Version 5.2.0 introduced the following:
Release Month-Year:

1. It is now possible to add fully qualified domain names to the DHCPatriot IPv4 firewall
2. Force lower case usernames now works from the admin form. Previously it only worked from the customer facing authentication page.
3. ISC DHCP version 4.2.4-P1 is now the core dhcp server. This release contains bug fixes as well as some refinements.
4. Sticky IP notes are now possible. Notes can be included with a sticky IP assignment so that it can be remembered why it was done.
5. Exclude IP notes are now possible. Notes can be included with an excluded IP so that it can be remembered why it was done.
6. DHCPatriotHealth now alerts if the processing of leases is behind by a measureable amount (100KB).
7. New Lease Length options have been added (2 minutes / 1 minutes / 30 seconds). Please note that these should ONLY be used on unauthenticated subnets, and ONLY if you are sure that it will be OK with all devices on the network. The default lease length for unauthenticated and authenticated subnets remains at 3 minutes and 8 hours respectively.
8. Captive portal login and thank you pages can now be totally replaced with your own content.
9. Repaired a problem where static IP was not being entered during web page authentication if it was not in a special static network (this is no longer required but was still being required by login page).
10. Turned down verbosity of EDAC so that it wouldn't continuously print log messages about ECC operations on so equipped DHCPatriot machines. It will still print errors.
11. A new report called Possible Hijacked IP is available under Auth DHCP Reports and Standard DHCP Reports. This report shows IP addresses that have been declined by a DHCP client in the last thirty days. It is useful for finding those DHCP Pool Addresses that have been manually configured on some equipment.
12. A bug was reported regarding suspend old devices. The update code was found to not be working properly and so devices that shouldnt have been suspended would get suspended. We have repaired the update code.
13. DHCPatriot software now supports running as a KVM virtual machine. This will allow us to release the DHCPatriot system for running inside a Red Hat virtual, for example, at some future date.
14. ACPI power events are now supported. This really has no relevance on the hardware based DHCPatriot system. This does, however, allow a virtual to be shut down.
15. It is now possible to search sessions for longer than 24 hours as long as you provide the username, MAC address, or IP address. If none of these is provided it will restrict to 24 hours of sessions.

16. Option 82 information is now recorded with the sessions. Search Sessions now has an 82 shown with each entry. Clicking this link results in a popup window that displays option 82 information for the session, if available.
17. New version of cron has been installed. The previous version had an issue that could cause cron jobs to no longer run. This would in turn cause logs to reach the maximum file size as they were not rotated.
18. New Linux kernel installed.
19. Option 82 information is now sent in the RADIUS accounting start packets in the Called-Station-Id attribute, if available.
20. It is now possible to set NTP servers for the DHCPatriot to use to retrieve time. If none are set, the DHCPatriot will continue to use the FNGi NTP servers.
21. It is now possible to set NTP servers for the DHCPatriot to give to customers via DHCP. If none are set the DHCPatriot will continue to give out its own IP addresses as the NTP servers to customers.
22. Upped the limit of the number of IPs that could be tracked making inbound connections to port 80 for rate limiting purposes from 100 to 10240. Some systems had more than 100 devices making large amounts of connections to the system at a rapid pace.
23. It is now possible to set DNS servers for the DHCPatriot to give to customers via DHCP per network. If none are set the DHCPatriot will continue to give out the default DNS servers to customers.
24. Database backup has been altered to facilitate more reliable backup and make it easier to restore in event of catastrophic failure.
25. It is now possible to specify per-network RADIUS servers. A default server must be specified, and then per-network RADIUS servers may be specified. This may make things more complicated. Especially if there are overlapping usernames. If there are overlapping usernames, then suspensions will need to be done by MAC address instead of username.
26. The DHCPatriot can now receive per-user Simultaneous Use Restrictions from RADIUS in the attribute number 62 (Port-Limit). Even if the global SimUseEnable setting is turned off on the DHCPatriot, setting Port-Limit as a RADIUS reply attribute will cause the DHCPatriot to limit the number of Simultaneous Sessions to the integer provided. The per-user setting overrides the global setting for that user.
27. Built-In Authentication now supports setting a Simultaneous Use Restriction for each user. This is in conjunction with the DHCPatriot now supporting a per-user Simultaneous Use Restriction as mentioned above.
28. It is now possible to mass change TFTP file assignments. This can be accessed under Standard DHCP Actions -> TFTP File Maintenance. Wildcard (asterisk (*)) may be used in the filename to match multiple similar files for consolidation purposes.
29. It is now possible to add/edit/suspend/delete customers in the built-in authentication using new API calls.