

Vendor: Cisco

Exam Code: 642-637

Exam Name: Securing Networks with Cisco Routers and

Switches (SECURE v1.0)

Version: DEMO

QUESTION 1

Refer to the exhibit. Given the partial output of the debug command, what can be determined?

```
Router# debug crypto isakmp
*ISAKMP (1009): received packet from 192.168.2.2 dport 500 sport 500 Global (I)
MM KEY EXCH
IS\overline{AKMP}:(1009): processing ID payload. message ID = 0 ISAKMP (1009): ID payload
         next-payload: 8
         type
                         : 1
                         : 192.168.2.2
         address
         protocol
                         : 17
          port
                         : 500
                          : 12
          length
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1009): processing HASH payload. message ID = 0
ISAKMP: (1009): SA authentication status:
                                                          authenticated
ISAKMP: (1009): SA has been authenticated with 192.168.2.2
```

- A. There is no ID payload in the packet, as indicated by the message ID = 0.
- B. The peer has not matched any offered profiles.
- C. This is an IKE quick mode negotiation.
- D. This is normal output of a successful Phase 1 IKE exchange.

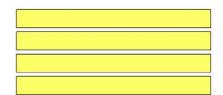
Answer: D

QUESTION 2

Drag and Drop Question.

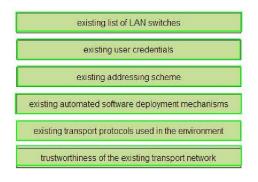
Drag the items on the left to the boxes on the right that identify important information you should collect prior to deploying 802.1X authentication in a Cisco IBNS environment. Not all items will be used.

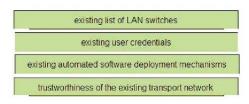
	existing list of LAN switches
	existing user credentials
	existing addressing scheme
6	existing automated software deployment mechanisms
	existing transport protocols used in the environment
	trustworthiness of the existing transport network



Answer:

Drag the items on the left to the boxes on the right that identify important information you should collect prior to deploying 802.1X authentication in a Cisco IBNS environment. Not all items will be used.





QUESTION 3

Refer to the exhibit. Which two Cisco IOS WebVPN features are enabled with the partial configuration shown? (Choose two.)

webvpn context MY-WEBVPN
policy group GROUP-POLICY
functions svc-enabled
svc keep-client-installed
svc address-pool MY-POOL
svc default-domain cisco.com
svc dns-server primary 10.10.1.1
svc split dns domain.com
svc split include 10.0.0.0 255.0.0.0
filter tunnel FILTER-ACL

- A. The end-user Cisco AnyConnect VPN software will remain installed on the end system.
- B. If the Cisco AnyConnect VPN software fails to install on the end-user PC, the end user cannot use other modes.

- C. Client based full tunnel access has been enabled.
- D. Traffic destined to the 10.0.0.0/8 network will not be tunneled and will be allowed access via a split tunnel.
- E. Clients will be assigned IP addresses in the 10.10.0.0/16 range.

Answer: AC

QUESTION 4

Refer to the exhibit. Which of these is correct regarding the configuration parameters shown?

```
crypto pki trustpoint MY-TRUSTPOINT
rsakeypair CS-KEYS
!
ip http server
!
crypto pki server MY-TRUSTPOINT
issuer-name CN=MY-CS,OU=VPN,O=Cisco,C=US
database url flash:/my-ca
database level complete
hash sha1
lifetime certificate 730
lifetime ca-certificate 3650
no grant auto
lifetime crl 5
```

- A. Complete certificates will be written to and stored in NVRAM.
- B. The RSA key pair is valid for five hours before being revoked.
- C. The router is configured as a certificate server.
- D. Certificate lifetimes are mismatched and will cause intermittent connectivity errors.
- E. The router has enrolled to the MY-TRUSTPOINT PKI server, which is an external CA server.

Answer: C

QUESTION 5

Refer to the exhibit. Based on the configuration that is shown in the exhibit, select the three answers that apply. (Choose three.)

switch(config)#interface GigabitEthernet1/0/10

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#switchport voice vlan 40

Switch(config-if)#authentication host-mode multi-domain

Switch(config-if)#authentication open

Switch(config-if)#authentication order mab dot1x

Switch(config-if)#authentication periodic

Switch(config-if)#authentication timer reauthenticate server

Switch(config-if)#mab

Switch(config-if)#dot1x pae authenticator

- A. The configuration supports multidomain authentication, which allows one MAC address on the voice VLAN and one on the data VLAN.
- B. Traffic will not flow for either the phone or the host computer until one device completes the 802.1X authentication process.
- C. Registration and DHCP traffic will flow on either the data or voice VLAN before authentication.
- D. The port will only require the 802.1X supplicant to authenticate one time.
- E. MAC Authentication Bypass will be attempted only after 802.1X authentication times out.
- F. Non-802.1X devices are supported on this port by setting up the host for MAC address authentication in the endpoint database.

Answer: ACF

QUESTION 6

Refer to the exhibit. What can be determined from the output of this show command?

Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
192.168.1.1 192.168.2.1 QM_IDLE 1002 ACTIVE

- A. The IPsec connection is in an idle state.
- B. The IKE association is in the process of being set up.
- C. The IKE status is authenticated.
- D. The ISAKMP state is waiting for quick mode status to authenticate before IPsec parameters are passed between peers
- E. IKE Quick Mode is in the idle state, indicating a problem with IKE phase 1.

Answer: C

QUESTION 7

You are troubleshooting a problem for which end users are reporting connectivity issues. Your network has been configured with Layer 2 protection controls. You have determined that the DHCP snooping database is correct and that proper static addressing maps have been configured. Which of these should be your next step in troubleshooting this problem?

- A. Generate a proxy ARP request and verify that the DHCP database has been updated as expected.
- B. Temporarily disable DHCP snooping and test connectivity again.
- C. Clear the ARP tables and have end users release and renew their DHCP-learned addressing.
- D. Use a protocol analyzer to determine if there are malformed DHCP or ARP packets.

Answer: D

QUESTION 8

You are finding that the 802.1X-configured ports are going into the error-disable state. Which command will show you the reason why the port is in the error-disable state, and which command will automatically be re-enabled after a specific amount of time? (Choose two.)

- A. show error-disable status
- B. show error-disable recovery
- C. show error-disable flap-status
- D. error-disable recovery cause security-violation
- E. error-disable recovery cause dot1x
- F. error-disable recovery cause I2ptguard

Answer: BD

QUESTION 9

Your company has a requirement that if security is compromised on phase 1 of a Diffie-Hellman key exchange that a secondary option will strengthen the security on the IPsec tunnel. What should you implement to ensure a higher degree of key material security?

- A. Diffie-Hellman Phase II ESP
- B. PFS Group 5
- C. Transform-set SHA-256
- D. XAUTH with AAA authentication
- E. Diffie-Hellman Group 5 Phase I

Answer: B

QUESTION 10

Refer to the exhibit. What can be determined about the IPS category configuration shown?

ip ips signature-category
category all
enabled false
retired true
category os ios
enabled true
retired false
event-action produce-alert reset-tcp-connection

- A. All categories are disabled.
- B. All categories are retired.
- C. After all other categories were disabled, a custom category named "os ios" was created
- D. Only attacks on the Cisco IOS system result in preventative actions.

Answer: D

Ensurepass.com Members Features:

- 1. Verified Answers researched by industry experts.
- 2. Q&As are downloadable in PDF and VCE format.
- 3. 98% success Guarantee and Money Back Guarantee.
- 4. Free updates for 180 Days.

View list of All Exam provided:

http://www.ensurepass.com/certfications?index=A

To purchase Lifetime Full Access Membership click here:

http://www.ensurepass.com/user/register

Valid Discount Code for 2014: SFOH-FZA0-7Q2S

To purchase the HOT Exams:

Ci	sco	CompTIA		Oracle	<u>VMWare</u>	IBM
100-101	640-554	220-801	LX0-101	<u>1Z0-051</u>	VCAD510	C2170-011
200-120	640-802	220-802	N10-005	<u>1Z0-052</u>	<u>VCP510</u>	C2180-319
300-206	<u>640-816</u>	BR0-002	SG0-001	<u>1Z0-053</u>	<u>VCP550</u>	C4030-670
300-207	640-822	CAS-001	SG1-001	<u>1Z0-060</u>	VCAC510	C4040-221
300-208	640-864	CLO-001	SK0-002	<u>1Z0-474</u>	VCP5-DCV	RedHat
350-018	642-467	<u>ISS-001</u>	SK0-003	<u>1Z0-482</u>	VCP510PSE	EX200
352-001	642-813	JK0-010	SY0-101	<u>1Z0-485</u>		EX300
400-101	642-902	JK0-801	SY0-301	<u>1Z0-580</u>		
640-461	700-302			<u>1Z0-820</u>		

