Cisco 642-532

CISCO 642-532 Securing Networks Using Intrusion Prevention Systems Exam (IPS)

Practice Test

Version 1.1

QUESTION NO: 1

Refer to the exhibit. You notice these alerts and others with some of the same attributes on your sensor when you arrive at work one morning. What is an appropriate action to take?

```
evIdsAlert: eventId=1111114419743472090 severity=high
vendor=Cisco
  originator:
    hostId: sensor1
    appName: sensorApp
    appInstanceId: 340
  time: 2005/03/21 10:47:53 2005/03/21 10:47:53 UTC
  signature: description=SYN23 id=60000
version=custom
    subsigId: 0
    sigDetails: My Sig Info
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.10.10
      port: 2151
    target:
      addr: locality=IN 10.0.1.50
      port: 23
  actions:
    deniedPacket: true
    deniedFlow: true
  riskRatingValue: 90
  interface: fe0_1
  protocol: tcp

evIdsAlert: eventId=1111100779743472268 severity=high
vendor=Cisco
  originator:
    hostId: sensor1
    appName: sensorApp
    appInstanceId: 340
  time: 2005/03/21 13:04:41 2005/03/21 13:04:41 UTC
  signature: description=ICMP Echo Request id=2004
version=81
    subsigId: 0
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.10.10
    target:
      addr: locality=IN 0.0.0.0
  summary: final=true initialAlert=0
summaryType=Regular 6
  alertDetails: Regular Summary: 6 events this interval ;
  riskRatingValue: 100                    www.pass4sures.com
  interface: fe0_1
```

A. Create an Active Host Block.

B. Activate all retired signatures.
C. Set Bypass mode to off for sensor1.
D. Lower the Target Value Ratings for hosts on your internal network.
E. Lower the Alert Severity level of signatures 2004 and 60000.

Answer: A

QUESTION NO: 2

How does a Cisco network sensor detect malicious network activity?

A. by performing in-depth analysis of the protocols that are specified in the packets that are traversing the network
B. by using behavior-based technology that focuses on the behavior of applications
C. by using a blend of intrusion detection technologies
D. by comparing network activity to an established profile of normal network activity

Answer: C

QUESTION NO: 3

Which three steps must you perform to prepare sensor interfaces for inline operations? (Choose three.)

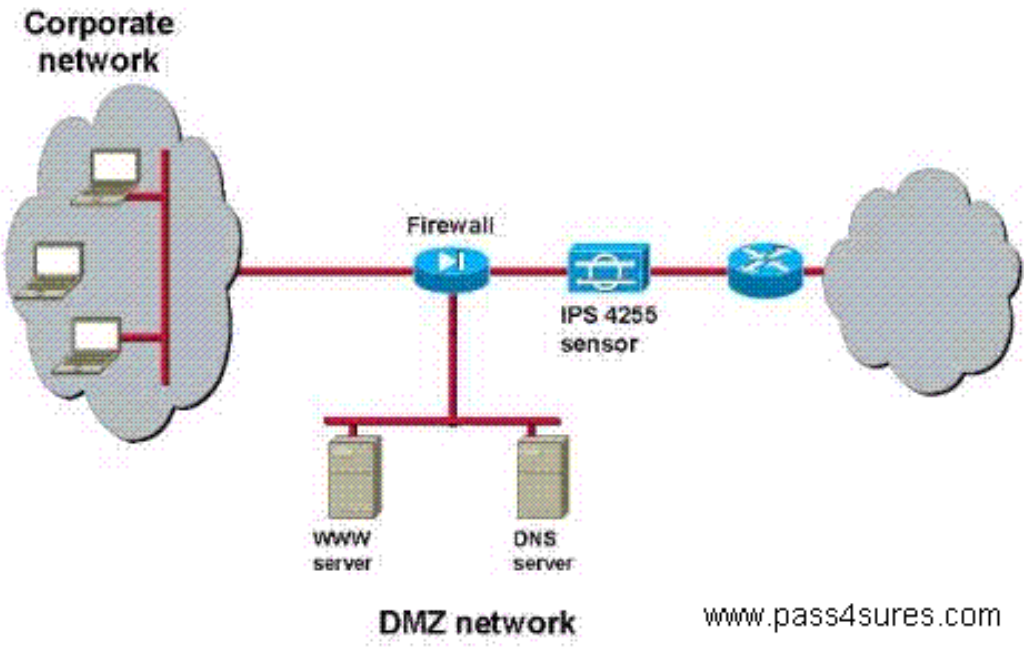
A. Add the inline pair to the default virtual sensor.
B. Configure an alternate TCP-reset interface
C. Enable two interfaces for the pair.
D. Disable any interfaces that are operating in promiscuous mode.
E. Disable all interfaces except the inline pair.
F. Create the interface pair.

Answer: A,C,F

QUESTION NO: 4

Refer to the exhibit. You are the security administrator for the network in the exhibit. You want your inline Cisco IPS 4255 sensor to drop packets that pose the most severe risk to your network, especially to the servers on your DMZ.

Which two should you use to accomplish your goal in the most time-efficient manner? (Choose two.)



A. Event Action Filter
B. Target Value Rating
C. Signature Fidelity Rating
D. Event Action Override
E. Application Policy
F. Alert Severity

Answer: B,D

QUESTION NO: 5

Which command resets all signature settings back to the factory defaults?

A. reset signatures
B. default service signature-definition
C. default service virtual-sensor
D. default signatures
E. reset signatures all

Answer: B

QUESTION NO: 6

For which purpose is a sensor license needed?

A. all sensor operations