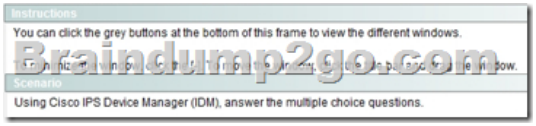
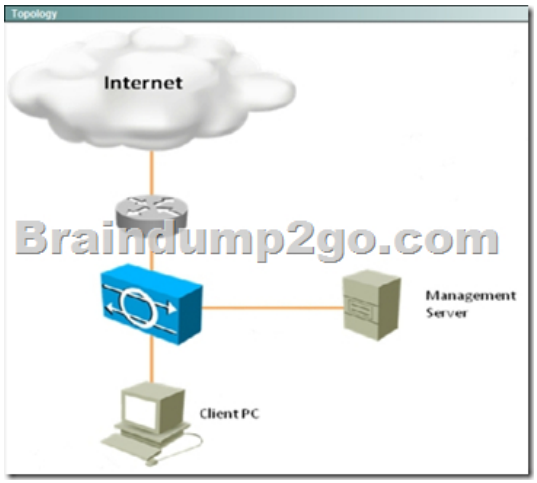
[2016.Aug.Latest100% Real 300-207 Braindumps PDF 251Q&As Free Download in Braindump2go[NQ61-NQ70

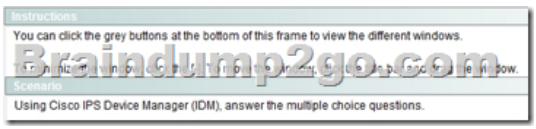
!!!2016/07 Cisco Official News!!!CCNP Security 300-207 SITCS:Implementing Cisco Threat Control Solutions Exam Questions Updated Today! Instant Free Download 300-207 SITCS PDF & 300-207 SITCS VCE Dumps from Braindump2go.com!100% Pass Guaranteed!100% Real Exam Questions! NEW QUESTION 61 - NEW QUESTION 70: 1.|2016/07 Latest 300-207 SITCS PDF & 300-207 SITCS VCE 251Q&As:http://www.braindump2go.com/300-207.html2.|2016/07 Latest 300-207 SITCS Exam Questions PDF:https://drive.google.com/folderview?id=0B272WrTALRHcbTlPUnl0Q1JTTjQ&usp=sharing QUESTION 61Hotspot Questions

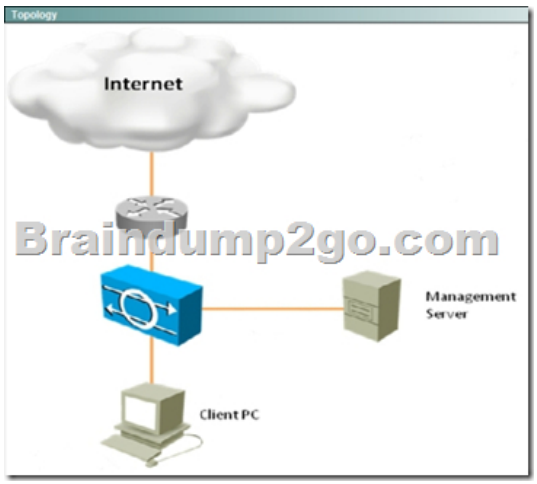






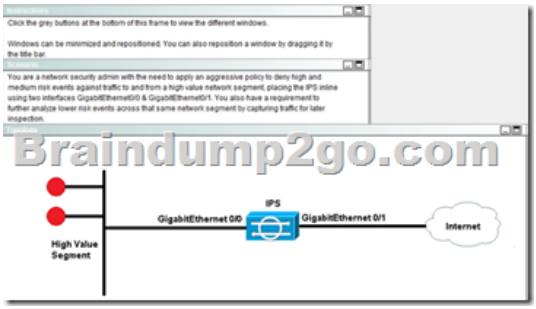
Which three statements about the Cisco IPS appliance configurations are true? (Choose three.) A. The maximum number of denied attackers is set to 10000.B. The block action duraton is set to 3600 seconds.C. The Meta Event Generator is globally enabled.D. Events Summarization is globally disabled.E. Threat Rating Adjustment is globally disabled. Answer: ABC QUESTION 62Hotspot Questions

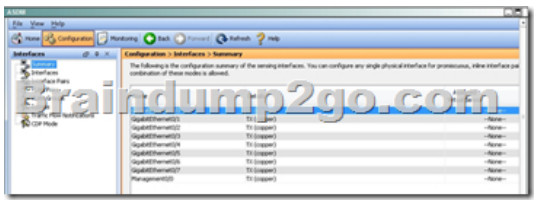




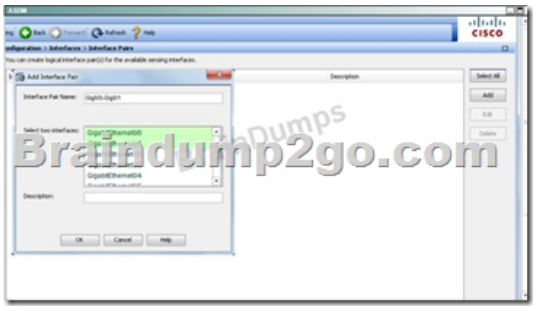


What is the status of OS Identification? A. It is only enabled to identify "Cisco IOS" OS using statically mapped OS fingerprintingB. OS mapping information will not be used for Risk Rating calculations.C. It is configured to enable OS mapping and ARR only for the 10.0.0.0/24 network.D. It is enabled for passive OS fingerprinting for all networks. Answer: DExplanation: Understanding Passive OS Fingerprinting Passive OS fingerprinting lets the sensor determine the OS that hosts are running. The sensor analyzes network traffic between hosts and stores the OS of these hosts with their IP addresses. The sensor inspects TCP SYN and SYNACK packets exchanged on the network to determine the OS type. The sensor then uses the OS of the target host OS to determine the relevance of the attack to the victim by computing the attack relevance rating component of the risk rating. Based on the relevance of the attack, the sensor may alter the risk rating of the alert for the attack and/or the sensor may filter the alert for the attack. You can then use the risk rating to reduce the number of false positive alerts (a benefit in IDS mode) or definitively drop suspicious packets (a benefit in IPS mode). Passive OS fingerprinting also enhances the alert output by reporting the victim OS, the source of the OS identification, and the relevance to the victim OS in the alert. Passive OS fingerprinting consists of three components:Passive OS learning occurs as the sensor observes traffic on the network.Based on the characteristics of TCP SYN and SYNACK packets, the sensor makes a determination of the OS running on the host of the source IP address. User-configurable OS identification You can configure OS host mappings, which take precedence over learned OS mappings. Computation of attack relevance rating and risk rating QUESTION 63Lab Simulation

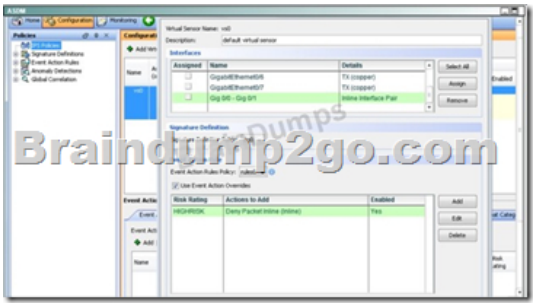




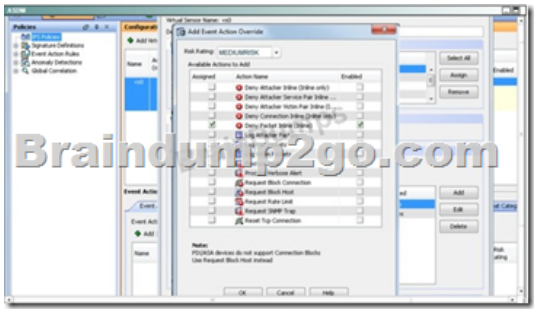
Answer: Steps are in Explanation below:First, enable the Gig 0/0 and Gig 0/1 interfaces:Second, create the pair under the "interface pairs" tab:



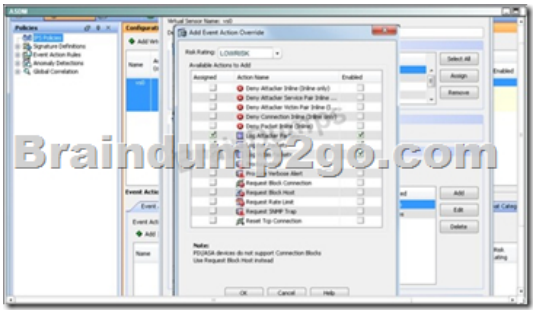
Then, apply the HIGHRISK action rule to the newly created interface pair:



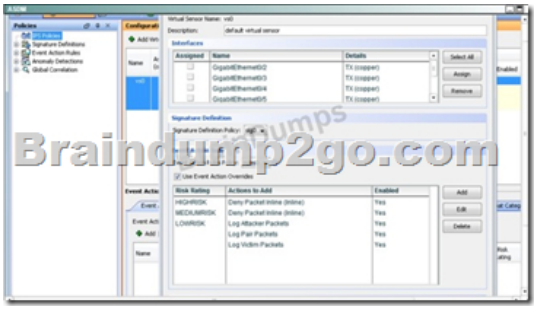
Then apply the same for the MEDIUMRISK traffic (deny attacker inline)

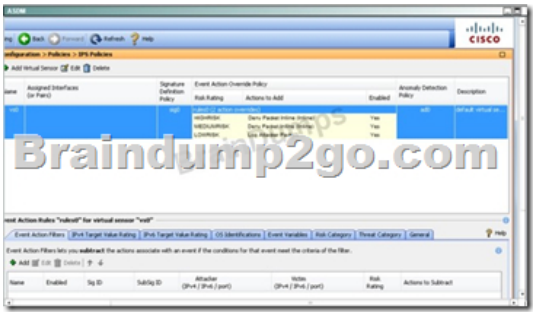


Finally. Log the packets for the LOWRICK event:



When done it should look like this:





QUESTION 64During initial configuration, the Cisco ASA can be configured to drop all traffic if the ASA CX SSP fails by using which command in a policy-map? A. cxsc failB. cxsc fail-closeC. cxsc fail-openD. cxssp fail-close Answer: B QUESTION 65A network engineer may use which three types of certificates when implementing HTTPS decryption services on the ASA CX? (Choose three.) A. Self Signed Server CertificateB. Self Signed Root CertificateC. Microsoft CA Server CertificateD. Microsoft CA Subordinate Root CertificateE. LDAP CA Server CertificateF. LDAP CA Root CertificateG. Public Certificate Authority Server CertificateH. Public Certificate Authority Root Certificate Answer: BDF QUESTION 66Cisco's ASA CX includes which two URL categories? (Choose two.) A. Proxy AvoidanceB. DropboxC. Hate SpeechD. FacebookE. Social NetworkingF. Instant Messaging and Video Messaging Answer: CE QUESTION 67A Cisco Web Security Appliance's policy can provide visibility and control of which two elements? (Choose two.) A. Voice and Video ApplicationsB. Websites with a reputation between -100 and -60C. Secure websites with certificates signed under an unknown CAD. High bandwidth websites during business hours Answer: CD QUESTION 68Which Cisco Web Security Appliance design requires minimal change to endpoint devices? A. Transparent ModeB. Explicit Forward ModeC. Promiscuous ModeD. Inline Mode Answer: A QUESTION 69What step is required to enable HTTPS Proxy on the Cisco Web Security Appliance? A. Web Security Manager HTTPS Proxy click EnableB. Security Services HTTPS Proxy click EnableC. HTTPS Proxy is enabled by defaultD. System Administration HTTPS Proxy click Enable Answer: B QUESTION 70Which two statements about Cisco Cloud Web Security functionality are true? (Choose two.) A. It integrates with Cisco Integrated Service Routers.B. It supports threat avoidance and threat remediation.C. It extends web security to the desktop, laptop, and PDA.D. It integrates with Cisco ASA Firewalls. Answer: AD !!!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=0B272WrTALRHcbTlPUnl0Q1JTTjQ&usp=sharing