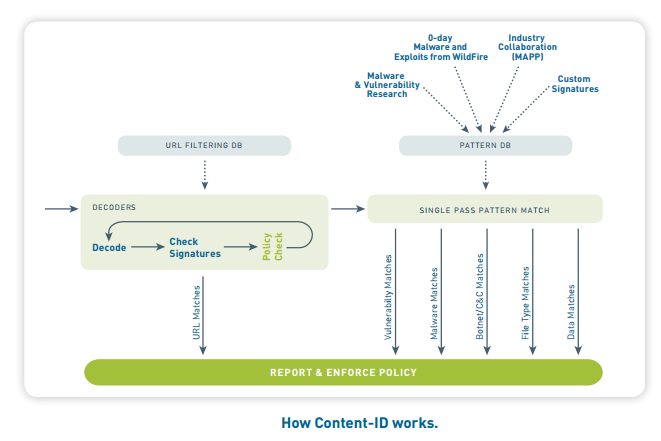
|  |  |
| --- | --- |
| **Network Security**  Diploma in CSF  Year 3 (Apr 2021) Semester 5 | Week 6 |
| Tutorial |
| **Content ID** | |

1. With reference to the diagram below, explain how the “Single Pass Pattern Match” is different from other multi-function firewalls.



|  |
| --- |
| • Content-ID is built on a single-pass architecture (SP3), it integrates multiple threat prevention disciplines (IPS, anti-malware, URL filtering, etc.) into a single stream-based engine with a uniform signature format.  • This allows traffic to be fully analyzed in a single pass without the incremental performance degradation seen in other multi-function gateways.  • The software is tied directly to a parallel processing hardware platform that uses function specific processors for threat prevention to maximizVhroughput and minimize latency. |

1. List and explain three security profiles that can be configured in a security policy.

|  |
| --- |
| There are 6 Security Profiles that can be configured in a security policy, namely:   1. Anti-Virus: Protects against worms and viruses , blocks spyware downloads   ii. Anti-Spyware: Blocks attempts by spyware to access the network.  iii. Vulnerability: Stops attempts to exploit system flaws or gain unauthorized access to systems  iv. URL Filtering: Restrict access to specific web sites and web site categories  v. File Blocking: Blocks selected file types  vi. Data Filtering: Prevents sensitive information such as credit card or social security numbers from leaving the area protected by the firewall  Anti-virus  The Anti-Virus profile defines actions to be taken if an infected file is detected as part of an application exchange. The listed applications represent the wide variety of vectors that modern viruses can take in infecting a system. For each application type an action can be defined.  The default action is to block any detected virus unless the protocol is POP3, IMAP or SMTP, then the default action is to alert. These three protocols are store-and-forward protocols: if an intermediate device drops the packets, SNMP/POP3/I MAP are designed to continually resend until the data is ultimately delivered. For these kinds of applications, the infected file needs to be removed at either the server or the client, not on the wire.  URL Filtering  A security policy can include specification of a URL filtering profile that blocks access to specific web sites and web site categories, or generates an alert when the specified web sites are accessed (a URL filtering license is required). You can also define a block list of web sites that are always blocked (or generate alerts) and an allow list of web sites that are always allowed. Pre-defined sets of web categories can be downloaded from Palo Alto Networks. PAN-OS supports two different URL filtering databases: loud PAN-DB. These URL filtering technologies will be discussed later in the module. Administrators can also define custom URL categories to customize the behavior of the URL filtering profiles. The URL Filtering feature can be used by placing categories directly in policies or attaching a URL Filtering profile to a security rule. URL filtering only affects HTTP and HTTPS traffic. The URL Category field can be used as a match condition for security, QoS, decryption, and Captive Portal policies. Both pre-defined and custom categories can be matched when using the URL category field. The URL category itself does not have an associated action — traffic behavior is controlled by the policy. The URL Filtering security profile provides granular control for traffic allowed by a security policy. As with other profiles, the URL filtering profile is only applied if the associated policy allows traffic. The profile can match URL categories, as well as individual URLs. Each category can be assigned a different action for more focused management. For example, a security policy could be created to allow all web browsing but have a policy which blocks all access to file sharing websites and logs all access to social networks.  File Blocking  File Blocking profiles control the flow of a wide range of file types by looking deep within the payload to identify the file type (as opposed to looking only at the file extension) to determine if the transfer of the file is allowed by policy. File blocking by type can be implemented on a per application basis. For example, an organization can use file blocking to enable the use of specific webmail application like Gmail and allow attachments but block the transfer of specific file types. The available actions for File Blocking profiles are:   * Block - Traffic is blocked, a Block log entry is generated, and a Response page is sent to the users browser if the traffic is web-based * Alert - Allow the user to access the file but add an alert to the URL log * Continue - Send a response page requiring the user to click Continue to proceed, log the action * Forward - Send the file to the WildFire cloud for analysis, log the action * Continue and Forward - Send a response page requiring the user to click (to confirm if there is a log created) * **Continue** to proceed and log the action. If the user continues, forward the file to the WildFire cloud and log the action. |