMP Connectors scan events reported to AMP cloud from "test-pc" windows machine that belongs to "Protect" group. What could be the issue?

Name 161.1.7.15

Description
CiscoFirepowerManagementCenterforVMWare

URL https://fmc1pod1.cisco.com/

Application Type Firepower Management Center

Cancel Update

Event Export Groups 1 group selected

Audit Audit Group for Cisco - zihussai

- A. The Windows machine belongs to an incorrect group in the AMP cloud policy
- B. FMC was not added in the AMP cloud
- C. The incorrect group is sheeted for the events ex-ort m the AMP cloud for the FMC.
- D. The Event must be viewed as a Connection event in the FMC
- E. The AMP cloud was not added in the FMC
- F. The Windows machine is not reporting scan events to the AMP cloud
- G. The Windows machine is not reporting events to the FMC

Correct Answer: A

QUESTION 8

Which option does a wired MAB appear in ISE RADIUS live logs?

- A. (Radius:Service-Type equals Framed) and (Radius:NAS-Port-Type equals Ethernet)
- B. (Radius:Service-Type equals Call-Check) and (Radius:NAS-Port-Type equals Ethernet)
- C. (Radius:Service-Type equals Call-Check) and (Radius:NAT-Port-Type equals PPPoEoVLAN)
- D. (Radius:Service-Type equals Call-Check) and (Radius:NAS-Port-Type equals PPPoEoVLAN)

Correct Answer: C

QUESTION 9

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

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

Correct Answer: B

QUESTION 10

Which four tasks are needed to configure RSA token authentication through ACS? (Choose four)

- A. Generate the sdconf.rec file on the RSA server for the authentication agent
- B. Add the ACS server to the allowed ODBC query list on the RSA server
- C. Define an OSBC client connection on the SRA server
- D. On the ACS server, define the ODBC connection and the stored SQL procedure needed to RSA server
- E. Define an authentication agent on the RSA server
- F. Add the RSA server as an external identity server on ACS
- G. Define an accounting agent on the RSA server
- H. Upload the sdconf.rec to the ACS server

Correct Answer: AEFH

QUESTION 11

Which statement is true regarding the failover link when ASAs are configured in a failover mode?

- A. The information sent over the failover link cannot be in clear text
- B. Failover key is not required for the secure communication over the failover link
- C. Configuration replication sent across the link can be secured using a failover key
- D. The information sent over the failover link cannot be in clear text but it could be secured communication using a failover key
- E. It is not recommended to use secure communication over failover link when ASA terminating the VPN tunnel.
- F. The information sent over the failover link can only be sent as a secured communication

Correct Answer: C

QUESTION 12

Which two statements about Cisco URL Filtering on Cisco IOS software are true?(Choose two)

- A. It supports Websense and N2H2 filtering at the same time.
- B. It supports local URL lists and third - party URL filtering servers
- C. By default, it uses ports 80 and 22.
- D. It supports HTTP and HTTPS traffic.
- E. By default, it allows all URLs when the connection to the filtering server is down.
- F. It requires minimal CPU time

Correct Answer: B

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

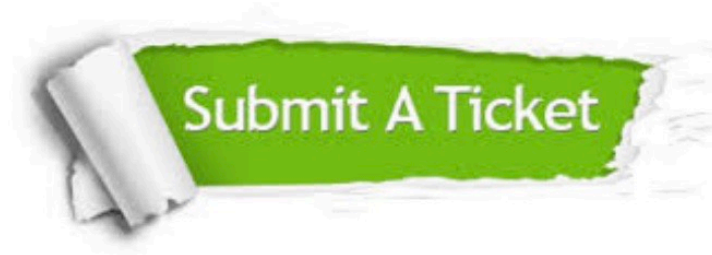
More than **800,000** Satisfied Customers Worldwide

Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

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

To update a previously submitted ticket:



 <p>One Year Free Update 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>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & 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.