IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

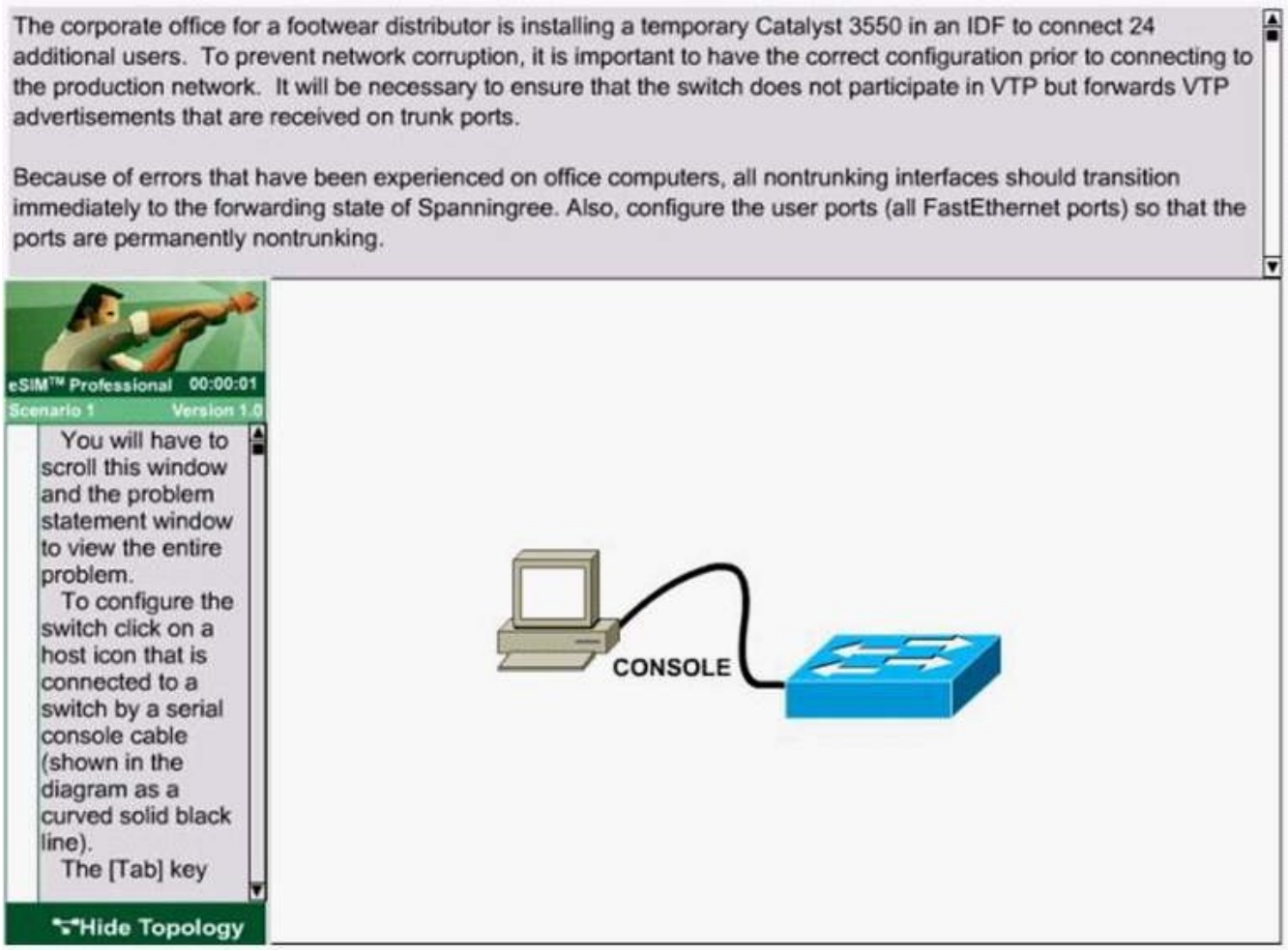
http://www.itrenzheng.com

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.)



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."

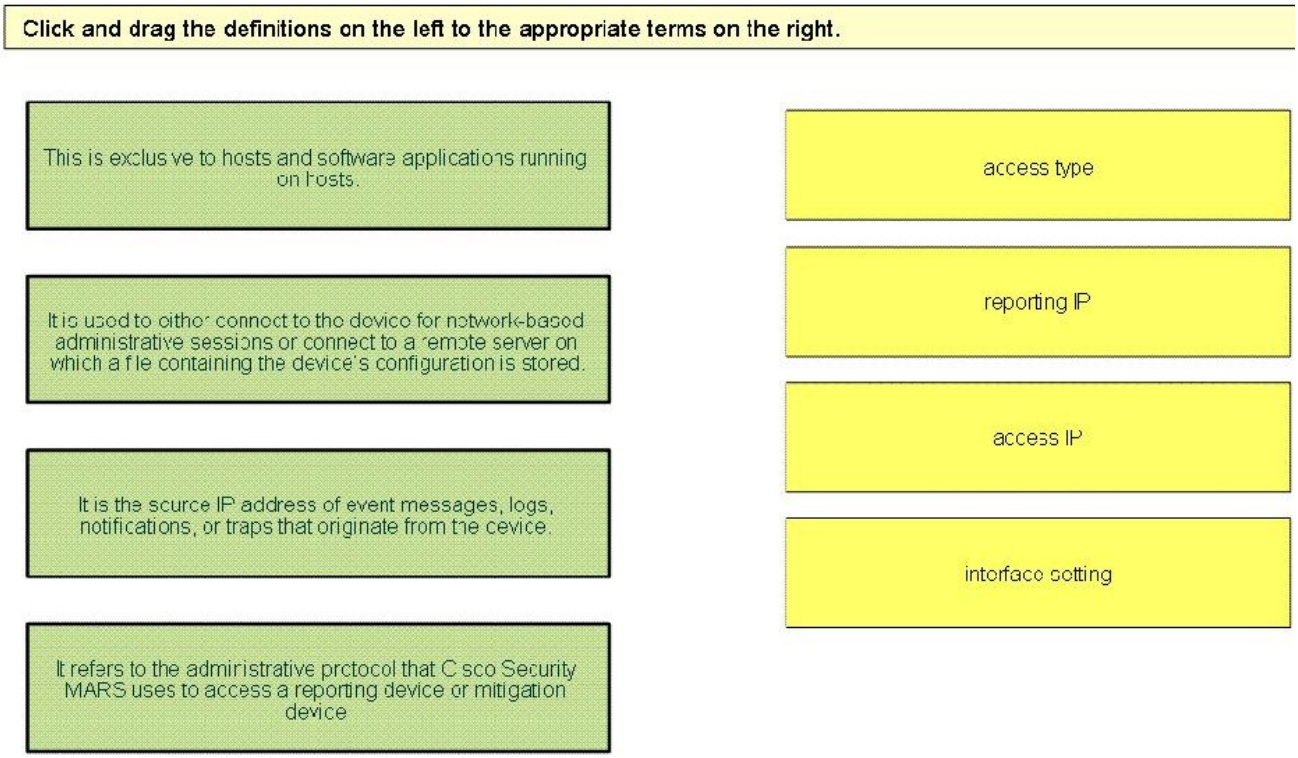
Correct:B C

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



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