Exam : 642-567
Advanced Security for Field Engineers

Demo Version

To Access Full Version, Please go to

QUESTION 1:

When issuing the show eou all command on a Cisco router acting as a NAD, you do not see any EOUoUDP sessions in the displayed output. Which, most likely, is the problem?

A. No clients have attempted access.
B. Clients are not configured to use EOUoUDP.
C. All NAC sessions have timed out.
D. The router is not properly configured.

Answer: D

QUESTION 2:

A college network administrator wants to restrict access to specific, targeted subnets by role, such as student, administration, faculty, and guest roles. How would this be accomplished using the Clean Access Manager (CAM)?

A. Define extended access-list templates, and apply each template to a specific user role.
B. Define IP-based traffic control policy for each role that specifies the target subnets.
C. Define a host-based traffic control policy for each role that specifies the target subnets.
D. Define a bandwidth policy for each role that specifies the target subnets.

Answer: B

QUESTION 3:

Which Cisco "all-in-one" security appliance automatically detects, isolates, and cleans infected and/or vulnerable devices that attempt to access a network?

A. Cisco Security Monitoring, Analysis and Response System (CS MARS) B.
Cisco Clean Access (CCA)
C. Security Device Manager (SDM)
D. Cisco Security Agent (CSA)

Answer: B

QUESTION 5:

Exhibit:

To configure the Mars appliance to send out an alert when the system rule fires, what should you fropm the MARS GUI screen shown?

A. Click on "Active" in the "Status" field, select the appropriate alerts, then apply.
B. Click on "None" in the "Action" field, select the appropriate alerts, then apply
C. Click "Edit" to edit the "Operation" field of the rule, select the appropriate alert option(s), then apply.
D. Click "Edit" to edit the "Event" field of the rule, select the appropriate alert option(s), then apply.
E. Click "Edit" to edit the "Reported User" field of the rule, select the appropriate alert option(s), then apply.

Answer: B

QUESTION 6:

When the maximum limit of 100 unauthorized non-responsive endpoints per NAD is reached, the router stops processing RADIUS requests for NAC to prevent DoS attacks on the ACS server. What then happens to legitimate users attempting access?

A. Users without CTA will be denied access.
B. Users with CTA will still receive posture validation tokens.
C. Users will have default network access (whatever is permitted by the access list [ACL] of the router interface).
D. All users will be denied access and placed into an "unknown" status.

Answer: C