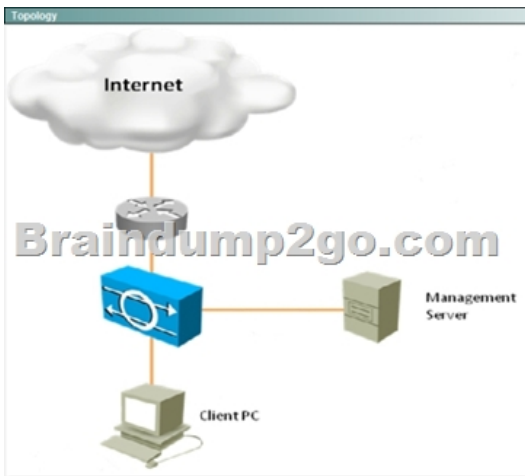


[2016.Aug.LatestDownload Braindump2go 300-207 Practice Questions 251q Free[NQ51-NQ60]

!!!2016/07 Cisco Official News!!!CCNP Security 300-207 SITCS:Implementing Cisco Threat Control Solutions Exam Questions Updated Today! Instant Free Download 300-207 SITCS PDF & 300-207 SITCS VCE Dumps from [Braindump2go.com](http://www.braindump2go.com)!100% Pass Guaranteed!100% Real Exam Questions! NEW QUESTION 51 - NEW QUESTION 60: 1.|2016/07 Latest 300-207 SITCS PDF & 300-207 SITCS VCE 251Q&As:<http://www.braindump2go.com/300-207.html>2.|2016/07 Latest 300-207 SITCS Exam Questions PDF:<https://drive.google.com/folderview?id=0B272WrTALRHcbTIPUnl0Q1JTTjQ&usp=sharing> QUESTION 51 HhB. regex-string (x0b[theblock.com])C. regex-string (x03[the]x05[block]0x3[com])D. regex-string (x03[T][H][E]x05[B][L][O][C][K]x03[.]C)[O][M] Answer: A QUESTION 52 Which three user roles are partially defined by default in Prime Security Manager? (Choose three.) A. networkoperator B. admin C. helpdesk D. securityoperator E. monitoringadmin F. systemadmin Answer: BCF QUESTION 53 Which three options are IPS signature classifications? (Choose three.) A. tuned signatures B. response signatures C. default signatures D. custom signatures E. preloaded signatures F. designated signatures Answer: ACD QUESTION 54 At which value do custom signatures begin? A. 1024 B. 10000 C. 1 D. 60000 Answer: D QUESTION 55 Which two commands are valid URL filtering commands? (Choose two.) A. url-server (DMZ) vendor smartfilter host 10.0.1.1 B. url-server (DMZ) vendor url-filter host 10.0.1.1 C. url-server (DMZ) vendor n2h2 host 10.0.1.1 D. url-server (DMZ) vendor CISCO host 10.0.1.1 E. url-server (DMZ) vendor web host 10.0.1.1 Answer: AC QUESTION 56 Which Cisco technology is a customizable web-based alerting service designed to report threats and vulnerabilities? A. Cisco Security Intelligence Operations B. Cisco Security IntelliShield Alert Manager Service C. Cisco Security Optimization Service D. Cisco Software Application Support Service Answer: B QUESTION 57 Hotspot Questions

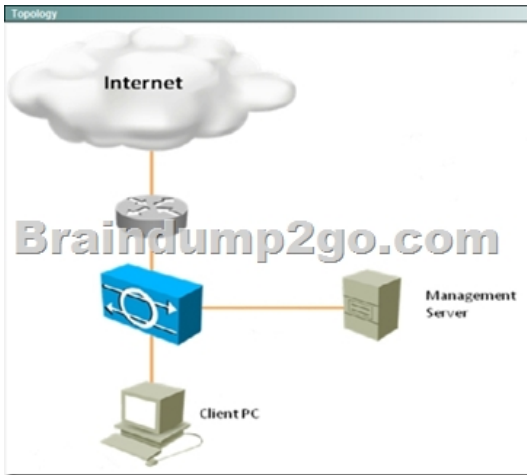
Instructions
You can click the grey buttons at the bottom of this frame to view the different windows.
Braindump2go.com
Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.



Which signature definition is virtual sensor 0 assigned to use? A. rules0B. vs0C. sig0D. ad0E. ad1F. sig1 Answer: C
Explanation: This is the default signature. You can create multiple security policies and apply them to individual virtual sensors. A security policy is made up of a signature definition policy, an event action rules policy, and an anomaly detection policy. Cisco IPS contains a default signature definition policy called sig0, a default event action rules policy called rules0, and a default anomaly detection policy called ad0. You can assign the default policies to a virtual sensor or you can create new policies. QUESTION 58

Hotspot Questions

Instructions
You can click the grey buttons at the bottom of this frame to view the different windows.
Braindump2go.com
Scenario
Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.



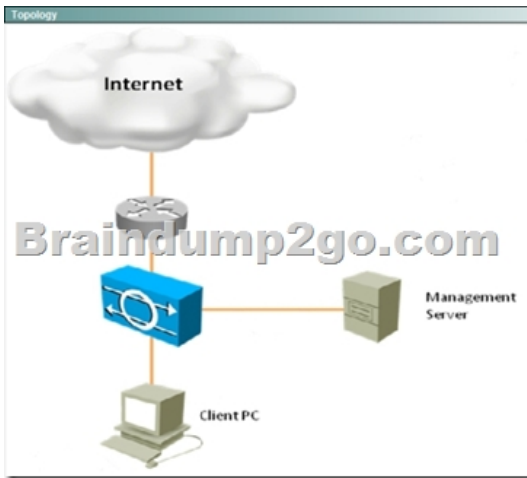
The screenshot shows the Cisco IDM interface. The 'Sensor Information' tab is active, displaying details for a sensor named 'sensor'. Key information includes: Host Name: ips, IP Address: 172.26.26.53, Device Type: IPS-4240-K9, Inclusion: No, Total Memory: 1984 MB, Total Sensing Interfaces: 4, Total Data Storage: 788 MB, and Analysis Engine Status: Running Normally. The 'Sensor Health' section shows two gauges: CPU usage at 17% and Memory usage at 77%. The 'Subscription' section shows the license status as 'Not expired until Aug 27, 2014 4:59:59 PM EST' and the signature version as 425.0. The 'Sub-Ports Status' section shows a table of interfaces with columns for Interface, Up, Enabled, Speed, Mode, Received Packets, and Transmitted Packets.

What action will the sensor take regarding IP addresses listed as known bad hosts in the Cisco SensorBase network? A. Global correlation is configured in Audit mode fortesting the feature without actually denying any hosts.B. Global correlation is configured in Aggressive mode, which has a very aggressive effect on deny actions.C. It will not adjust risk rating values based on the known bad hosts list.D. Reputation filtering is disabled. Answer: D
Explanation: This can be seen on the Global Correlation Inspection/Reputation tab show below:

The screenshot shows the 'Global Correlation Inspection' configuration page in Cisco IDM. The 'Global Correlation Inspection' section has a radio button selected for 'Use updates from the SensorBase network to adjust the risk rating'. Below this, there are three radio buttons: 'Standard' (selected), 'Global correlation data will moderately influence the decision to deny traffic.', and 'Do not utilize updates from the SensorBase network to adjust the risk rating.'. The 'Reputation' section has a radio button selected for 'Do not use the list of known bad hosts in the Global Correlation database.'. The 'Test Global Correlation' section has a checkbox for 'Do not deny traffic due to global correlation data. However, report on deny actions as if global correlation inspection and reputation filtering was active.' which is currently unchecked.

QUESTION 59 Hotspot Questions

Instructions
You can click the grey buttons at the bottom of this frame to view the different windows.
Scenario
Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.



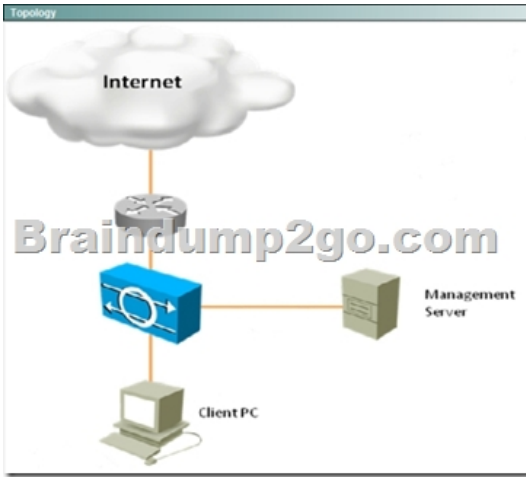
The screenshot shows the Cisco IPS Device Manager (IDM) interface. The 'Sensor Information' tab is active, displaying details for a sensor named '3550041-14612096'. Key information includes: Host Name: ipa, IP Address: 172.26.36.53, Device Type: 3PS-4240-K3, In-System: No, Total Memory: 1980 MB, Total Sensing Interfaces: 4, Total Data Storage: 768 MB, and Analysis Engine Status: Running Normally. There are several progress bars for CPU, Memory Usage, and Analysis Engine. The 'Sensor Health' section shows 'Network Security Health' as 'Good' and 'License' as 'Not expired until Aug 27, 2011 4:05:59 PM PST'. The 'Network Participation' section shows 'Global Correlation' as 'Not Checked'.

To what extent will the Cisco IPS sensor contribute data to the Cisco SensorBase network? A. It will not contribute to the SensorBase network. B. It will contribute to the SensorBase network, but will withhold some sensitive information. C. It will contribute the victim IP address and port to the SensorBase network. D. It will not contribute to Risk Rating adjustments that use information from the SensorBase network. Answer: B Explanation: To configure network participation, follow these steps: Step 1 Log in to IDM using an account with administrator privileges. Step 2 Choose Configuration > Policies > Global Correlation > Network Participation. Step 3 To turn on network participation, click the Partial or Full radio button: Partial--Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent. Full--All data is contributed to the SensorBase Network In this case, we can see that this has been turned off as shown below:

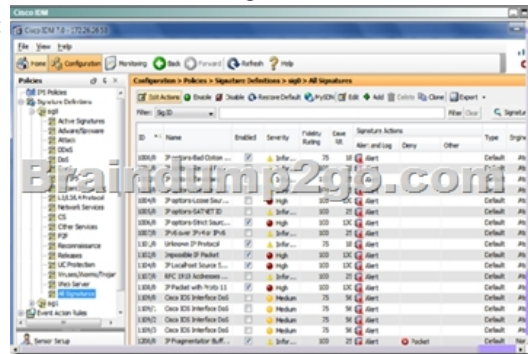
The screenshot shows the 'Global Correlation Inspection' configuration page in Cisco IPS Device Manager. The 'Global Correlation Inspection' section is expanded, showing options for 'Global Correlation Inspection'. The 'Global Correlation Inspection' section has three radio buttons: 'Allow updates from the SensorBase network to adjust the risk rating.' (selected), 'Standard... Global Correlation data will moderately influence the decision to deny traffic.', and 'Do not allow updates from the SensorBase network to adjust the risk rating.'. Below this, there are checkboxes for 'Do not use the list of known bad IPs in the Global Correlation database.' and 'Do not deny traffic due to global correlation data. However, report on deny actions as if global correlation inspection and reputation filtering are active.'.

QUESTION 60 Hotspot Questions

Instructions
You can click the grey buttons at the bottom of this frame to view the different windows.
Scenario
Using Cisco IPS Device Manager (IDM), answer the multiple choice questions.



Which two statements about Signature 1104 are true? (Choose two.)
 A. This is a custom signature.
 B. The severity level is High.
 C. This signature has triggered as indicated by the red severity icon.
 D. Produce Alert is the only action defined.
 E. This signature is enabled, but inactive, as indicated by the 0 to that follows the signature number.
 Answer: B, D
 Explanation: This can be seen here where signature 1004 is the 5th one down:



!!!RECOMMEND!!! Braindump2go 2016/07 New Cisco 300-207 Exam VCE and PDF 251Q&As Dumps Download:
<http://www.braindump2go.com/300-207.html> [100% 300-207 Exam Pass Promised!] 2016/07 Cisco 300-207 New Questions and Answers PDF:
<https://drive.google.com/folderview?id=0B272WrTALRHcbTIPUnl0Q1JTTjQ&usp=sharing>