[January 2018 SY0-401 New Questions Free Download In Lead2pass 1868q

SY0-401 Exam Questions Free Download From Lead2pass: https://www.lead2pass.com/sy0-401.html QUESTION 1Which of the following should be deployed to prevent the transmission of malicious traffic between virtual machines hosted on a singular physical device on a network? A. HIPS on each virtual machineB. NIPS on the networkC. NIDS on the networkD. HIDS on each virtual machineAnswer: AExplanation:Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. QUESTION 2Which of the following components of an all-in-one security appliance would MOST likely be configured in order to restrict access to peer-to-peer file sharing websites? A. Spam filterB. URL filterC. Content inspectionD. Malware inspection Answer: BExplanation:The question asks how to prevent access to peer-to-peer file sharing websites. You access a website by browsing to a URL using a Web browser or peer-to-peer file sharing client software. A URL filter is used to block URLs (websites) to prevent users accessing the website.Incorrect Answer:A: A spam filter is used for email. All inbound (and sometimes outbound) email is passed through the spam filter to detect spam emails. The spam emails are then discarded or tagged as potential spam according to the spam filter configuration. Spam filters do not prevent users accessing peer- to-peer file sharing websites.C: Content inspection is the process of inspecting the content of a web page as it is downloaded. The content can then be blocked if it doesn't comply with the company's web policy. Content- control software determines what content will be available or perhaps more often what content will be blocked. Content inspection does not prevent users accessing peer-to-peer file sharing websites (although it could block the content of the sites as it is downloaded).D: Malware inspection is the process of scanning a computer system for malware. Malware inspection does not prevent users accessing peer-to-peer file sharing websites. QUESTION 3Pete, the system administrator, wants to restrict access to advertisements, games, and gambling web sites. Which of the following devices would BEST achieve this goal? A. FirewallB. SwitchC. URL content filterD. Spam filter Answer: CExplanation:URL filtering, also known as web filtering, is the act of blocking access to a site based on all or part of the URL used to request access. URL filtering can focus on all or part of a fully qualified domain name (FQDN), specific path names, specific filenames, specific fi le extensions, or entire specific URLs. Many URL-filtering tools can obtain updated master URL block lists from vendors as well as allow administrators to add or remove URLs from a custom list. QUESTION 4The administrator receives a call from an employee named Joe. Joe says the Internet is down and he is receiving a blank page when typing to connect to a popular sports website. The administrator asks Joe to try visiting a popular search engine site, which Joe reports as successful. Joe then says that he can get to the sports site on this phone. Which of the following might the administrator need to configure? A. The access rules on the IDSB. The pop up blocker in the employee's browserC. The sensitivity level of the spam filterD. The default block page on the URL filter Answer: DExplanation:A URL filter is used to block access to a site based on all or part of a URL. There are a number of URL-filtering tools that can acquire updated master URL block lists from vendors, as well as allow administrators to add or remove URLs from a custom list. QUESTION 5Layer 7 devices used to prevent specific types of html tags are called: A. FirewallsB. Content filtersC. RoutersD. NIDS Answer: BExplanation:A content filter is a is a type of software designed to restrict or control the content a reader is authorised to access, particularly when used to limit material delivered over the Internet via the Web, e-mail, or other means. Because the user and the OSI layer interact directly with the content filter, it operates at Layer 7 of the OSI model. QUESTION 6Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site? A. Internet content filterB. FirewallC. Proxy serverD. Protocol analyzer Answer: AExplanation:Web filtering software is designed to restrict or control the content a reader is authorised to access, especially when utilised to restrict material delivered over the Internet via the Web, e-mail, or other means. QUESTION 7A review of the company's network traffic shows that most of the malware infections are caused by users visiting gambling and gaming websites. The security manager wants to implement a solution that will block these websites, scan all web traffic for signs of malware, and block the malware before it enters the company network. Which of the following is suited for this purpose? A. ACLB. IDSC. UTMD. Firewall Answer: CExplanation:An all-in-one appliance, also known as Unified Threat Management (UTM) and Next Generation Firewall (NGFW), is one that provides a good foundation for security. A variety is available; those that you should be familiar with for the exam fall under the categories of providing URL filtering, content inspection, or malware inspection.Malware inspection is the use of a malware scanner to detect unwanted software content in network traffic. If malware is detected, it can be blocked or logged and/or trigger an alert. QUESTION 8Which of the following is BEST at blocking attacks and providing security at layer 7 of the OSI model? A. WAFB. NIDSC. RoutersD. Switches Answer: AExplanation:A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By

customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.As the protocols used to access a web server (typically HTTP and HTTPS) run in layer 7 of the OSI model, then web application firewall (WAF) is the correct answer. QUESTION 9Which of the following should the security administrator implement to limit web traffic based on country of origin? (Select THREE). A. Spam filterB. Load balancerC. AntivirusD. ProxiesE. FirewallF. NIDSG. URL filtering Answer: DEGExplanation:A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers.Firewalls manage traffic using a rule or a set of rules. A URL is a reference to a resource that specifies the location of the resource. A URL filter is used to block access to a site based on all or part of a URL. QUESTION 10A security engineer is reviewing log data and sees the output below: POST: /payload.php HTTP/1.1HOST: localhostAccept: */*Referrer: http://localhost/ *******HTTP/1.1 403 ForbiddenConnection: closeLog: Access denied with 403. Pattern matches form bypass Which of the following technologies was MOST likely being used to generate this log? A. Host-based Intrusion Detection SystemB. Web application firewallC. Network-based Intrusion Detection SystemD. Stateful Inspection FirewallE. URL Content Filter Answer: BExplanation:A web application firewall is a device, server add-on, virtual service, or system filter that defines a strict set of communication rules for a website and all visitors. It's intended to be an application- specific firewall to prevent cross-site scripting, SQL injection, and other web application attacks. **SY0-401 dumps full version (PDF&VCE):** https://www.lead2pass.com/sy0-401.html **Large amount of free SY0-401 exam questions on Google Drive:** https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E You may also need: SY0-501 exam dumps: https://drive.google.com/open?id=1Hm6GQHDVOsEnyhNf3EHqIGEtor5IUsfu