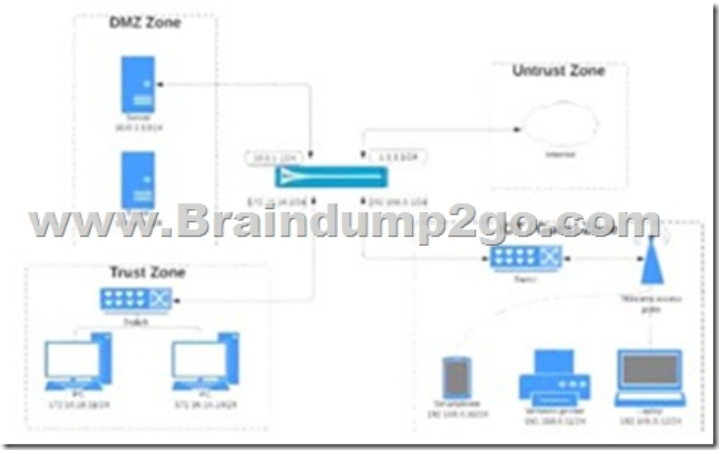
[May-2022Free PCNSA 273Q PCNSA Exam Dumps Braindump2go Offer[Q254-Q266

May/2022 Latest PCNSA Exam Dumps with PDF and VCE Free Updated Today! Following are some new PCNSA Real Exam Questions!QUESTION 254Which DNS Query action is recommended for traffic that is allowed by Security policy and matches Palo Alto Networks Content DNS Signatures?A. blockB. sinkholeC. alertD. allowAnswer: BExplanation:To enable DNS sinkholing for domain queries using DNS security, you must activate your DNS Security subscription, create (or modify) an Anti-Spyware policy to reference the DNS Security service, configure the log severity and policy settings for each DNS signature category, and then attach the profile to a security policy rule.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns-security/enable-dns-securityQUESTION 255 Which stage of the cyber-attack lifecycle makes it important to provide ongoing education to users on spear phishing links, unknown emails, and risky websites?A. reconnaissanceB. deliveryC. exploitationD. installationAnswer: BExplanation:Weaponization and Delivery: Attackers will then determine which methods to use in order to deliver malicious payloads. Some of the methods they might utilize are automated tools, such as exploit kits, spear phishing attacks with malicious links, or attachments and malvertizing. Gain full visibility into all traffic, including SSL, and block high-risk applications. Extend those protections to remote and mobile devices.Protect against perimeter breaches by blocking malicious or risky websites through URL filtering. Block known exploits, malware and inbound command-and-control communications using multiple threat prevention disciplines, including IPS, anti-malware, anti-CnC, DNS monitoring and sinkholing, and file and content blocking.Detect unknown malware and automatically deliver protections globally to thwart new attacks. Provide ongoing education to users on spear phishing links, unknown emails, risky websites, etc.https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycleQUESTION 256What are three factors that can be used in domain generation algorithms? (Choose three.)A. cryptographic keysB. time of dayC. other unique valuesD. URL custom categoriesE. IP addressAnswer: ABCExplanation:Domain generation algorithms (DGAs) are used to auto-generate domains, typically in large numbers within the context of establishing a malicious command-and-control (C2) communications channel. DGA-based malware (such as Pushdo, BankPatch, and CryptoLocker) limit the number of domains from being blocked by hiding the location of their active C2 servers within a large number of possible suspects, and can be algorithmically generated based on factors such as time of day, cryptographic keys, or other unique values.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security/domain-generation-algorithm-detection
QUESTION 257Which action would an administrator take to ensure that a service object will be available only to the selected device group?A. create the service object in the specific templateB. uncheck the shared optionC. ensure that disable override is selectedD. ensure that disable override is clearedAnswer: DExplanation:
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-device-groups/create-objects-for-use-in-shared-or-device-group-policyQUESTION 258If using group mapping with Active Directory Universal Groups, what must you do when configuring the User-ID?A. Create an LDAP Server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSLB. Configure a frequency schedule to clear group mapping cacheC. Configure a Primary Employee ID number for user-based Security policiesD. Create a RADIUS Server profile to connect to the domain controllers using LDAPS on port 636 orAnswer: AExplanation:If you have Universal Groups, create an LDAP server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL, then create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that users and group information is available for all domains and subdomains.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groupsQUESTION 259Which administrative management services can be configured to access a management interface?A. HTTP, CLI, SNMP, HTTPSB. HTTPS, SSH telnet SNMPC. SSH: telnet HTTP, HTTPSD. HTTPS, HTTP. CLI, APIAnswer: DExplanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/management-interfacesYou can use the following user interfaces to manage the Palo Alto Networks firewall:Use the Web Interface to perform configuration and monitoring tasks with relative ease. This graphical interface allows you to access the firewall using HTTPS (recommended) or HTTP and it is the best way to perform administrative tasks.Use the Command Line Interface (CLI) to perform a series of tasks by entering commands in rapid succession over SSH (recommended), Telnet, or the console port. The CLI is a no-frills interface that supports two command modes, operational and configure, each with a distinct hierarchy of commands and statements. When you become familiar with the nesting structure and syntax of the commands, the CLI provides quick response times and administrative efficiency. Use the XML API to streamline your operations and integrate with existing, internally developed applications and repositories. The XML API is a web service implemented using HTTP/HTTPS requests and responses.Use Panorama to perform

web-based management, reporting, and log collection for multiple firewalls. The Panorama web interface resembles the firewall web interface but with additional functions for centralized management.QUESTION 260Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?A. Palo Alto Networks Bulletproof IP AddressesB. Palo Alto Networks C&C IP AddressesC. Palo Alto Networks Known Malicious IP AddressesD. Palo Alto Networks High-Risk IP AddressesAnswer: AExplanation:To block hosts that use bulletproof hosts to provide malicious, illegal, and/or unethical content, use the bulletproof IP address list in policy.QUESTION 261Which attribute can a dynamic address group use as a filtering condition to determine its membership?A. tagB. wildcard maskC. IP addressD. subnet maskAnswer: AExplanation:Dynamic Address Groups: A dynamic address group populates its members dynamically using looks ups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall.
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-address-groupsQUESTION 262View the diagram. What is the most restrictive yet fully functional rule to allow general Internet and SSH traffic into both the DMZ and Untrust/lnternet zones from each of the lOT/Guest and Trust Zones?



A.


B.


C.


D.


Answer: CQUESTION 263An administrator needs to add capability to perform real-time signature lookups to block or sinkhole all known malware domains.Which type of single unified engine will get this result?A. User-IDB. App-IDC. Security Processing EngineD. Content-IDAnswer: AQUESTION 264Which solution is a viable option to capture user identification when Active Directory is not in use?A. Cloud Identity EngineB. group mappingC. Directory Sync ServiceD. Authentication PortalAnswer: DQUESTION 265You receive notification about a new malware that infects hosts. An infection results in the infected host attempting to contact a command-and-control server. Which Security Profile when applied to outbound Security policy rules detects and prevents this threat from establishing a command-and-control connection?A. Antivirus ProfileB. Data Filtering

ProfileC. Vulnerability Protection ProfileD. Anti-Spyware ProfileAnswer: DExplanation:Anti-Spyware Security Profiles block spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus enabling you to detect malicious traffic leaving the network from infected clients.QUESTION 266Which built-in IP address EDL would be useful for preventing traffic from IP addresses that are verified as unsafe based on WildFire analysis Unit 42 research and data gathered from telemetry?A. Palo Alto Networks C&C IP AddressesB. Palo Alto Networks Bulletproof IP AddressesC. Palo Alto Networks High-Risk IP AddressesD. Palo Alto Networks Known Malicious IP AddressesAnswer: DExplanation:Palo Alto Networks Known Malicious IP Addresses--Contains IP addresses that are verified malicious based on WildFire analysis, Unit 42 research, and data gathered from telemetry (Share Threat Intelligence with Palo Alto Networks). Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/built-in-edlsResources From:1.2022 Latest Braindump2go PCNSA Exam Dumps (PDF & VCE) Free Share: https://www.braindump2go.com/pcnsa.html2.2022 Latest Braindump2go PCNSA PDF and PCNSA VCE Dumps Free Share: https://drive.google.com/drive/folders/1_IuXSO289LtQJX5BZt3iARfEaVckaP-x?usp=sharing3.2021 Free Braindump2go PCNSA Exam Questions Download:https://www.braindump2go.com/free-online-pdf/PCNSA-PDF-Dumps(254-266).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!