1. Repaired a problem where it was impossible to add multiple firewall rules simultaneously for a single IP or subnet in System Configuration -> Firewall. Previously, it would add one rule and stop. Now it will add all rules that are ticked.
2. Removed some older (FNGi) firewall rules that were no longer needed.
3. Repaired a problem where it was impossible to add multiple firewall rules simultaneously for a single IP or subnet in System Configuration -> Firewallv6. Previously, it would add one rule and stop. Now it will add all rules that are ticked.
4. Repaired a problem where adding certain IPs or Subnets under System Configuration -> Firewallv6 would cause a crash of the web administration interface making the adding of such rules impossible. It now allows the adding of such rules with no crash.
5. Repaired a problem where some clients would request absurdly low preferred-lifetime values (such as 30 seconds) when obtaining a DHCPv6 lease. The server would honor these requests as there was no value set for preferred-lifetime. This would cause the clients to renew at a rapid pace. We now explicitly set a preferred-lifetime length of 10% less than the lease length avoiding this client problem.
6. Changed prefix length offering mode such that it will offer prefix of any length now. Previously, if the client sent a hint for the size of prefix desired, it would offer only a smaller prefix if the exact size wasn't available. If there were no smaller prefix (ie: client asking for /60 and /48 size is configured) then it wouldn't offer any prefix to that client. Now it will offer the /48 if thats what it has configured. It will offer something regardless of what the client asks for.
7. SNMP: Added DHCPv6 leases per second value available at OID: .1.3.6.1.4.1.2021.50.140
8. Added DHCPv6 leases per second value and historical graph to System Configuration -> Server Status in the web admin GUI.
9. DHCPv6: Lease length settings will now apply even to sticky IP addresses. Previously, sticky IP assignments in DHCPv6 would receive a 12 hour lease by default. Now they will receive an assignment of whatever length that was configured in DHCPv6 (IPv6) -> Shared Network for the network that they are a part of.
10. DHCPv6: Search Sessions now has the mac formatted to match the rest of the interface with the popup manufacturer name and clickable for manufacturer detail.
11. DHCPv6: View Address Usage (in the popup showing users online in the clicked subnet) now has the mac formatted to match the rest of the interface with the popup manufacturer name and clickable for manufacturer detail.
12. DHCPv6: View Authenticated users under DHCPv6 now allows clicking the username to receive a popup of all current and past sessions just like in the DHCPv4 side.
13. DHCPv6: Search Sessions under DHCPv6 now allows clicking the username to receive a popup of all current and past sessions just like in the DHCPv4 side.
14. DHCPv6: The View Address Usage subnet popup under DHCPv6 now allows clicking the username to receive a popup of all current and past sessions just like in the DHCPv4 side.
15. DHCPv6: All of the lists in the DHCPv6 (IPv6) menu section that did not feature sorting by column are now sortable by column in the display.
16. DHCPv6: 'Auto Suspend Authorized Devices' (box 19 under System Configuration -> General Setup) now applies to DHCPv6 authenticated devices as well.
17. DHCPv6: 'Auto Suspend Old Devices' (Box 20 under System Configuration -> General Setup) now applies to DHCPv6 authenticated devices as well.
18. DHCPv6: 'Auto Suspend Never Used Devices' (Box 21 under System Configuration -> General Setup) now applies to DHCPv6 authenticated devices as well.
19. DHCPv6: 'Auto Delete Suspended Devices' (Box 22 under System Configuration -> General Setup) now applies to DHCPv6 authenticated devices as well.
20. The performance estimate in the upper right hand corner of the web based GUI now adjusts for DHCPv6 average lease lengths and usage. If you have DHCPv6 configured with lower lease lengths, you can expect a drop in these numbers.

21. It is now possible to remotely monitor the DHCPv6 process. The SNMP OID: .1.3.6.1.4.1.2021.52.9.4.1.2.5.68.72.67.80.54.1 will produce a string: "1558031527:1" which contains the datetime:status (where 1 is up and 999 is down). The datetime should be within the last 5 minutes or the service should be considered down. Please note that this only confirms the process is running. It does not test if DHCPv6 is actually possible.
22. System Configuration -> Server Status now shows the status of the DHCPv6 service on both DHCPatriot devices.
23. A problem was repaired in System Configuration -> Server Status where 'Extended DHCPatriot Health' items were actually only showing the status of patriot-2 twice across both the patriot-1 and patriot-2 columns.
24. The current version of the system software on each device is now shown in System Configuration -> Server Status.
25. The current uptime of each device is now shown in System Configuration -> Server Status.
26. SNMP (DHCPv6): It is now possible to retrieve a list of subnets used in the DHCPv6 networks (authenticated or not) with the OID: 1.3.6.1.4.1.2021.50.80.1 for dynamic subnets and 1.3.6.1.4.1.2021.53.80.2 for prefix delegations. For example:
    COMMAND: snmpwalk -v1 -On -c lnx-snmp patriot-1.alpha.network1.net .1.3.6.1.4.1.2021.53.80.2
    RETURN:
    .1.3.6.1.4.1.2021.53.80.2.1 = STRING: "2620:0:2e58::/46"
    .1.3.6.1.4.1.2021.53.80.2.2 = STRING: "2:2:2::/47"
    .1.3.6.1.4.1.2021.53.80.2.3 = STRING: "4:4:4::/47"

27. SNMP (DHCPv6): It is now possible to get number of addresses or prefix in use for configured subnets or prefix delegations with the OID: 1.3.6.1.4.1.2021.53.90.1 (addresses in use) or 1.3.6.1.4.1.2021.53.90.2 (prefix in use). For example:
    COMMAND: snmpwalk -v1 -On -c lnx-snmp patriot-1.alpha.network1.net .1.3.6.1.4.1.2021.53.90.2
    RETURN:
    .1.3.6.1.4.1.2021.53.90.2.1 = INTEGER: 1
    .1.3.6.1.4.1.2021.53.90.2.2 = INTEGER: 0
    .1.3.6.1.4.1.2021.53.90.2.3 = INTEGER: 0
    The .1 or .2 or .3 at the end of the OID correspond to the ones from the subnet or prefix list.
28. SNMP (DHCPv6): It is now possible to get number of prefix available for configured prefix delegations with the OID: 1.3.6.1.4.1.2021.53.100.2 (prefix available). For example:
    COMMAND: snmpwalk -v1 -On -c lnx-snmp patriot-1.alpha.network1.net .1.3.6.1.4.1.2021.53.100.2
    RETURN:
    .1.3.6.1.4.1.2021.53.100.2.1 = INTEGER: 4
    .1.3.6.1.4.1.2021.53.100.2.2 = INTEGER: 2
    .1.3.6.1.4.1.2021.53.100.2.3 = INTEGER: 2
    The .1 or .2 or .3 at the end of the OID correspond to the ones from the prefix list.
29. SNMP (DHCPv6): It is now possible to get a listing of networks for which you can get total dynamic usage stats with OID: 1.3.6.1.4.1.2021.53.110. For example:
    COMMAND: snmpwalk -v1 -On -c lnx-snmp patriot-1.alpha.network1.net .1.3.6.1.4.1.2021.53.110
    RETURN:
    .1.3.6.1.4.1.2021.53.110.1.1 = STRING: "FNGipv6Test[1]"
    .1.3.6.1.4.1.2021.53.110.1.2 = STRING: "TEST[15]"
    .1.3.6.1.4.1.2021.53.110.2.1 = STRING: "FNGipv6Test[1]"

.1.3.6.1.4.1.2021.53.110.2.2 = STRING: "TEST[15]"
Where .1.n or .2.n at the end is for dynamic subnets (.1.n) or dynamic prefix delegation (.2.n)

30. SNMP (DHCPv6): It is now possible to get total used dynamic subnet addresses or prefix delegations using OID: 1.3.6.1.4.1.2021.53.120.1 (subnet) or 1.3.6.1.4.1.2021.53.120.2 (prefix) For example:
    COMMAND: snmpwalk -v1 -On -c lnx-snmp patriot-1.alpha.network1.net .
    1.3.6.1.4.1.2021.53.120
    RETURN:
    .1.3.6.1.4.1.2021.53.120.1.1 = INTEGER: 2
    .1.3.6.1.4.1.2021.53.120.1.2 = INTEGER: 0
    .1.3.6.1.4.1.2021.53.120.2.1 = INTEGER: 1
    .1.3.6.1.4.1.2021.53.120.2.2 = INTEGER: 0
    the .1 or .2 at the end of the OID correspond to the network names from the listing of networks previously mentioned.
31. SNMP (DHCPv6): It is now possible to get number of total prefix available for configured prefix delegations with the OID: 1.3.6.1.4.1.2021.53.130.2 (prefix available). For example:
    COMMAND: snmpwalk -v1 -On -c lnx-snmp patriot-1.alpha.network1.net .
    1.3.6.1.4.1.2021.53.130
    RETURN:
    .1.3.6.1.4.1.2021.53.130.2.1 = INTEGER: 4
    .1.3.6.1.4.1.2021.53.130.2.2 = INTEGER: 4
    The .1 or .2 at the end of the OID correspond to the ones from the prefix list.
32. Clarified System Configuration -> Custom Web Certificate instructions with the following: NOTE: It could take up to one hour for web certificate changes to take effect. If you want it to take effect sooner, you may reboot the DHCPatriot devices to cause it to take effect immediately.
33. DHCPv6: View Address Usage now supports graphs with the graph links the same as the DHCPv4 version.
34. DHCPv6: View Address Usage has been re-written to use the stored graph values so the content could be up to five minutes old the same as the DHCPv4 version. This was done for performance reasons as generating the data on the fly can be quite intensive on available resources.
35. Repaired a problem where the latest version of Google Chrome would not load the page or perform the action after a confirmation dialogue box. Had to change the method of loading the next page after confirmation. The new method is confirmed working in the following browsers:

    MacOS
    • Firefox
    • Chrome
    • Safari

    Windows 10
    • Microsoft Edge (only works if a valid certificate is installed - popup windows will not work properly if no valid certificate)
    • Firefox
    • Chrome
    • Opera

36. Repaired a problem where the total amount of available IPs for a subnet were, at times, being computed incorrectly resulting in an oscillation of the graph line up and down.

37. Auth DHCP Reports -> Search Sessions has received an enhancement. It is now possible to hover over the IP address for a session and see what type, shared network and subnet the IP address is part of. Type refers to authenticated or standard.
38. Standard DHCP Reports -> Search Sessions has received an enhancement. It is now possible to hover over the IP address for a session and see what type, shared network and subnet the IP address is part of. Type refers to authenticated or standard.
39. Both Auth and Standard DHCP versions of 'Possible Hijacked IP' now show what type, shared network and subnet the IP address is part of on hover. Type refers to authenticated or standard.
40. Auth DHCP Reports -> View Authenticated Users now supports hovering over the IP address to show what type (auth/standard), shared network and subnet the IP address is part of. This for both the IP the user device currently has as well as the static IP that the device is assigned. It should be possible to quickly note that the IP and assigned IP are not in the same shared network with this addition.
41. DHCPv6 (IPv6) -> Search Sessions has received an enhancement. It is now possible to hover over the IP address for a session and see what type, shared network and subnet the IP address is part of.
42. DHCPv6 (IPv6) -> View Authenticated Users now supports hovering over the IP address to show what type , shared network and subnet the IP address is part of. This for both the IP the user device currently has as well as the static IP that the device is assigned. It should be possible to quickly note that the IP and assigned IP are not in the same shared network with this addition.
43. DHCPv6: Simultaneous use restrictions are now supported in authenticated DHCPv6. In System Configuration -> General Setup, set 19) Simultaneous Use (DHCPv6) to desired simuse. Port-Limit via RADIUS is also supported. This RADIUS attribute is already supported in DHCPv4 simultaneous use. There is no separate attribute for DHCPv6. So if that attribute is set, it will apply to DHCPv6 as well.
44. DHCPv6: It is now possible to limit the viewing of network utilization and searching of sessions to certain networks in DHCPv6. A new section for limiting administrators to specific DHCPv6 networks has appeared in System Configuration -> Administrators
45. Captive portal and Authentication changes. The assignment of RADIUS servers and specific captive portal configurations to specific networks has been moved to the shared network configuration for DHCPv4 (Auth DHCP Config -> Shared Network). Additionally, the DHCPv6 version of this (DHCPv6 (IPv6) -> Shared Network) has been added. Previously, in both the Captive Portal and Authentication setup screens, the shared network had to be chosen to assign a specific configuration to that shared network. Now, create one or more specific Captive Portal or authentication configurations in their respective setup screens (A DEFAULT configuration is still required), then assign these to the specific shared network (or networks) in their respective setup areas (DHCPv4 or DHCPv6). This will eliminate the need to have the same Captive Portal configuration (for example) 12 times to have a special configuration of Captive Portal assigned to 12 shared networks. Radius server group and Captive Portal Scope selection boxes have appeared under each shared network configuration screen (authenticated DHCPv4 and DHCPv6). Specific configurations that already exist at the time of install of 6.4.0 will be handled automatically. This automatic process will not whittle down the number of configurations but you could do that by hand after the install is completed.
46. Since the Captive Portal and Authentication configuration screens now apply to both Authenticated DHCPv4 and DHCPv6, these configuration screens have been moved to the System Configuration menu.
47. DHCPv6 now shows the shared network specific captive portal screen (or the DEFAULT screen) depending on what was chosen in DHCPv6 (IPv6) -> Shared Network.

48. BUG: On the captive portal page, if the authentication server failed to respond, no error message was shown. This has been corrected and an error of "Authentication server failed to respond" is now shown.
49. The new captive portal and RADIUS settings are now supported in Auth DHCP Actions -> Authorize Customer and DHCPv6 (IPv6) -> Authorize Device.
50. The new captive portal and RADIUS settings are now supported in Captive Portal authentication.
51. The backend operations (CLI etc...) now support the new RADIUS settings
52. Certain protections against cross site scripting attacks and the like have been beefed up on the DHCPatriot system. Further enhancements will come in a later version.
53. Repaired a problem where Class attribute was detected even when not present during RADIUS authentication. This had a side affect of slowing down RADIUS communication when there was a backlog due to the way it is handled.
54. NOTE: Microsoft Edge will not properly show popup windows (such as a list of sessions for a specific user from View Authenticated Users) unless a valid security certificate is installed. A valid security certificate may be installed via System Configuration -> Custom Web Certificate.