[May-2021Exam Pass 100%!Braindump2go 300-710 PDF Dumps 300-710 153 Instant Download[Q130-Q153

May/2021 Latest Braindump2go 300-710 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 300-710 Real Exam Questions!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: CQUESTION 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: DQUESTION 135A network administrator is concerned about (he 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: DQUESTION 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: AQUESTION 137A connectivity issue is occurring between a client and a server which are communicating through a Cisco Firepower device While troubleshooting, a network administrator sees that traffic is reaching the server, but the client is not getting a response.Which step must be taken to resolve this issue without initiating traffic from the client?A. Use packet-tracer to ensure that traffic is not being blocked by an access list.B. Use packet capture to ensure that traffic is not being blocked by an access list.C. Use packet capture to validate that the packet passes through the firewall and is NATed to the corrected IP address.D. Use packet-tracer to validate that the packet passes through the firewall and is NATed to the corrected IP address.Answer: DQUESTION 138An organization must be able to ingest NetFlow traffic from their Cisco FTD device to Cisco Stealthwatch for behavioral analysis.What must be configured on the Cisco FTD to meet this requirement?A. flexconfig object for NetFlowB. interface object to export NetFlowC. security intelligence object for NetFlowD. variable set object for NetFlowAnswer: AQUESTION 139An engineer is tasked with deploying an internal perimeter firewall that will support multiple DMZs Each DMZ has a unique private IP subnet range. How is this requirement satisfied?A. Deploy the firewall in transparent mode with access control policies.B. Deploy the firewall in routed mode with access control policies.C. Deploy the firewall in routed mode with NAT configured.D. Deploy the firewall in transparent mode with NAT configured.Answer: BQUESTION 140An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down.What must be configured to accomplish this task?A. redundant interfaces on the firewall cluster mode and switchesB. redundant interfaces on the firewall noncluster mode and switchesC. vPC on the switches to the interface mode on the firewall dusterD. vPC on the switches to the span EtherChannel on the firewall clusterAnswer: DQUESTION 141What is the advantage of having Cisco Firepower devices send events to Cisco Threat

Response via the security services exchange portal directly as opposed to using syslog?A. All types of Cisco Firepower devices are supported.B. An on-premises proxy server does not need to be set up and maintained.C. Cisco Firepower devices do not need to be connected to the Internet.D. Supports all devices that are running supported versions of Cisco Firepower.Answer: BQUESTION 142A network administrator notices that remote access VPN users are not reachable from inside the network. It is determined that routing is configured correctly, however return traffic is entering the firewall but not leaving it.What is the reason for this issue?A. A manual NAT exemption rule does not exist at the top of the NAT table.B. An external NAT IP address is not configured.C. An external NAT IP address is configured to match the wrong interface.D. An object NAT exemption rule does not exist at the top of the NAT table.Answer: DQUESTION 143An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic concurrently.How must the devices be implemented in this environment?A. in active/active modeB. in a cluster span EtherChannelC. in active/passive modeD. in cluster interface modeAnswer: CQUESTION 144When deploying a Cisco ASA Firepower module, an organization wants to evaluate the contents of the traffic without affecting the network. It is currently configured to have more than one instance of the same device on the physical appliance.Which deployment mode meets the needs of the organization?A. inline tap monitor-only modeB. passive monitor-only modeC. passive tap monitor-only modeD. inline modeAnswer: BQUESTION 145A network administrator notices that inspection has been interrupted on all non-managed interfaces of a device. What is the cause of this?A. The value of the highest MTU assigned to any non-management interface was changed.B. The value of the highest MSS assigned to any non-management interface was changed.C. A passive interface was associated with a security zone.D. Multiple inline interface pairs were added to the same inline interface.Answer: AQUESTION 146An administrator is creating interface objects to better segment their network but is having trouble adding interfaces to the objects. What is the reason for this failure?A. The interfaces are being used for NAT for multiple networks.B. The administrator is adding interfaces of multiple types.C. The administrator is adding an interface that is in multiple zones.D. The interfaces belong to multiple interface groups.Answer: DQUESTION 147Which two conditions must be met to enable high availability between two Cisco FTD devices? (Choose two.)A. same flash memory sizeB. same NTP configurationC. same DHCP/PPoE configurationD. same host nameE. same number of interfacesAnswer: BEQUESTION 148 A network administrator 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 "show tech" file for the device in question. B. A "troubleshoot" file for the device in question.C. A "troubleshoot" file for the Cisco FMC.D. A "show tech" for the Cisco FMC.Answer: BQUESTION 149An engineer is building a new access control policy using Cisco FMC. The policy must inspect a unique IPS policy as well as log rule matching.Which action must be taken to meet these requirements?A. Configure an IPS policy and enable per-rule logging.B. Disable the default IPS policy and enable global logging.C. Configure an IPS policy and enable global logging.D. Disable the default IPS policy and enable per-rule logging.Answer: AQUESTION 150A network administrator needs to create a policy on Cisco Firepower to fast-path traffic to avoid Layer 7 inspection. The rate at which traffic is inspected must be optimized. What must be done to achieve this goal?A. Enable the FXOS for multi-instance.B. Configure a prefilter policy.C. Configure modular policy framework.D. Disable TCP inspection.Answer: BQUESTION 151A network engineer is tasked with minimising traffic interruption during peak traffic limes.When the SNORT inspection engine is overwhelmed, what must be configured to alleviate this issue?A. Enable IPS inline link state propagationB. Enable Pre-filter policies before the SNORT engine failure.C. Set a Trust ALL access control policy.D. Enable Automatic Application Bypass.Answer: DQUESTION 152A VPN user is unable to conned lo web resources behind the Cisco FTD device terminating the connection. While troubleshooting, the network administrator determines that the DNS responses are not getting through the Cisco FTD.What must be done to address this issue while still utilizing Snort IPS rules?A. Uncheck the "Drop when Inline" box in the intrusion policy to allow the traffic.B. Modify the Snort rules to allow legitimate DNS traffic to the VPN users.C. Disable the intrusion rule threshes to optimize the Snort processing.D. Decrypt the packet after the VPN flow so the DNS queries are not inspectedAnswer: BQUESTION 153An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighbouring Cisco devices or use multicast in their environment. What must be done to resolve this issue?A. Create a firewall rule to allow CDP traffic.B. Create a bridge group with the firewall interfaces. C. Change the firewall mode to transparent.D. Change the firewall mode to routed.Answer: DResources From:1.2021 Latest Braindump2go 300-710 Exam Dumps (PDF & VCE) Free Share:https://www.braindump2go.com/300-710.html2.2021 Latest Braindump2go 300-710 PDF and 300-710 VCE Dumps Free Share: https://drive.google.com/drive/folders/1k8dhswD5V9ioQSctkVOlp0ooiELn46gL?usp=sharing3.2021 Free Braindump2go 300-710 Exam Questions Download:https://www.braindump2go.com/free-online-pdf/300-710-PDF-Dumps(130-153).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!