



The Top Certification Site **OVER 1000 EXAMS FROM ALL VENDORS**

IT Exam World .com

- Verified Answers and Explanations
- Printable questions and answers
- Update per 15-20 Days
- Instant Download
- Security Multi Order
- 24*7 Support
- Pass on Your First Try Guarantee

 **Interactive Exams**
Self Exam Engine

 **Questions & Answers**
With Explanations

 **Study Guides**

 **Preparation Labs**

 **Audio Exams**

Exam : 642-567
Advanced Security for Field Engineers

Demo Version

To Access Full Version, Please go to
www.itexamworld.com

QUESTION 1:

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

- A. No clients have attempted access.
- B. Clients are not configured to use EOUnUDP.
- 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:

Rule time: Network Activity: Windows Popup Spam										Status: Active			
Action:										Time Range: 0h:00m			
Description: This correlation affects excessive traffic (likely pop up spam) from the same source to the Windows Messenger service.													
Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Oper	
1		TARGET01, ANY	ANY	MSMessengerService_UDP (src port: ANY, dst port: 1826-1829, proto: UDP)		ANY	None	ANY	ANY	20			
							1 to 25 of 48		25 per page		Jump to 1-25		
Edit		Change Status										Duplicate	

To configure the Mars appliance to send out an alert when the system rule fires, what should you from 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