|  |  |
| --- | --- |
| Inject Report #3 – Firewall Policy | Team 11 |

Member Assigned:

|  |  |
| --- | --- |
| Request: | Develop a firewall policy for the Palo Alto device. Requirements:   1. Permit required services to be scored, 2) Restrict outbound traffic 3) Restrict transiting traffic between segments 4) Deny all other traffic 5) Enable threat protection on permitted traffic. |
| Steps Taken: | The default security policy rule is deleted. New rules are added with information such as the rule name, source zone/IP, destination IP, an application to block, and the action(s) to take when a threat is detected, and where to log them. |
| Screenshots (if applicable): |  |
| Report Details (e.g., address questions that were asked in inject) | **These steps are a great way to test safety and effectiveness of the policies:**  Security profiles can also be attached to rules, which scans allowed traffic for threats. This is done in the Actions>Profiles>Profile Type tab.  Palo Alto allows for testing of the rules, by running a security policy match test.  Select Device > Troubleshooting and select Security Policy Match from the Select Test drop-down.  Enter the Source and Destination IP addresses.  Enter the Protocol.  Execute the security policy match test.  Specific rule example/info goes here |
| Any remaining vulnerabilities/issues | None. |
| Additional Info: | Nothing to report. |