

IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

Exam : **642-544**

Title : Implementing Cisco Security
Monitoring, Analysis and
Response System

Version : DEMO


1.Refering to the rule shown on the MARS GUI screen, which two of the following statements are correct?(Choose two.)

The corporate office for a footwear distributor is installing a temporary Catalyst 3550 in an IDF to connect 24 additional users. To prevent network corruption, it is important to have the correct configuration prior to connecting to the production network. It will be necessary to ensure that the switch does not participate in VTP but forwards VTP advertisements that are received on trunk ports.

Because of errors that have been experienced on office computers, all nontrunking interfaces should transition immediately to the forwarding state of Spanningree. Also, configure the user ports (all FastEthernet ports) so that the ports are permanently nontrunking.

eSIM™ Professional 00:00:01
Scenario 1 Version 1.0

You will have to scroll this window and the problem statement window to view the entire problem.
To configure the switch click on a host icon that is connected to a switch by a serial console cable (shown in the diagram as a curved solid black line).
The [Tab] key



Hide Topology

- A.This rule will fire if the offset 1 condition occurs "OR" if the offset 2 condition occurs.
- B.This rule will fire if the offset 3 condition occurs.
- C.The expressions between cells are "AND" while the expressions between items in the same cell are "OR".
- D.This is a user-defined rule.
- E.This rule can be deleted after changing its status to "inactive."

Correct: B C

2.To configure a Microsoft Windows IIS server to publish logs to the Cisco Security MARS, which log agent is installed and configured on the Microsoft Windows IIS server?

- A.pnLog agent
- B.Cisco Security MARS agent
- C.SNARE
- D.None. Cisco Security MARS is an agentless device.

Correct: C

3.Drop

Click and drag the definitions on the left to the appropriate terms on the right.

This is exclusive to hosts and software applications running on hosts.

It is used to either connect to the device for network-based administrative sessions or connect to a remote server on which a file containing the device's configuration is stored.

It is the source IP address of event messages, logs, notifications, or traps that originate from the device.

It refers to the administrative protocol that Cisco Security MARS uses to access a reporting device or mitigation device.

access type

reporting IP

access IP

interface setting

Correct:

Green choice4---->Yellow Choice1

Green choice3---->Yellow Choice2

Green choice2---->Yellow Choice3

Green choice1---->Yellow Choice4

4.A Cisco Security MARS appliance cannot access certain devices through the default gateway. Troubleshooting has determined that this is a Cisco Security MARS configuration issue. Which additional Cisco Security MARS configuration will be required to correct this issue?

- A.use the Cisco Security MARS GUI or CLI to enable a dynamic routing protocol
- B.use the Cisco Security MARS CLI to add a static route
- C.use the Cisco Security MARS GUI to configure multiple default gateways
- D.use the Cisco Security MARS GUI or CLI to configure multiple default gateways

Correct:B

5.Which action enables the Cisco Security MARS appliance to ignore false-positive events by either dropping the events completely, or by just logging them to the database?

- A.creating system inspection rules using the drop operation
- B.creating drop rules
- C.inactivating the rules
- D.inactivating the events
- E.deleting the false-positive events from the Incidents page
- F.deleting the false-positive events from the Event Management page

Correct:B