Exam Code: 642-567

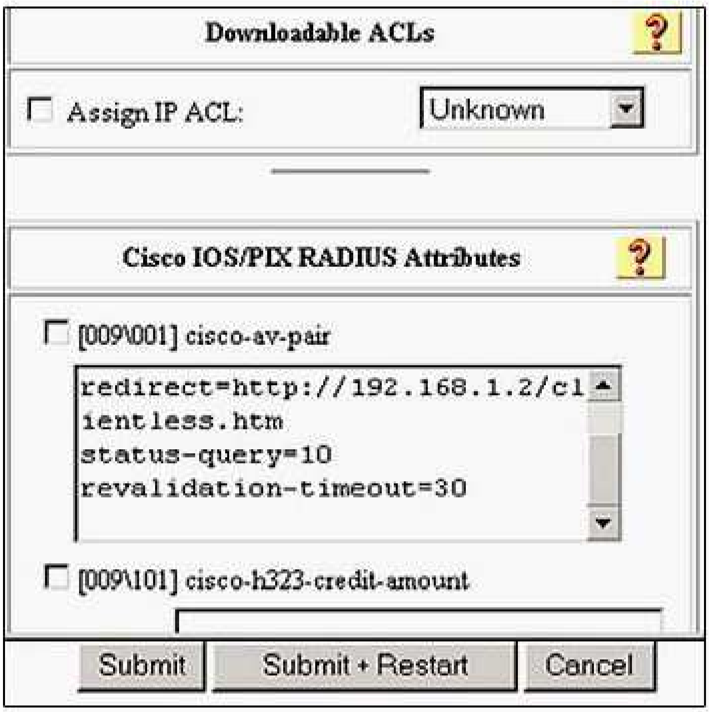
Exam Name: Advanced Security for Field Engineers

Vendor: CISCO

Version: DEMO

Part: A

1: Refer to the exhibit. You are troubleshooting a problem with a clientless host. It is showing up as 'unknown' or URL redirection is not working. You have determined that the problem lies in the Cisco ACS configuration. Which two parameters must be changed in order to correct this behavior? (Choose two)



Downloadable ACLs

□ Assign IP ACL: Unknown

Cisco IOS/PIX RADIUS Attributes

□ [009\001] cisco-av-pair

```
redirect=http://192.168.1.2/cl
ientless.htm
status-query=10
revalidation-timeout=30
```

□ [009\101] cisco-h323-credit-amount

A.Check "Assign IP ACL."

B.Change the dropdown to "Healthy."

C.Check the "[0900\001] cisco-av-pair" box.

D.Change the redirect statement to http://192.168.1.2/healthy.htm.

E.Increase the status-query timer to 20 to help prevent a query timeout.

Correct Answers: A C

2: Which CCA out-of-band solution statement is correct?

A.All client traffic flows through the CAS while access switch VLAN management is performed out of band.

B.Access switch to CAM configuration and status change messages are communicated via a proprietary protocol.

C.The switchport access and authentication VLAN information is sent to the access switch from the CAM.

D.As a laptop device accesses the CCA network, the access switch sends the device's MAC address to the CAS.

Correct Answers: C

3: What is specified when the command ip radius source-interface is entered in the global configuration mode of a Cisco switch acting as a NAD?

A.the interface for all outgoing RADIUS packets

B.that all interfaces are sources for RADIUS authentication requests

C.that Layer 2 packets received are converted and passed to the RADIUS server as Layer 3 IP packets

D.the interface where the sourced RADIUS packets should be received at the switch

Correct Answers: A

5: Which browser plug-in is required to view the charts and graphs on the MARS Appliance?

A.Macromedia Flash Player

B.Sun Microsystems Java

C.Microsoft PowerPoint

D.Adobe SVG Viewer

Correct Answers: D

7: Which is a benefit of using the dollar variable (like $TARGET01) when creating queries in MARS?

A.The dollar variable enables multiple queries to reference the same common 5-tuples information using a variable.

B.The dollar variable ensures that the probes and attacks that are reported are happening to the same host.

C.The dollar variable allows matching of any unknown reporting device.

D.The dollar variable allows matching of any event type groups.

E.The dollar variable enables the same query to be applied to different reports.

Correct Answers: B

8: Which command can you use to verify operation between a Network Admission Control (NAC) agent and a Network Access Device (NAD)?

A.show eapoupd all

B.show eou all

C.show nac all

D.show nac access-list all

Correct Answers: B

9: Regarding MARS Appliance rules, which three statements are correct? (Choose three.)

A.There are three types of rules: System Inspection Rules, User Inspection Rules, and Drop Rules.

B.Rules can be saved as reports.

C.Rules can be deleted.

D.Rules trigger incidents.

E.Rules can be defined using a seed file.

F.Rules can be created using a query.

Correct Answers: A D F

10: When restoring archived data to a MARS Appliance, which is the best practice to follow?

A.Use HTTPS to protect the data transfer.

B.Use secured FTP to protect the data transfer.

C.Use "mode 5" restore from the MARS CLI to provide enhanced security during the data transfer.

D.Use the Admin > System Maintenance > Data Archiving on the MARS GUI to perform restore operations online.

E.To avoid problems, only restore to a same or higher-end MARS Appliance.

Correct Answers: E

11: If the CAS is configured to autogenerate an IP address pool of 30 subnets with a netmask of /30, beginning at address 192.168.10.0, which IP address is leased to the end-user host on the second subnet?

A.192.168.10.4

B.192.168.10.5

C.192.168.10.6

D.192.168.10.7

Correct Answers: C

12: Identify three ways an administrator can implement Cisco Clean Access (CCA) to protect a network. (Choose three.)

A.CTA only

B.CSA only

C.CAA only

D.CAA and network scan

E.network scan only

F.end-user scan only

Correct Answers: C D E

13: Which three statements are correct about the MARS Global Controller? (Choose three.)

A.The Global Controller can correlate events from different Local Controllers into a common session.

B.One Global Controller can support multiple Local Controllers.

C.Each zone can have one Local Controller.

D.All Local Controllers events are propagated to the Global Controller for correlations.

E.The Global Controller and the Local Controllers can be running different MARS OS versions.

F.Based on a selected Local Controller, incidents on the Global Controller can be viewed.

Correct Answers: B C F