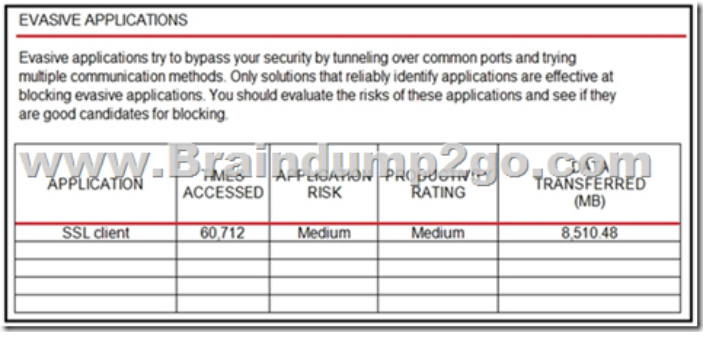
[January-2023Download Braindump2go 300-710 Exam VCE for Free[Q106-Q136

January/2023 Latest Braindump2go 300-710 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Updated 300-710 Real Exam Questions!QUESTION 106An organization is setting up two new Cisco FTD devices to replace their current firewalls and cannot have any network downtime. During the setup process, the synchronization between the two devices is failing.What action is needed to resolve this issue?A. Confirm that both devices have the same port-channel numberingB. Confirm that both devices are running the same software versionC. Confirm that both devices are configured with the same types of interfacesD. Confirm that both devices have the same flash memory sizesAnswer: DExplanation:The devices must have the same type and number of interfaces and software needs to be on same version.However, the question is specifically touching on synchronization issues.If you are using units with different flash memory sizes in your High Availability configuration, make sure the unit with the smaller flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger flash memory to the unit with the smaller flash memory will fail.
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/firepower_threat_defense_high_availability.htmlQUESTION 107There is an increased amount of traffic on the network and for compliance reasons, management needs visibility into the encrypted traffic.What is a result of enabling TLS'SSL decryption to allow this visibility?A. It prompts the need for a corporate managed certificateB. It has minimal performance impactC. It is not subject to any Privacy regulationsD. It will fail if certificate pinning is not enforcedAnswer: AQUESTION 108An organization wants to secure traffic from their branch office to the headquarter building using Cisco Firepower devices, They want to ensure that their Cisco Firepower devices are not wasting resources on inspecting the VPN traffic. What must be done to meet these requirements?A. Configure the Cisco Firepower devices to ignore the VPN traffic using prefilter policiesB. Enable a flexconfig policy to re-classify VPN traffic so that it no longer appears as interesting trafficC. Configure the Cisco Firepower devices to bypass the access control policies for VPN traffic.D. Tune the intrusion policies in order to allow the VPN traffic through without inspectionAnswer: CExplanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-ravpn.htmlQUESTION 109 A network administrator is seeing an unknown verdict for a file detected by Cisco FTD.Which malware policy configuration option must be selected in order to further analyse the file in the Talos cloud?A. Spero analysisB. Malware analysisC. Dynamic analysisD. Sandbox analysisAnswer: CExplanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.htmlQUESTION 110An engineer has been tasked with providing disaster recovery for an organization's primary Cisco FMC. What must be done on the primary and secondary Cisco FMCs to ensure that a copy of the original corporate policy is available if the primary Cisco FMC fails?A. Configure high-availability in both the primary and secondary Cisco FMCsB. Connect the primary and secondary Cisco FMC devices with Category 6 cables of not more than 10 meters in length.C. Place the active Cisco FMC device on the same trusted management network as the standby deviceD. Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device failsAnswer: AExplanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.htmlQUESTION 111An engineer is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of ACME001 and a password of Cisco388267669.Which command set must be used in order to accomplish this?A. configure manager add ACME001 <registration key> <FMC IP>B. configure manager add <FMC IP> ACME0O1 <registration key>C. configure manager add DONTRESOLVE <FMC IP> AMCE001 <registration key>D. configure manager add <FMC IP> registration key> ACME001Answer: DExplanation:
https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118596-configure-firesight-00.htmlQUESTION 112Refer to the exhibit. An organization has an access control rule with the intention of sending all social media traffic for inspection. After using the rule for some time, the administrator notices that the traffic is not being inspected, but is being automatically allowed.What must be done to address this issue?

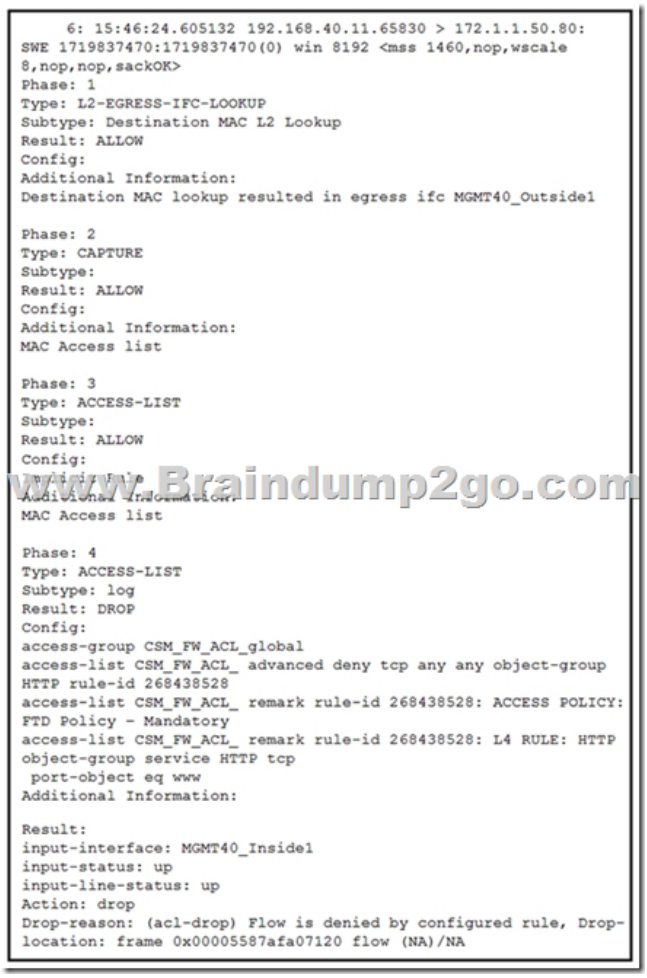
A. Modify the selected application within the ruleB. Change the intrusion policy to connectivity over security.C. Modify the rule action from trust to allowD. Add the social network URLs to the block listAnswer: CExplanation:Rule 4: Allow is the final rule. For this rule, matching traffic is allowed; however, prohibited files, malware, intrusions, and exploits within that traffic are detected and blocked. Remaining non-prohibited, non-malicious traffic is allowed to its destination, though it is still subject to identity requirements and rate limiting. You can configure Allow rules that perform only file inspection, or only intrusion inspection, or neither.
https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/access_control_rules.htmlQUESTION 113A user within an organization opened a malicious file on a workstation which in turn caused a ransomware attack on the network.What should be configured within the Cisco FMC to ensure the file is tested for viruses on a sandbox system?A. Capacity handlingB. Local malware analysisC. Spere analysisD. Dynamic analysisAnswer: DExplanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html#ID-2199-000005faQUESTION 114An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events filing the database and overloading the Cisco FMC. A monitored NAT device is executing multiple updates of its operating system in a short period of time. What configuration change must be made to alleviate this issue?A. Leave default networks.B. Change the method to TCP/SYN.C. Increase the number of entries on the NAT device.D. Exclude load balancers and NAT devices.Answer: DExplanation:The system can identify many load balancers and NAT devices by examining your network traffic.
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Network_Discovery_Policies.htmlQUESTION 115administrator is configuring SNORT inspection policies and is seeing failed deployment messages in Cisco FMC. What information should the administrator generate for Cisco TAC to help troubleshoot?A. A Troubleshoot" file for the device in question.B. A "show tech" file for the device in questionC. A "show tech" for the Cisco FMC.D. A "troubleshoot" file for the Cisco FMCAnswer: DExplanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.htmlQUESTION 117A network engineer is receiving reports of users randomly getting disconnected from their corporate applications which traverses the data center FTD appliance Network monitoring tools show that the FTD appliance utilization is peaking above 90% of total capacity. What must be done in order to further analyze this issue?A. Use the Packet Export feature to save data onto external drivesB. Use the Packet Capture feature to collect real-time network trafficC. Use the Packet Tracer feature for traffic policy analysisD. Use the Packet Analysis feature for capturing network dataAnswer: BExplanation:
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html
QUESTION 118IT management is asking the network engineer to provide high-level summary statistics of the Cisco FTD appliance in the network. The business is approaching a peak season so the need to maintain business uptime is high. Which report type should be used to gather this information?A. Malware ReportB. Standard ReportC. SNMP ReportD. Risk ReportAnswer: D Explanation:Because the report is for non security specialist and will come with recommendations that will help to issues during a period of peaks.The Firepower System offers two types of reports:Risk Reports - High-level summaries of risks found on your network.Standard Reports - Detailed, customizable reports about all aspects of your Firepower System.Risk ReportsRisk reports are portable, high-level, easy-to-interpret summaries of risks found in your organization. You can use these reports to share information about areas of risk, and recommendations for addressing these risks, with people who do not have access to your system and who may not be network security experts. These reports are intended to facilitate discussion about areas for investment in the security of your network.QUESTION 119Refer to the exhibit. An administrator is looking at some of the reporting capabilities for Cisco Firepower and noticed this section of the Network Risk report showing a lot of SSL activity that cloud be used for evasion. Which action will mitigate this risk?


EVASIVE APPLICATIONS

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
SSL client	60,712	Medium	Medium	8,510.48

A. Use SSL decryption to analyze the packets.B. Use encrypted traffic analytics to detect attacksC. Use Cisco AMP for Endpoints to block all SSL connectionD. Use Cisco Tetration to track SSL connections to servers.Answer: AExplanation: https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-ssl-decryption.html
QUESTION 120An administrator is setting up Cisco Firepower to send data to the Cisco Stealthwatch appliances. The NetFlow_Set_Parameters object is already created, but NetFlow is not being sent to the flow collector. What must be done to prevent this from occurring?A. Add the NetFlow_Send_Destination object to the configurationB. Create a Security Intelligence object to send the data to Cisco StealthwatchC. Create a service identifier to enable the NetFlow serviceD. Add the NetFlow_Add_Destination object to the configurationAnswer: DQUESTION 121With a recent summer time change, system logs are showing activity that occurred to be an hour behind real time. Which action should be taken to resolve this issue?A. Manually adjust the time to the correct hour on all managed devicesB. Configure the system clock settings to use NTP with Daylight Savings checkedC. Manually adjust the time to the correct hour on the Cisco FMC.D. Configure the system clock settings to use NTPAnswer: DExplanation:Note that the time displayed on most pages on the web interface is the local time, which is determined by using the time zone you specify in your local configuration. Further, the Firepower Management Center automatically adjusts its local time display for daylight saving time (DST), where appropriate. However, recurring tasks that span the transition dates from DST to standard time and back do not adjust for the transition. That is, if you create a task scheduled for 2:00 AM during standard time, it will run at 3:00 AM during DST. Similarly, if you create a task scheduled for 2:00 AM during DST, it will run at 1:00 AM during standard time.#Documentation: Configuring a Recurring Task
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Scheduling_Tasks.html
QUESTION 122A network administrator notices that SI events are not being updated The Cisco FTD device is unable to load all of the SI event entries and traffic is not being blocked as expected.What must be done to correct this issue?A. Restart the affected devices in order to reset the configurationsB. Manually update the SI event entries to that the appropriate traffic is blockedC. Replace the affected devices with devices that provide more memoryD. Redeploy configurations to affected devices so that additional memory is allocated to the SI moduleAnswer: DExplanation:Workaround: If you think this is happening, redeploy configurations to the affected devices.
https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/security_intelligence_blacklisting.htmlQUESTION 123Refer to the exhibit. What must be done to fix access to this website while preventing the same communication to all other websites?



A. Create an intrusion policy rule to have Snort allow port 80 to only 172.1.1.50.B. Create an intrusion policy rule to have Snort allow port 443 to only 172.1.1.50.C. Create an access control policy rule to allow port 443 to only 172.1.1.50.D. Create an access control policy rule to allow port 80 to only 172.1.1.50.Answer: DQUESTION 124A network administrator discovers that a user connected to a file server and downloaded a malware file. The Cisc FMC generated an alert for the malware event, however the user still remained connected. Which Cisco APM file rule action within the Cisco FMC must be set to resolve this issue?A. Detect FilesB. Malware Cloud LookupC. Local Malware AnalysisD. Reset ConnectionAnswer: DExplanation:Cisco recommends that you enable Reset Connection for the Block Files and Block Malware actions to prevent blocked application sessions from remaining open until the TCP connection resets. If you do not reset connections, the client session will remain open until the TCP connection resets itself.QUESTION 125Which feature within the Cisco FMC web interface allows for detecting, analyzing and blocking malware in network traffic?A. intrusion and file eventsB. Cisco AMP for EndpointsC. Cisco AMP for NetworksD. file policiesAnswer: CExplanation:Advanced Malware Protection (AMP) for Firepower can detect, capture, track, analyze, log, and optionally block the transmission of malware in network traffic. In the Firepower Management Center web interface, this feature is called AMP for Networks, formerly called AMP for Firepower. Advanced Malware Protection identifies malware using managed devices deployed inline and threat data from the Cisco cloud.
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_policies_and_advanced_malware_protection.htmlQUESTION 126Which license type is required on Cisco ISE to integrate with Cisco FMC pxGrid?A. mobilityB. plusC. baseD. apexAnswer: CExplanation:Only base licensing is required for pxGrid integration. You can use PassiveID with just base licensing which passes that onto the FMC through pxGrid. If you want to use context sharing and Rapid Threat Containment, THEN you need Plus licensing.https://www.routexp.com/2017/11/cisco-ise-base-plus-and-apex-licenses.html
QUESTION 127A network engineer wants to add a third-party threat feed into the Cisco FMC for enhanced threat detection Which action should be taken to accomplish this goal?A. Enable Threat Intelligence Director using STIX and TAXIIB. Enable Rapid Threat Containment using REST APIsC. Enable Threat Intelligence Director using REST APIsD. Enable Rapid Threat Containment using STIX and TAXIIAnswer: AExplanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisco_threat_intelligence_director__tid_.htmlQUESTION 128What is a feature of Cisco AMP private cloud?A. It supports anonymized retrieval of threat intelligenceB. It supports security intelligence filtering.C. It disables direct connections to the public cloud.D. It performs dynamic analysisAnswer: CExplanation:Connecting a Firepower Management Center to an AMP private cloud disables existing direct connections to the public AMP cloud.
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/file_policies_and_amp_for_firepower.htmlQUESTION 129An engineer has been tasked with using Cisco FMC to determine if files being sent through the network are malware.Which two configuration tasks must be performed to achieve this file lookup? (Choose two.)A. The Cisco FMC needs to include a SSL decryption policy.B. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.C. The Cisco FMC needs to connect to the Cisco ThreatGrid service directly for sandboxing.D. The Cisco FMC needs to connect with the FireAMP Cloud.E. The Cisco FMC needs to include a file inspection policy for malware lookup.Answer: AEExplanation: Bobster is referencing local malware analysis requirements, but we have no information that local malware analysis is begin used. By default theat grid is used, and threat grid needs no configuration on the FMC to connect to the cloud. The question states "which configuration tasks" - we dont need to do anything related to threat grid afaik.QUESTION 130An organization is using a Cisco FTD and Cisco ISE to perform identity-based access controls. A network administrator is analyzing the Cisco FTD events and notices that unknown user traffic is being allowed through the firewall.How should this be addressed to block the traffic while allowing legitimate user traffic?A. Modify the Cisco ISE authorization policy to deny this access to the user.B. Modify Cisco ISE to send only legitimate usernames to the Cisco FTD.C. Add the unknown user in the Access Control Policy in Cisco FTD.D. Add the unknown user in the Malware & File Policy in Cisco FTD.Answer: CQUESTION 131An engineer is restoring a Cisco FTD configuration from a remote backup using the command restore remote-manager-backup location 1.1.1.1 admin /volume/home/admin BACKUP_Cisc394602314.zip on a Cisco FMG. After connecting to the repository, an error occurred that prevents the FTD device from accepting the backup file. What is the problem?A. The backup file is not in .cfg format.B. The backup file is too large for the Cisco FTD deviceC. The backup file extension was changed from tar to zipD. The backup file was not enabled prior to being appliedAnswer: CQUESTION 132A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?A. Add the hash to the simple custom deletion list.B. Use regular expressions to block the malicious file.C. Enable a personal firewall in the infected endpoint.D. Add the hash from the infected endpoint to the network block list.Answer: AQUESTION 133A network

engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?A. Specify the BVl IP address as the default gateway for connected devices.B. Enable routing on the Cisco FirepowerC. Add an IP address to the physical Cisco Firepower interfaces.D. Configure a bridge group in transparent mode.Answer: DExplanation:Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a ?bump in the wire,? or a ?stealth firewall,? and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place.Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other. https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.htmlQUESTION 134An organization has a Cisco IPS running in inline mode and is inspecting traffic for malicious activity. When traffic is received by the Cisco IRS, if it is not dropped, how does the traffic get to its destination?A. It is retransmitted from the Cisco IPS inline set.B. The packets are duplicated and a copy is sent to the destination.C. It is transmitted out of the Cisco IPS outside interface.D. It is routed back to the Cisco ASA interfaces for transmission.Answer: AExplanation:Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped. https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v60_chapter_01011010.pdfQUESTION 135A network administrator is concerned about the high number of malware files affecting users' machines. What must be done within the access control policy in Cisco FMC to address this concern?A. Create an intrusion policy and set the access control policy to block.B. Create an intrusion policy and set the access control policy to allow.C. Create a file policy and set the access control policy to allow.D. Create a file policy and set the access control policy to block.Answer: C Explanation:Access control rules:Rule 3: Block evaluates traffic third. Matching traffic is blocked without further inspection. Traffic that does not match continues to the final rule.Rule 4: Allow is the final rule. For this rule, matching traffic is allowed; however, prohibited files, malware, intrusions, and exploits within that traffic are detected and blocked. Remaining non-prohibited, non-malicious traffic is allowed to its destination, though it is still subject to identity requirements and rate limiting. You can configure Allow rules that perform only file inspection, or only intrusion inspection, or neither.QUESTION 136An engineer is investigating connectivity problems on Cisco Firepower that is using service group tags. Specific devices are not being tagged correctly, which is preventing clients from using the proper policies when going through the firewall How is this issue resolved?A. Use traceroute with advanced options.B. Use Wireshark with an IP subnet filter.C. Use a packet capture with match criteria.D. Use a packet sniffer with correct filteringAnswer: CExplanation:Capture could just be exported and imported in wireshark. Also, you would be able to use match argument to specify devices instead of subnet, and also SGTs if you want to. Resources From:1.2022 Latest Braindump2go 300-710 Exam Dumps (PDF & VCE) Free Share: https://www.braindump2go.com/300-710.html2.2022 Latest Braindump2go 300-710 PDF and 300-710 VCE Dumps Free Share: https://drive.google.com/drive/folders/1k8dhswD5V9ioQSctkVOlp0ooiELn46gL?usp=sharingFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!