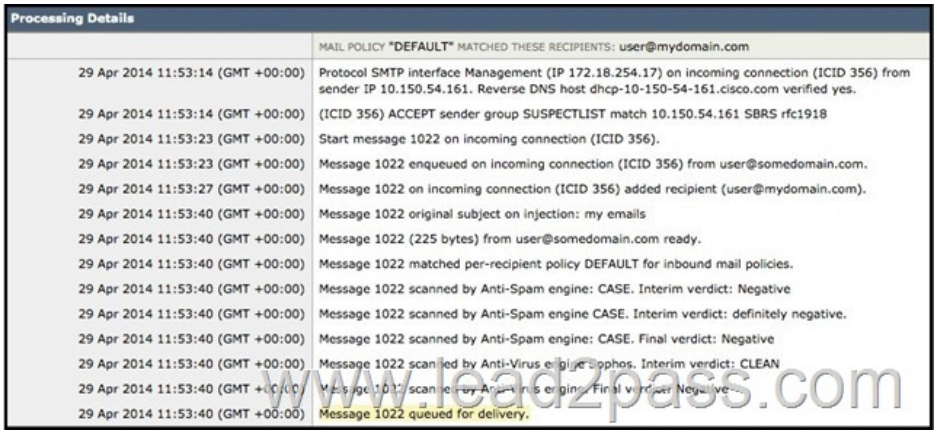
[PDF&VCE Lead2pass Offering Free 300-207 Dumps Files For Free Downloading By 300-207 Exam Candidates (81-100)

2016 October Cisco Official New Released 300-207 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! 2016 timesaving comprehensive guides for Cisco 300-207 exam: Using latest released Lead2pass 300-207 exam questions, quickly pass 300-207 exam 100%! Following questions and answers are all new published by Cisco Official Exam Center! Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/300-207.html QUESTION 81 An ASA with an IPS module must be configured to drop traffic matching IPS signatures and block all traffic if the module fails. Which describes the correct configuration? A. Inline Mode, Permit Traffic B. Inline Mode, Close Traffic C. Promiscuous Mode, Permit Traffic D. Promiscuous Mode, Close TrafficAnswer: B QUESTION 82 A new Cisco IPS device has been placed on the network without prior analysis. Which CLI command shows the most fired signature? A. Show statistics virtual-sensor B. Show event alert C. Show alert D. Show version Answer: A QUESTION 83 Which three options are characteristics of router-based IPS? (Choose three.) A. It is used for large networks. B. It is used for small networks. C. It supports virtual sensors. D. It supports multiple VRFs. E. It uses configurable anomaly detection. F. Signature definition files have been deprecated. Answer: BDF QUESTION 84 What are three best practices for a Cisco Intrusion Prevention System? (Choose three.) A. Checking for new signatures every 4 hours B. Checking for new signatures on a staggered schedule C. Automatically updating signature packs D. Manually updating signature packs E. Group tuning of signatures F. Single tuning of signatures Answer: BCE QUESTION 85 Which three statements concerning keystroke logger detection are correct? (Choose three.) A. requires administrative privileges in order to run B. runs on Windows and MAC OS X systems C. detects loggers that run as a process or kernel module D. detects both hardware- and software-based keystroke loggers E. allows the administrator to define "safe" keystroke logger applications Answer: ACE QUESTION 86 Which three webtype ACL statements are correct? (Choose three.) A. are assigned per-Connection Profile B. are assigned per-user or per-Group Policy C. can be defined in the Cisco AnyConnect Profile Editor D. supports URL pattern matching E. supports implicit deny all at the end of the ACL F. supports standard and extended webtype ACLs Answer: BDE QUESTION 87 Which four advanced endpoint assessment statements are correct? (Choose four.) A. examines the remote computer for personnel firewalls applications B. examines the remote computer for antivirus applications C. examines the remote computer for antispyware applications D. examines the remote computer for malware applications E. does not perform any remediation but provides input that can be evaluated by DAP records F. performs active remediation by applying rules, activating modules, and providing updates where applicable Answer: ABCF QUESTION 88 Which statement regarding hashing is correct? A. MD5 produces a 64-bit message digest B. SHA-1 produces a 160-bit message digest C. MD5 takes more CPU cycles to compute than SHA-1. D. Changing 1 bit of the input to SHA-1 can change up to 5 bits in the output. Answer: B QUESTION 89 What is the access-list command on a Cisco IPS appliance used for? A. to permanently filter traffic coming to the Cisco IPS appliance via the sensing port B. to filter for traffic when the Cisco IPS appliance is in the inline mode C. to restrict management access to the sensor D. to create a filter that can be applied on the interface that is under attack Answer: C QUESTION 90 How does a user access a Cisco Web Security Appliance for initial setup? A. Connect the console cable and use the terminal at 9600 baud to run the setup wizard. B. Connect the console cable and use the terminal at 115200 baud to run the setup wizard. C. Open the web browser at 192.168.42.42:8443 for the setup wizard over https. D. Open the web browser at 192.168.42.42:443 for the setup wizard over https. Answer: C QUESTION 91 What command alters the SSL ciphers used by the Cisco Email Security Appliance for TLS sessions and HTTPS access? A. sslconfig B. sslciphers C. tlsconifg D. certconfig Answer: A QUESTION 92 Joe was asked to secure access to the Cisco Web Security Appliance to prevent unauthorized access. Which four steps should Joe implement to accomplish this goal? (Choose four.) A. Implement IP access lists to limit access to the management IP address in the Cisco Web Security Appliance GUI. B. Add the Cisco Web Security Appliance IP address to the local access list. C. Enable HTTPS access via the GUI/CLI with redirection from HTTP. D. Replace the Cisco self-signed certificate with a publicly signed certificate. E. Put the Cisco WSA Management interface on a private management VLAN. F. Change the netmask on the Cisco WSA Management interface to a 32-bit mask. G. Create an MX record for the Cisco Web Security Appliance in DNS. Answer: ACDE QUESTION 93 Which command is used to enable strong ciphers on the Cisco Web Security Appliance? A. interfaceconfig B. strictssl C. etherconfig D. adminaccessconfig Answer: B QUESTION 94 Which Cisco ESA command is used to edit the ciphers that are used for GUI access? A. interfaceconfig B. etherconfig C. certconfig D. sslconfig Answer: D QUESTION 95 In order to set up HTTPS decryption on the Cisco Web Security Appliance, which two steps must be performed? (Choose two.) A. Enable and accept the EULA under Security Services > HTTPS Proxy. B. Upload a publicly signed server certificate. C. Configure or upload a certificate authority certificate. D. Enable HTTPS decryption in Web

Security Manager > Access Policies. Answer: AC QUESTION 96 When a Cisco Email Security Appliance joins a cluster, which four settings are inherited? (Choose four.) A. IP address B. DNS settings C. SMTP routes D. HAT E. RAT F. hostname G. certificates Answer: BCDE QUESTION 97 The helpdesk was asked to provide a record of delivery for an important email message that a customer claims it did not receive. Which feature of the Cisco Email Security Appliance provides this record? A. Outgoing Mail Reports B. SMTP Routes C. Message Tracking D. Scheduled Reports E. System Administration Answer: C QUESTION 98 Connections are being denied because of SenderBase Reputation Scores. Which two features must be enabled in order to record those connections in the mail log on the Cisco ESA? (Choose two.) A. Rejected Connection Handling B. Domain Debug Logs C. Injection Debug Logs D. Message Tracking Answer: AD QUESTION 99 Which five system management and reporting protocols are supported by the Cisco Intrusion Prevention System? (Choose five.) A. SNMPv2c B. SNMPv1 C. SNMPv2 D. SNMPv3 E. syslog F. SDEE G. SMTP Answer: ABCFG QUESTION 100 Refer to the exhibit. The system administrator of mydomain.com received complaints that some messages that were sent from sender user@somedomain.com were delayed. Message tracking data on the sender shows that an email sample that was received was clean and properly delivered. What is the likely cause of the intermittent delays?



A. The remote MTA has a SenderBase Reputation Score of -1.0. B. The remote MTA is sending emails from RFC 1918 IP addresses. C. The remote MTA has activated the SUSPECTLIST sender group. D. The remote MTA has activated the default inbound mail policy. Answer: C Lead2pass is confident that our NEW UPDATED 300-207 exam questions and answers are changed with Cisco Official Exam Center. If you cannot pass 300-207 exam, never mind, we will return your full money back! Visit Lead2pass exam dumps collection website now and download 300-207 exam dumps instantly today! 300-207 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDM2V5bnM0dTVhYjg 2016 Cisco 300-207 exam dumps (All 251 Q&As) from Lead2pass: http://www.lead2pass.com/300-207.html [100% Exam Pass Guaranteed]