Release Notes for DrayTek Vigor 3220 (UK/Ireland)

Firmware Version	3.9.0 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	17th December 2018
Build Date	14th November 2018
Revision	77758
Applicable Models	Vigor 3220
Locale	UK Only

New Features

1. OpenVPN is now supported as a Remote Dial-in User VPN protocol.

   Important Note: The router's OpenVPN server is automatically enabled on the router upon upgrade to 3.9.0 firmware, which listens on TCP & UDP ports 1194 by default and will take precedence over port forwarding to a LAN server using these ports.
   This service and its listening ports can be configured from the [VPN and Remote Access] > [OpenVPN] menu, or disabled in [VPN and Remote Access] > [Remote Access Control]

2. The router's Switch Management can now manage the VigorSwitch G1080, P1092 & P2121
3. Let's Encrypt certificate support added
4. Hotspot Web Portal can now support IPv6 clients
5. Support for dial-out IPsec VPN with XAuth to Cisco EZ VPN Server

Improvements

1. Hotspot Web Portal Database stored on USB can now be encrypted by enabling "Database Encryption" in [Hotspot Web Portal] > [Users Information] > [Database Setup]
2. Added support for data compression of VigorAP management
3. Support user management on the client authentication by the RADIUS server
4. IPsec EAP option added to IKEv2 LAN to LAN VPN to use X.509 for authentication
5. Hotspot Web Portal logs for user connection & disconnection can now be sent via syslog
6. Support NAT mode for IKEv2 LAN to LAN dial-out connection and IKEv2 NAT mode with EAP MSCHAPv2 authentication
7. SNMPv1 and SNMPv2 can now be enabled / disabled separately from SNMPv3 operation in [System Maintenance] > [SNMP]
8. Added TR-069 parameters for enabling/disabling [Data Flow Monitor] function
9. SNMP monitoring clients can now read out the CPU load and memory usage percentages as part of the router and firmware details in the sysDescr.0 (OID 1.3.6.1.2.1.1.1) value
10. Added a note in [Diagnostics] > [DoS Flood Table] to inform the user to enable [DoS Defense] first to display DoS Flood information for SYN / UDP / ICMP flooding
11. Added support for Dynu DDNS as a dynamic DNS provider
12. The router's SSL VPN server port can now be set via the CLI command "mngt sslvpnport"
13. TR-069 login message no longer displays model information from the router

14. Specific LAN interface can be selected for use with TR-069 management in [System Maintenance] > [TR-069] with the "ACS Server On" setting
15. USB Thermometer was not detected in some configurations
16. Improved handling of non-standard characters in the "Service Name" field of [NAT] > [Port Redirection]
17. The router's web interface could become inaccessible after importing a Vigor 2925 config
18. Wrong IP address for the subnet mask "/15". Correct IP address should be "255.254.0.0"
19. High Availability (HA) did not work when IPv6 was disabled
20. The "Block DNS" option in an APP Enforcement profile could be automatically enabled upon upgrade to 3.8.9.x firmware, resulting in App Enforcement blocking DNS unintentionally
21. The number of available LAN subnets was incorrect in CLI
22. Unable to allocate static IP address to IKEv2 VPN client
23. Unable to apply multiple static routes to CPE device
24. CLI command "ip bandwidth del <IP>" did not work
25. The router did not reboot automatically upon receiving new parameter settings from VigorACS, for setting changes that require a restart
26. Web Syslog in [Diagnostics] > [Syslog Explorer] can now be used when "Syslog Server" is not enabled or configured in [System Maintenance] > [Syslog / Mail Alert]
27. VLAN 6 and 7 could not be configured if VLAN 0-5 were configured and saved first in [LAN] > [VLAN] configuration
28. When selecting Internet IP in Determine WAN IP, DrayDDNS did not update with correct IP, or an error message of "WAN IP not present" appeared
29. Authenticating Hotspot Web Portal clients via Google authentication did not work
30. Unable to block a static route by the firewall when a remote dial-in user is connected
31. Available interfaces for a static route set by CLI and GUI were different
32. Custom (cycle in days) setting for WAN Budget did not operate correctly in some scenarios
33. Improved interoperability with Xbox One and UPnP / DMZ host
34. Data quota set on [User Management] > [User Profile] would be reset to zero after re-login
35. Vigor router ignored Don't Fragment flag in IP header
36. Custom local admin user account could not log in from WAN when "Admin Login from Internet" option is disabled
37. Data Flow Monitor did not display VPN traffic in some scenarios
38. Wireless clients would be disconnected from a VigorAP (e.g., VigorAP910C) when adding a new MAC address to Access Control List on [Central Management] > [AP] > [WLAN Profile]
39. SNMP data could be different from the readings on the router's dashboard
40. Dashboard and Station List displayed incorrect IP address when more than one entry existed on Bind IP to MAC
41. Corrected wording in some TR-069 parameters
42. Unable to restore configuration settings for LAN to LAN VPN, Bind IP to MAC and Wireless LAN via HTTPS when IPv6 was disabled

Known Issues

1. Configuration settings in 3.9.0 firmware are not backwards compatible with 3.8.7.
   It is not possible to downgrade from 3.9.0 to 3.8.7 and retain settings. To downgrade, use the .rst file to clear settings.

Before upgrade to 3.9.0 we recommend taking a backup of the previous configuration. To downgrade to 3.8.7 onto a unit running 3.9.0, first .rst reflash 3.8.7 and then restore a previously saved .cfg from 3.8.7 or earlier.

2. See New Features entry #1 for notes on OpenVPNs impact on Port Redirections for TCP/UDP port 1194

Firmware File Types

The ZIP file contains the firmware with two different file extensions, .ALL and .RST. The firmware is identical but the RST file contains factory default settings. If you install the ALL file, your router will retain all existing settings. If you use the RST file, <u>all settings will be wiped from your router</u>.

Upgrade Instructions

It is recommended that you take a configuration backup prior to upgrading the firmware. This can be done from the router's system maintenance menu.

To upgrade firmware, select *'firmware upgrade'* from the router's system maintenance menu and select the correct file. Ensure that you select the ALL file <u>unless</u> you want to wipe out your router's settings back to factory default.

Manual Upgrade

 If you cannot access the router's menu, you can put the router into 'TFTP' mode by holding the RESET whilst turning the unit on and then use the Firmware Utility. That will enable TFTP mode. TFTP mode is indicated by all LEDs flashing. This mode will also be automatically enabled by the router if there is a firmware/settings abnormality. Upgrading from the web interface is easier and recommended – this manual mode is only needed if the web interface is inaccessible.

Firmware Version	3.8.9.2 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	16th August 2018
Build Date	16th July 2018
Revision	75274
Applicable Models	Vigor 3220
Locale	UK Only

New Features

(None)

Improvements

1. Firewall filter rules were not correctly applied to Routed LAN subnets
2. Web interface could not be accessed via HTTPS from in some network environments
3. NAT loopback could not operate with port forwards configured using ports 768 to 1023

Known Issues

1. Configuration settings in 3.8.9.2 firmware are not backwards compatible with 3.8.7.
   It is not possible to downgrade from 3.8.9.2 to 3.8.7 and retain settings. To downgrade, use the .rst file to clear settings.
   Before upgrade to 3.8.9.2 we recommend taking a backup of the previous configuration. To downgrade to 3.8.7 onto a unit running 3.8.9.2, first .rst reflash 3.8.7 and then restore a previously saved .cfg from 3.8.7 or earlier.

Firmware Version	3.8.9.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient Note: A previous firmware (3.8.8.2) was a **critical release**. This f/w includes all changes/improvements that were in 3.8.8.2.
Release Date	29th June 2018
Build Date	12th June 2018
Revision	74510
Applicable Models	Vigor 3220
Locale	UK Only

New Features

(None)

Improvements

1. Fixed the App Enforcement profile issue in 3.8.9 firmware
2. Fixed the Web UI Issue if Bandwidth Limit and Data Flow Monitor were enabled in 3.8.9 firmware

Known Issues

1. Configuration settings in 3.8.9.1 firmware are not backwards compatible with 3.8.7.
It is not possible to downgrade from 3.8.9.1 to 3.8.7 and retain settings. To downgrade, use the .rst file to clear settings.
Before upgrade to 3.8.9.1 we recommend taking a backup of the previous configuration. To downgrade to 3.8.7 onto a unit running 3.8.9.1, first .rst reflash 3.8.7 and then restore a previously saved .cfg from 3.8.7 or earlier.

Firmware Version	3.8.9
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	5th June 2018
Build Date	18th May 2018
Revision	73931
Applicable Models	Vigor 3220
Locale	UK Only

Important Note – Bandwidth Limit & Remote Management

If Bandwidth Limit is configured and enabled on the Vigor 3220, keep using 3.8.8.2 firmware and wait for the next firmware release. The 3.8.9 firmware cannot be managed through the Web UI if Bandwidth Limit is enabled on the router.
In the event that the router has been upgraded to 3.8.9 and Bandwidth Limit is enabled, either of these two methods can be used to regain access to the router's web interface:

1. Disable Bandwidth Limit function by telnet or ssh with command "ip bandwidth off"
2. Temporarily disconnect the WAN cables from the router's WAN ports, to access the router's Web UI from the LAN and disable Bandwidth Limit

New Features

1. Firewall Filter rules can now be linked to specified LAN and WAN interfaces by selecting a Direction then clicking Advanced and selecting the interfaces that the Filter rule will affect
2. ISO 3166 Country objects configured in [Objects Setting] > [Country Object] menu can be applied as Source / Destination IP ranges in Firewall Filter rules
3. Router's status LEDs & port LEDs can be turned off or put into "LED Sleep Mode" when inactive, configured in [System Maintenance] > [Panel Control]
4. Dashboard layout can be configured from [System Maintenance] > [Dashboard Control]
5. Added Users Information section to Hotspot Web Portal (requires USB storage to operate) to store details of users that have connected through the Hotspot Web Portal
6. Support for mOTP and 2FA (two factor authentication) via e-mail/SMS added for remote management in [System Maintenance] > [Administrator Password]
7. Support DrayOS IKEv1 IPsec XAuth as a VPN protocol for Remote Dial-In User VPN tunnels
8. Remote Monitoring & Management (RMM) mechanism added for use with VigorACS
9. Support for EAP Tunneled Transport Layer Security (EAP_TTLS) security method added to [Applications] > [Local 802.1X General Setup].
10. Configuration backup / restore is now available for Remote Dial-In User and LAN-to-LAN profiles to back up all VPN profiles configured, separately from the main router configuration file
11. Larger certificate files now supported in [Certificate Management] > [Local Certificate] making it possible to include additional certificates required to complete a certificate chain
12. Factory Default configuration of DMZ Subnet's IP address is now 192.168.254.1/24. This does not affect existing DMZ Subnet configuration on upgrade
13. LAN IP Alias added to [LAN] > [General Setup] to define which WAN is used for outbound traffic by sending to a different Gateway address for the router

14. The Strict Bind setting in [LAN] > [Bind IP to MAC] can now be applied only to selected LAN subnets / VLANs instead of all LAN interfaces when enabled

Improvements

1. Support for VigorACS 2 version 2.3.0
2. Layout of [WAN] > [Internet Access] > [Details Page] improved to group essential settings in the left pane, with additional / advanced options grouped in the right pane
3. IKEv2 LAN to LAN VPN tunnels can specify these new Proposal options:
   a. Diffie-Hellman (DH) Group 19 (256-bit Elliptic Curve)
   b. Diffie-Hellman (DH) Group 20 (384-bit Elliptic Curve)
   c. Diffie-Hellman (DH) Group 21 (512-bit Elliptic Curve)
4. Central AP Management profiles now have options to configure AP-assisted Client Roaming parameters
5. Support Channel Width selection on [Central Management] > [AP] > [WLAN Profile]
6. When upgrading firmware, selecting a firmware file and clicking the "Preview" button will display details of the firmware selected
7. Improvements to WAN Budget scheduling
8. Layout of [VPN and Remote Access] > [Connection Management] improved
9. Support WAN DHCP option 121 for adding new static route
10. The CLI command "port status" could not display the Flow Control status of WAN1 correctly
11. Resolved Dynamic DNS status log display issue when viewing the log via the View Log button in [Applications] > [Dynamic DNS]
12. Some router icons were not displayed when viewing connected routers in the [Central Management] > [VPN] > [CPE Management] > [Managed Devices List]
13. Schedule entries configured to operate overnight did not work correctly
14. The firewall default rule when set to Block, would block DNS responses from the router if a LAN client used the router as its DNS server
15. NAT Port Redirection entries configured through the CLI did not take effect unless disabled and re-enabled
16. NAT Port Redirection entries configured with TCP protocol could not be enabled
17. Improved interoperability with UBDDNS Dynamic DNS provider
18. The router could sent incorrect DNS queries if Syslog / Mail Alert was enabled
19. Certificate import can now be performed via CLI using "mngt cert_import" command via URL
20. Enabling Session Limit could block Internet connectivity for Remote Dial-In User VPN tunnel connections from VPN clients sending Internet traffic through the VPN tunnel

Known Issues

1. The router cannot be managed from the Web UI if Bandwidth Limit is enabled on the router. This will be corrected in the next firmware release.

2. Configuration settings in 3.8.9 firmware are not backwards compatible with 3.8.7.
   It is not possible to downgrade from 3.8.9 to 3.8.7 and retain settings. To downgrade, use the .rst file to clear settings. Before upgrade to 3.8.9 we recommend taking a backup of the previous configuration. To downgrade to 3.8.7 onto a unit running 3.8.9, first .rst reflash 3.8.7 and then restore a previously saved .cfg from 3.8.7 or earlier.

Firmware Version	3.8.8.2
Release Type	**Critical** – Upgrade recommended immediately
Release Date	18th May 2018
Build Date	18th May 2018
Revision	73944
Applicable Models	Vigor 3220
Locale	UK Only

New Features

None

Improvements

1. This firmware includes improvements to harden the web interface against attacks. We have become aware of specific attacks against router, including DrayTek models where hackers have altered specific settings relating to your DNS servers and DHCP settings. You should urgently check those settings on your router. If they appear to have been tampered with, correct them and change your admin password and for any other config anomalies. Restore a config backup if you have one (from prior to the attack). We continue to investigate this issue but the first priority was to issue updated firmware.

Known Issues

1. Configuration settings in 3.8.8.2 firmware are not backwards compatible with 3.8.7.
   It is not possible to downgrade from 3.8.8.2 to 3.8.7 and retain settings. To downgrade, use the .rst file to clear settings.
   Before upgrade to 3.8.8.2 we recommend taking a backup of the previous configuration. To downgrade to 3.8.7 onto a unit running 3.8.8.2, first .rst reflash 3.8.7 and then restore a previously saved .cfg from 3.8.7 or earlier.

Firmware Version	3.8.8.1
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	5th April 2018
Build Date	15th March 2018
Revision	72567
Applicable Models	Vigor 3220
Locale	UK Only

New Features

1. LAN to LAN VPN profiles increased to 200
2. Remote Dial-In User VPN profiles increased to 200

Improvements

1. Improved interoperability with ISPs using PPP for IPv6 connectivity
2. Improved password entry validation in the [Quick Start Wizard]
3. Syslog data could not be sent when the Syslog Port in [System Maintenance] > [Syslog / Mail Alert] was configured to a value other than "514"
4. Bandwidth limit could not limit data traffic if the "IP Routed Subnet" option was enabled

Known Issues

2. Configuration settings in 3.8.8.1 firmware are not backwards compatible with 3.8.7.
   It is not possible to downgrade from 3.8.8.1 to 3.8.7 and retain settings. To downgrade, use the .rst file to clear settings.
   Before upgrade to 3.8.8.1 we recommend taking a backup of the previous configuration. To downgrade to 3.8.7 onto a unit running 3.8.8.1, first .rst reflash 3.8.7 and then restore a previously saved .cfg from 3.8.7 or earlier.

Firmware Version	3.8.7
Release Type	**Regular** – Upgrade recommended when convenient
Release Date	4th January 2018
Build Date	30th November 2017
Revision	69828
Applicable Models	Vigor 3220
Locale	UK Only

New Features

1. Support for BGP (Border Gateway Protocol)
2. Supported LAN subnet size increased to 1023 IP addresses per subnet (/22)
3. [Hotspot Web Portal] replaces [LAN] > [Web Portal Setup]
4. Support for IPsec IKEv2 for LAN to LAN tunnels and Remote Dial-in User VPN clients that support Pre-Shared-Key authentication
5. IPsec VPN now supports SHA2_256 (SHA256) authentication algorithm
6. Forward packets from WAN to VPN tunnel (single-arm VPN)
7. WAN Connection Detection - Ping Detect now supports Primary/Secondary Ping IP, Interval & Retry parameters
8. Added [NAT] > [ALG] menu to configure the router's SIP & RTSP ALG (Application Layer Gateway) functionality
9. Added Bandwidth Utilisation Notification Settings to [System Maintenance] > [TR-069] to give more detailed bandwidth usage information to VigorACS
10. DrayDDNS (DrayTek Dynamic DNS) support added in [Applications] > [Dynamic DNS]
11. Added [Firewall] > [Diagnostics] to test filter rules

Improvements

1. Default Protocol for NAT Port Redirection entries is now "TCP/UDP"
2. Switch Management now supports management of the VigorSwitch P1280
3. Auto backup router configuration to USB Storage either periodically or upon setting change
4. Resolved an issue with QoS operation when Bandwidth Limit is also enabled
5. Schedule entries can now operate on a set date each month, or daily cycle (max 30 days)
6. Automatic monthly reset of User Profile time/data quotas (with monthly schedule entry)
7. Maximum MTU for LAN ports increased to 1500 bytes
8. Improved compatibility of configuration file restoration from other Vigor routers

Known Issues

(None)

Firmware Version	3.8.4.1
Release Type	**Regular** – Upgrade recommended when convenient Note: A previous firmware (3.8.4) was a **critical release**. This f/w includes all changes/improvements that were in 3.8.4.
Release Date	26th September 2017
Build Date	28th August 2017
Revision	68158
Applicable Models	Vigor 3220
Locale	UK Only

New Features

1. Support for extra TR-069 parameters

Improvements

1. Improved IPsec LAN to LAN VPN throughput
2. Certificates generated by the router can now be signed with the SHA-256 algorithm
3. Policy Route can now direct traffic through virtual WAN (Multi-PVC) interfaces
4. Inter-LAN Routing table in [LAN] > [General Setup] now allows routing between LAN1 and DMZ Port when VLANs are not enabled
5. Web Content Filter incorrectly classified "petlog.org.uk" as an Uncategorised website
6. Interoperability improvements to the router's SSH server
7. Improved FTP server to prevent FTP bounce scanning
8. SNMP access was unable to filter by Manager Host IP
9. Improved algorithm used for encrypting configuration file in [System Maintenance] > [Configuration Backup] when saving router configuration with a password
10. Improved handling of sending Syslog log information to a hostname
11. Improved resilience of the router's Switch Management functionality
12. Disabling the Firewall could stop Hardware Acceleration being applied to sessions
13. The Start Date of the Root CA certificate created in [Certificate Management] > [Trusted CA Certificate] would be 1 day after the time of creation
14. Resolved an issue with PPTP VPN Passthrough for NAT to some types of internal PPTP VPN server
15. NAT Loopback did not work correctly with routed LAN subnets
16. Enabling Session Limit could cause a WAN interface to remain offline
17. WAN IP Alias addresses did not work correctly with ports opened in [NAT] > [Open Ports]
18. Corrected an issue with Bandwidth Limit when applied with IP Object addresses

19. Layout and wording improved in the following sections:
    a. [Applications] > [IGMP]
    b. [Firewall] > [General Setup]
    c. [LAN] > [VLAN]
20. Interface selection box was not displayed in web interface for "Force router to use "DNS server IP address" settings specified in" setting
21. USB port 2 used for 3G/4G WAN is more clearly identified in [WAN] > [Internet Access]

Known Issues

1. Access List does not currently apply to the router's TR-069 Management service, which uses TCP 8069 by default

Firmware Version	3.8.4
Release Type	**Critical** – Upgrade recommended immediately
Release Date	4th January 2017
Build Date	16th December 2016
Revision	61275
Applicable Models	Vigor 3220
Locale	UK Only

New Features

1. Added [Central Switch Management] > [Switch Management] to manage compatible VigorSwitches
2. [WAN] > [Internet Access] > [IPv6] PPP WAN now supports IPv6 RIPng (RIP for IPv6)
3. Support for DNSSEC added in [Application] > [DNS Security]
4. Firewall configuration can be backed up / restored from [Firewall] > [General Setup]
5. Firewall Wizard Mode added to [Firewall] > [Filter Setup] > [Edit Filter Set]
6. Firewall Diagnostics to test filter rules added in [Firewall] > [Diagnose]
7. Ping Detect latency Graph is available in [Diagnostics] > [Traffic Graph] for WAN interfaces using Ping for WAN Connection Detection
8. [Objects Setting] > [IP Objects] can now be uploaded to the router in CSV format
9. IP Objects can now be automatically created from the router's current ARP table
10. IP Objects can now be automatically created from the router's Routing Table
11. [NAT] > [Port Redirection] and [Open Ports] can specify an allowed Source IP Object (Single IP, Subnet or Range IP) to allow only specified IPs to access port forwards without making Firewall Filter Rules
12. VoIP QoS Statistics / Log added to [Bandwidth Management] > [Quality of Service]
13. Support for USB Thermometer
14. [Online Status] displays DSL details of a Vigor 130 modem connected to a WAN interface

Improvements

1. Security improvements including one or more considered critical.
2. DNS servers could not be configured for DHCP on subnets other than LAN1
3. AP Management can now be disabled from [System Maintenance] > [Management]
4. Added options in [System Maintenance] > [Management] to disable HTTPS management via TLS 1.0, TLS 1.1 or TLS 1.2
5. High Availability can now operate over IPv6 in addition to IPv4
6. Bandwidth Limit and Session Limit now support IPv6
7. LAN IP Alias feature added to control WAN interface used for outbound traffic by specifying a different Gateway IP on client devices
8. Configuration backup filename format improved i.e.
   v3220_<date (yyyymmdd)>_<router name>_<firmware version>.cfg

Known Issues

(None)

Firmware Version	3.8.2.2 (First Release)
Release Date	18th May 2016
Applicable Models	Vigor 3220
Locale	UK/Ireland ONLY

First Release of Firmware for this model

[END OF FILE]