Release Notes for DrayTek Vigor 3900 (UK/Ireland)

Firmware Version	1.5.1.6 (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	23rd February 2024
Release Date	27th August 2024
Revision	8218
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

Important Notice – READ BEFORE UPGRADING FIRMWARE

The "%" character is no longer supported in the admin password. If the character "%" is currently in use as the router's admin password, you must change the password before upgrading to the new firmware version.

If the character "%" is used as the admin password and you've upgraded to the new firmware version without changing the password, please use the following CLI commands via Telnet/SSH to change the admin password.

> enable
> configure system
> admin_passwd

New Features

(none)

Improvements

1. Improvements to the Web GUI Security

Known Issue

1. **Change to accepted Admin Password Characters** – The % character is no longer supported in the router's admin password, you must change the password to remove "%" characters before upgrading to the new firmware
2. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
3. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
4. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Important Note - Upgrading Firmware

Do not upgrade directly from 1.0.5 (and earlier) to 1.5.1.6.

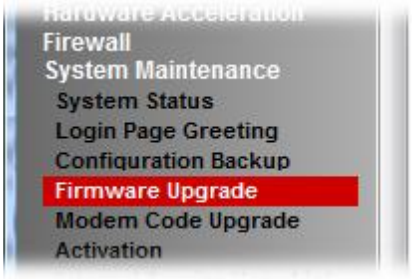
Due to differences in the Web UI and functionality the router MUST first be upgraded to at least 1.0.7.1 prior to upgrading to 1.5.1.6.

Upgrade your router to Version 1.0.7.1 or later first, and afterwards upgrade the router to Version 1.5.1.6.

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.



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	1.5.1.5 (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	6th October 2023
Release Date	27th October 2023
Revision	8217
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

Important Notice – READ BEFORE UPGRADING FIRMWARE

The "%" character is no longer supported in the admin password. If the character "%" is currently in use as the router's admin password, you must change the password before upgrading to the new firmware version.

If the character "%" is used as the admin password and you've upgraded to the new firmware version without changing the password, please use the following CLI commands via Telnet/SSH to change the admin password.

> enable
> configure system
> admin_passwd

New Features

(none)

Improvements

1. Improvements to the Web GUI Security to prevent possibility of occurrence of File System verify check fail after log-in to Web UI. If observed on older firmware then recommended action is to allow router to perform recovery system and then upgrade firmware.

Known Issue

1. **Change to accepted Admin Password Characters** – The % character is no longer supported in the router's admin password, you must change the password to remove "%" characters before upgrading to the new firmware
2. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
3. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
4. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.5.1.4 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	14th April 2022
Release Date	30th May 2022
Revision	8214
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

Important Notice – READ BEFORE UPGRADING FIRMWARE

The "%" character is no longer supported in the admin password. If the character "%" is currently in use as the router's admin password, you must change the password before upgrading to the new firmware version.

If the character "%" is used as the admin password and you've upgraded to the new firmware version without changing the password, please use the following CLI commands via Telnet/SSH to change the admin password.

> enable
> configure system
> admin_passwd

New Features

(none)

Improvements

1. Improved Web GUI Security
2. Updated HTTPS mechanism to address the CVE-2022-0778 (OpenSSL)
3. Factory default setting now disables TR-069 access from the WAN, configured from [System Maintenance] > [Access Control]
4. Set the OpenVPN encryption version to TLS 1.2 by default
5. Let's Encrypt certificate renewal could fail when Access Control was enabled
6. IKEv2 EAP Remote-Dial-In-User VPN could not be connected or could cause the SmartVPN Client to crash if the Subject Alt Name in the router's local certificate was copy/pasted with a ":" character in the value

Known Issue

1. **Change to accepted Admin Password Characters** – The % character is no longer supported in the router's admin password, you must change the password to remove "%" characters before upgrading to the new firmware
2. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
3. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only

4. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes:
   http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.5.1.3 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	18th March 2021
Release Date	22nd April 2021
Revision	8203
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

(none)

Improvements

1. Improved Web GUI security
2. Xauth dial-in username is now recorded to Syslog upon connection/use
3. Updated DNSMASQ for CERT/CC and CISA Reports (VU#434904 / ICSA-21-019-01)
4. Resolved an issue that incorrectly caused the router to send Syslog messages to report "passwd: Password for *x* changed by root", with some specific configuration settings
5. A display error issue after performing the Auto Firmware Upgrade
6. Disabled SNMP was re-enabled after router's system reboot
7. Router did not respond to Let's Encrypt certificate
8. The 2FA authentication via mail through WAN did not work if WAN port was configured as Static
9. Importing remote certificate for VPN did not work properly
10. Resolved downloading Let's Encrypt certificate issue
11. IKEv2 EAP did not working when Let's Encrypt certificate was renewed
12. IPsec VPN could not be established for dial-out IKEv2_EAP tunnels with Xauth
13. IPsec VPN could not reconnect after VPN Peer's WAN IP was changed
14. Improved compatibility with IKEv2 EAP clients connecting with passwords longer than 32 characters

Known Issue

1. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.5.1.2 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	28th August 2020
Release Date	28th September 2020
Revision	8183
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

(none)

Improvements

1. The Router's self-signed certificate will change upon upgrade for compatibility with new browser certificate requirements.
   Starting from September 2020, many client OS & browsers will limit publicly trusted TLS server certificate lifetime to 398 days or less, and connections will be rejected if certificates exceed this. This firmware patch will automatically re-sign all self-signed certificate lifetimes to 395 days (was 2 years or longer in older versions)
2. Improved IPsec VPN stability with multiple WAN interfaces
3. LAN DNS did not work for LAN to LAN VPN
4. Firewall country object mechanism improvements

Known Issue

1. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes:
   http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.5.1.1 (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	5th June 2020
Release Date	26th June 2020
Revision	8172
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

(none)

Improvements

1. Improved WebGUI security
2. Disabled local/remote port forwarding via SSH
3. DNS could not be resolved over VPN for Remote Dial-In VPN users with a local DNS server
4. Improved IPsec VPN stability
5. Resolved a problem with User Profiles, caused by special character " ' " in the Name
6. Fixed an issue that could cause the web interface to stop responding in some conditions
7. Improved NTP time checking behaviour after the router is rebooted
8. In some scenarios, Network Address Translation wasn't applied to all outgoing TCP packets
9. Bind IP to MAC table did not sort correctly when set to sort alphabetically
10. Reduced time to load initial Dashboard display when logging in to the router's web interface
11. Let's Encrypt certificate was not applied to Web UI with management from internet disabled
12. IPsec Xauth username was not displayed correctly in VPN Connection Management
13. Some Firewall Filter Rule settings could not be applied to OpenVPN connections
14. IPsec Aggressive mode Pre-Shared Key could not be saved if Peer ID was empty
15. Dial-In IKEv2 MultiSA VPN connection could not be established with the router behind NAT
16. L2TP over IPsec VPNs could not be terminated correctly from VPN Connection Management
17. In some rare conditions, the router could stop passing LAN-to-LAN IPsec VPN traffic

Known Issue

1. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.5.1 (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	6th February 2020
Release Date	7th February 2020
Revision	8136
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

1. Two-Factor Authentication is now supported for additional web interface security
2. IKEv2 EAP Dial-Out LAN to LAN tunnel (e.g. NordVPN Server)
3. Support certificate choices for OpenVPN
4. Support ACMEv2 for Let's Encrypt certificate

Improvements

1. Improved WebGUI security
2. Changing LDAP server port did not work properly
3. Both the SNMPv1 and SNMPv2 can be enabled/disabled
4. Default cipher for OpenVPN is now AES-256-CBC
5. WAN Inbound Load Balance can no longer be enabled without active profiles configured
6. Added support for static IP address assignment to IKEv2 EAP VPN clients
7. APPE signature updated
8. SSH Server version updated
9. IP database for country objects updated
10. Let's Encrypt certificate improvements:
    a) Reduced the retry interval
    b) Fixed certificate generation when IP ACL was enabled
    c) Fixed IKEv2 EAP certificate issue with Windows 10
11. Improved SSL VPN compatibility with Apple devices.
    Self-Signed certificate's Valid To date is now 2 years from date of generation. Regenerate the router's Self-Signed Certificate to meet the new trusted certificate requirements of Apple iOS 13 & macOS 10.15. Longer Valid To periods can be specified by generating a Local Certificate and self-signing it with the router's internal Root CA.
12. Route policy with normal priority and disabled failover had higher priority than VPN routing
13. In some cases, router would reply to packets for non-open ports on WAN by default
14. Second PPPoE WAN connection could not be established in some scenarios
15. Central AP management for VigorAP920RPD updated
16. Product registration to VigorACS server mechanism improved
17. WCF was only compatible with firewall default policy set to Accept rule
18. SSL VPN legend in PPP General Setup page updated

Firmware Version	1.4.4 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	8th July 2019
Release Date	29th July 2019
Revision	8057
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Switch Management supports VigorSwitch G1280
2. Support Radius authentication for OpenVPN
3. DDNS update would fail in some circumstances
4. Improved CPU usage when running PPPoE server for 100 clients
5. For the web portal, the PC would be directed to a null web page after clicking the OK button in the Bulletin Board
6. Port Redirection and VPN connection became non-functioning after running the router for a few days
7. Web portal's logout function did not work with the Chrome Browser
8. Vigor router did not offer IP for IKEv2 EAP user integrated with RADIUS and DHCP relay
9. OpenVPN VPN tunnel could not authenticate if the password contained "#" or "." characters
10. [Central Management] > [AP Management] did not list VigorAP903
11. Unified format of [AP Management] / [Switch Management] support list
12. Unable to import IP bind MAC file if login language wasn't English
13. Windows 10 IKEv2 EAP Client had to enter the password twice for creating the VPN connection to Vigor router

Known Issues

1. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.4.3 (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	8th March 2019
Release Date	13th March 2019
Revision	8012
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Additional Web Interface XSS protections
2. Updated MAC object OUI database
3. Support for DHCP option 121 in the router's WAN DHCP client
4. Support for Comma character ',' in advanced DHCP options
5. A problem with the Open VPN debug log could cause a problem with logging in to the router's web interface
6. VPN Syslog was shown in Others tab instead of VPN tab of Syslog Utility
7. VigorACS generated an offline alarm for the Vigor router when the router was configured to use HTTPS for the VigorACS server URL
8. Authentication via LDAP server failed when the username contained special characters i.e. '('

Known Issues

1. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.4.2.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	28th January 2019
Release Date	29th January 2019
Revision	7982
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. In some circumstances, after a period of uptime, the web interface, SSH and Telnet management interfaces could respond from the Internet when remote management for these interfaces was disabled
2. Tx/Rx bytes in [Diagnostics] > [Data Flow Monitor] can be reset by disabling & enabling Data Flow Monitor
3. It was not possible to log into the Web user interface in some specific circumstances
4. Country code setting could not be configured with Google Chrome browser
5. Web Content Filter license information could be displayed incorrectly after loading a configuration file from a different router
6. Device Name for VigorAP displayed incorrectly in [Central Management] > [AP Management] > [Dashboard]
7. LDAP Search Button did not work when the Regular DN setting contained space
8. Port Description could not be added on active uplink port in [Central Management] > [Switch Management] > [Profile]
9. IP configured in Keyword Accept rule was blocked when HTTPS Filter was enabled
10. Router reboot could occur with both URL/WCF and HTTPS Filter were enabled
11. Web Portal now supports Responsive web design for mobile phones
12. An incorrect message displayed in the Web Portal on Android Phones
13. FTP transfers could cause higher than normal CPU usage
14. SNMP OID IfDescr displayed many unknown PPP1500 interfaces
15. SNMP OID of WAN Interface changed each time the WAN interface disconnected and reconnected
16. Unable to block SNMP from WAN
17. ARP cache could not be cleared
18. Syslog was not sent to remote syslog server after changing WAN IP
19. Router sent multiple mail alerts notifying of WAN disconnection if the WAN did not receive DHCP response
20. No traffic passed between subnets configured on [LAN] > [General Setup] > [More Subnet] when HA was working and the master device was down
21. Improved Rogue DHCP server detection and alarm feature
22. WhatsApp could not be blocked when the “Allow non-HTTP Traffic” option was disabled

23. Unable to save WLAN profile on [Central Management] > [AP Management] > [WLAN profile] when SSID3 was disabled but SSID was enabled
24. WANs allowed for OpenVPN can be selected in [VPN and Remote Access] > [OpenVPN General Setup]
25. Improved stability of IPsec Multiple SA tunnels
26. Improved stability of IPsec VPNs linked to IP Routed LAN interfaces
27. SSL VPN (SSL dial-in profile) could not be established when using Let's Encrypt Certificate
28. A user profile with static IP address could not establish OpenVPN tunnel
29. OpenVPN tunnel could not be established for LAN interfaces with DHCP disabled and "Specify Remote Dial-in IP" set
30. LAN DNS addresses were not correctly specified for OpenVPN tunnel clients
31. Static IP could not be assigned for an OpenVPN tunnel if the address was out of LAN DHCP range
32. Improved interoperability with CheckPoint VPN router by resolving IKE phase1 rekey failure
33. IPsec VPN tunnel to Cisco peer could be established but would not pass data through the tunnel

Known Issues

1. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.4.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	5th September 2018
Release Date	2nd October 2018
Revision	7846
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

1. VigorSwitch P2280 & G2280 can now be managed by the router's Switch Management

Improvements

1. USB Thermometer was not detected in some configurations
2. Configuration Backup made through VigorACS could not be restored
3. SNMP service stopped working for a period of time and recovered again
4. Removed duplicate OpenVPN service enable setting in [OpenVPN General Setup]
5. Subnets other than /24 were not assigned correctly to OpenVPN clients
6. IPsec LAN to LAN tunnels could not be created through central VPN management
7. Added support for management of VigorAP 920R
8. Central AP Management was unable to manage VigorAPs
9. IPsec VPNs with multiple SA tunnels were unstable
10. After downgrading to v1.3.3.2, Vigor router would upgrade to v1.4.0 automatically
11. Improved IPsec VPN stability
12. LAN packets for DHCP relay could not be routed through the WAN correctly
13. Corrected the functionality of the WAN Bridge to VLAN feature
14. "File System Verify failed" message incorrectly displayed when logging into WUI
15. If disabling a "packet-triggered" VPN IPsec LAN to LAN profile, the profile could not reconnect the tunnel after the WAN interface dropped & reconnected
16. Improved IPsec VPN stability for profiles configured with a subnet mask of /32
17. IPsec dial-in user VPN failed to connect where the VPN client was behind NAT and IPsec profile configured with static remote host address
18. Improved stability of the Data Flow Monitor function

Firmware Version	1.4.0 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	21st May 2018
Release Date	26th June 2018
Revision	7716
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

1. OpenVPN support added as a VPN protocol for Remote Dial-In Users
2. DrayDDNS (DrayTek Dynamic DNS) support added in [Applications] > [Dynamic DNS]
3. Support for Let's Encrypt HTTPS certificates added in:
   [Certificate Management] > [Local Certificate] (click Let's Encrypt button to configure)
4. Support for Remote Dial-In user IKEv2 connections using Windows 7, 8, 10 VPN client
5. Inter-LAN Routing configuration now supports Route Groups to give detailed control of connectivity between VLANs

Improvements

1. Support for VigorACS Server version 2.3.0
2. Configuring a backup WAN interface in [Routing]>[Load Balance Pool] now allows the backup interface to operate as a backup for multiple WAN interfaces, instead of a single WAN
3. Setting the Load Balance Mode to Session-Based now allows selection of protocols to exclude from the Session-Based Load Balance mechanism i.e. HTTPS & IPsec
4. Added "Exclude LAN-to-WAN Traffic from DoS Defense" option to ignore outbound traffic from DoS defense in [Firewall]>[DoS Defense]>[System]
5. Support source NAT for incoming traffic in [NAT]>[Port Redirection] with the Change Source IP setting, which translates the external IP into the specified internal source IP
6. Improved handling efficiency of IPsec ISAKMP packets
7. Improvements to VPN handling to increase VPN upload & download throughput
8. IKEv2 IPsec VPN now supports FQDN as a Local / Remote ID type
9. Remote Dial-In User IKEv2 VPN now supports LDAP / RADIUS authentication
10. Improved IKEv2 VPN tunnel interoperability with Fortinet VPN endpoints
11. 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)
12. Improved display of VPN uptime in [VPN and Remote Access] > [Connection Management]
13. Added note to [VPN and Remote Access] > [PPP General Setup] with recommended VPN types for each client platform
14. Allowed IPsec Dial-In Security methods (DES, 3DES, AES) can now be specified for IPsec Remote Dial-In Users from [VPN and Remote Access] > [IPsec General Setup]
15. Changing LAN configuration settings (except for the router's LAN IP) no longer drops active Internet / VPN connections

16. Improved wording in [VPN and Remote Access] > [PPP General Setup] > L2TP tab
17. Updated OpenSSL for CVE-2018-0739
18. Reduced the time from router restart / power up to activate the router's LAN and WAN interfaces
19. Added an import/export button for keyword objects
20. Updated APP Enforcement signatures
21. Update the Cyren URL Category Check Link
22. Added "More log" (more detailed syslogs) option in [Firewall]>[Filter Setup]>[URL/WCF Category Filter] profiles
23. DrayTek WCF and URL filter log can be displayed on [System Maintenance]>[Syslog/Mail Alert]>[Syslog File]
24. Support default route and failover function for BGP
25. Added auto configuration backup option in [System Maintenance]>[Configuration Backup]
26. The warning message for changing access port number will be shown only when remote access is enabled
27. Add an option (for user/guest profile) to log out online device when login number over the limit
28. Support router's local services (NTP, DNS and so on) via WAN alias IP
29. Improved the interface to add WAN IP Alias entries in [WAN]>[General Setup]
30. Vigor router can intercept the DNS packets to reply or forward the DNS query according to LAN DNS setting
31. Add an option of "Enable / Disable SMBv1" in [USB Application]>[SAMBA Server]>[General Setup]
32. Improved the menu layout for AP Management
33. DoS options can no longer be modified when the DoS Defense Enable option is not ticked
34. Support destination IP selections for white list settings on [User Management]>[Web Portal]>[General Setup]
35. Use System Time instead of Browser Time to display Traffic Graph
36. CSM: Unable to open Yahoo WEB page after applying URL keyword "flickr" for web page blocking
37. GRE tunnel was not displayed in the connection management after the profile was renamed
38. Renaming the IPsec profile in [VPN and Remote Access]>[VPN Profile]>[IPsec] resulted in empty MultipleSA settings for that profile
39. IPsec VPN tunnels connecting in NAT mode to WAN Alias IP could not pass traffic correctly
40. Use Alias IP was incorrectly displayed on policy route web page when USB WAN interface was selected
41. SNMP Trap packets could not be sent through WAN Alias IP
42. IPsec VPN was up but no traffic passed through after some time (VPN routes disappeared)
43. When authenticating SSL VPN with MSCHAPv2, authentication could be delayed by 30s
44. Unable to add more than one VPN remote subnet via CLI command "more_remotesubnet"
45. Improved connectivity for LAN clients connecting to Remote Dial-In Users connected via VPN
46. Traffic was unable to pass through IPsec multi-SA tunnel
47. Vigor router did not validate End IP in IP Object range
48. Unable to register to VigorACS 2 successfully in some situations
49. AP management mechanism did not send the provision packet to VigorAP in some scenarios

50. Static route via LAN PPPoE client did not work (LAN client works)
51. Disabling a PPPoE user profile still allowed a user to make PPPoE connection with that profile
52. System time displayed on mobile web interface was 2hrs off from desktop web interface
53. LDAP Search function is no longer available in Simple mode
54. Improved resilience of the router's Mail service
55. When WAN Inbound Load Balance was on, Vigor router would do DNS query from WAN for other domains outside the configured IP
56. Vigor router could not generate correct amount of user access logs in some conditions i.e. 1000 connections established in 5 seconds
57. Could not use 'space' in defining name of certificate
58. Accessing Vigor router from WAN2 was allowed even only set the Internet Access Control to WAN1 on [System Maintenance]>[Access Control]
59. End user got 2 email alerts when WAN was down
60. Ping connection detection did not disconnect USB WAN
61. Display error for TTL on [Diagnostics]>[Session Table]>[NAT]
62. DDNS user-defined profile could not upload the IP to the server properly when using HTTPS
63. URL/Web filter couldn't block HTTPS website if HTTPS was accepted in an IP filter profile with “if no further match”
64. Firewall Syslog could not be disabled when the rule action was “Block If No Further Match ”
65. Syslog could send some unnecessary information for RADIUS authenticated connections
66. Additional TR-069 parameters added for these menus & settings:
    a) [VPN and Remote Access]
    b) Local ID/Remote ID of [VPN and Remote Access]>[VPN Profiles]>[Basic]
    c) [NAT]
    d) [Routing] and [LAN/WAN VLAN]
    e) [DNS Security]
    f) [GVRP]
    g) [IGMP Proxy]
    h) [High Availability]
    i) [Wake on LAN]
    j) [SMS/Mail alert service]
    k) Local / Remote address of [Bandwidth Management]
    l) [Profile Number Limit]

Known Issues

1. **Central VPN Management** – If Central VPN Management is configured and used to manage other DrayTek routers, keep using F/W 1.3.3.2 and wait for the next firmware release. Routers cannot be managed / monitored through Central VPN Management with F/W 1.4.0.
2. **Central AP Management** – If Central AP Management is configured and used to manage VigorAP access points, keep using F/W 1.3.3.2 and wait for the next firmware release. VigorAPs cannot be managed / monitored through Central AP Management with F/W 1.4.0.
3. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update

4. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
5. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.3.3.2 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	11th April 2018
Release Date	1st May 2018
Revision	7677
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. When using the Web Portal to control Internet access, Guest accounts could not log in to the Web Portal for Internet access

Known Issues

1. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Important Note - Upgrading Firmware

Do not upgrade directly from 1.0.5 (and earlier) to 1.3.3.2.
Due to differences in the Web UI and functionality the router MUST first be upgraded to at least 1.0.7.1 prior to upgrading to 1.3.3.2.
Upgrade your router to Version 1.0.7.1 or later first, and afterwards upgrade the router to Version 1.3.3.2.

Firmware Version	1.3.3.1 (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	28th March 2018
Release Date	3rd April 2018
Revision	7657
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Improvement related to firmware security
2. Resolved IPsec stability issue that was present in 1.3.3 firmware
3. Remote Dial-In user accounts created in 1.3.3 firmware could not establish a VPN tunnel after restarting the router

Known Issues

1. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.3.3 (Formal Release)
Release Type	**Critical** – Upgrade recommended immediately
Build Date	22nd March 2018
Release Date	22nd March 2018
Revision	7640
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

(None)

Improvements

1. Improvement related to firmware security

Known Issues

1. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. **IP Filter** - F/W 1.2.0 onwards changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.3.2 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	24th November 2017
Release Date	12th December 2017
Revision	7459
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

1. Fast NAT functionality added to improve outbound NAT throughput by bypassing firewall processing for specified local subnet(s) going through selected WAN interfaces. Configured in [NAT] > [Fast NAT]

Improvements

1. Updated DNSMasq to improve security, for more details please read this security advisory: https://www.draytek.co.uk/information/our-technology/dnsmasq-vulnerability
2. Configured and functioning URL/Web Category Profiles could display as a blank profile in the web interface
3. Syslog output would report the rate unit as Kbps when setting the Filtering Rate (Mbps) in [Firewall] > [DoS Defense] > [Switch Rate Limit] > [Storm Filter]
4. Access Barrier for HTTPS management could potentially block an authenticated HTTPS management session
5. Corrected a potential error which might result in flooding a WAN interface removed from the Load Balance Pool
6. The Counter value for URL/Web Category Filter rules could not increment when blocking HTTPS websites
7. LDAP with Bind Type set to “Regular Mode” – When clicking the Search button for Base DN, the router would attempt to bind with Root, which caused compatibility issues with Windows LDAP servers
8. HTTPS filtering behaviour was incorrect when filtering with a keyword of “.”
9. Improved reliability of filtering by File Extension with the Firewall
10. High Availability failover did not occur when all WANs failed on the primary router
11. Multiple subnets available through a VPN Trunk in Backup mode were unavailable when Primary Interface VPN tunnel dropped and the Backup Interface VPN tunnel became active
12. VPN tunnels were unable to route traffic if a PPPoE WAN was disconnected, remained offline for over 12 hours and was then reconnected
13. Dial Out IPsec VPN could not establish if VPN server hostname started with a number (0-9)
14. After upgrade from firmware 1.2.2, [VPN and Remote Access] > [Connection Management] could not display profile names for IPsec VPN tunnels, displaying a “Lack of Ptype” error
15. Web Portal could conflict with IP filter rules
16. Improved [Bandwidth Management] > [Bandwidth Limit] rate limiting algorithm
17. AP Management broadcast packets no longer send through VPN tunnels, this can be enabled in [AP Management] > [General Setup] by enabling “Pass-Through VPN”
18. Improved Web Portal login page load times
19. QoS profiles and Firewall Filter Rules can now specify up to 200 Service Type Objects

20. IPsec VPN stability improvements

Known Issues

1. **High Availability** - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. **L2TP Tunnel -** Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. **IP Filter** - F/W 1.2.0 onwards Changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.3.1 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	11th July 2017
Release Date	27th July 2017
Revision	7156
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

1. Fast Route functionality added to improve throughput by bypassing firewall processing for specified routed subnets (VPN tunnels etc.). Located in [Routing] > [Fast Route].

Improvements

1. Resolved an issue that could stop the router from resolving DNS hostnames, this would affect any services that resolve hostnames to IP addresses, such as Content Filtering, NTP, Mail Alert, DNS Server etc.
2. Improvements to Samba service to ensure immunity to CVE-2017-7494
3. Updated SSH server
4. Updated App Enforcement signatures to improve handling / blocking of:
    a. Hotspot
    b. UltraSurf
    c. PPstream
    d. Google Hangouts
5. [NAT] > [Server Load Balance] can now balance based on “Source IP”
6. Central AP Management can select all managed VigorAPs to apply WLAN Profiles / AP Maintenance tasks
7. Resolved an issue with [User Management] > [Web Portal] and SMS authentication
8. [User Management] > [User Profile] > Apply All tab could not alter PPTP settings
9. IPsec VPN tunnels could not re-establish VPN connection over specified “Failover to” WAN
10. Resolved an issue with IPv6 when using an IPv6 WAN configured for DHCPv6 PD (IAID)
11. iPad / iPhone devices with iOS 10.3.1 and later could not establish IKEv2 VPN tunnel
12. XAuth VPN tunnel could not authenticate if the password contained “#” or “.” characters
13. The router could not perform DDNS update for “Strato” Dynamic DNS
14. Improved PPPoE server efficiency
15. IPv6 Ping Diagnostics would not display the ping result
16. Resolved a display issue with Switch Management’s Switch Hierarchy view

Known Issues

1. High Availability - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process. Reconfigure High Availability after updating the firmware.
2. Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. F/W 1.2.0 onwards Changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.3.0 (Formal Release)
Release Type	**Regular** – Upgrade recommended when convenient
Build Date	26th April 2017
Release Date	17th May 2017
Revision	7020
Applicable Models	Vigor 3900
Locale	UK & Ireland Only

New Features

1. Support for GRE Tunnel under [VPN and Remote Access] > [VPN Profiles] > [GRE] for compatibility with Cisco routers
2. Support for IKEv2 IPsec VPN tunnels
3. XAuth authentication support for IPsec Remote Dial-In Teleworker VPN tunnels
4. Central AP Management support – manage up to 50 VigorAP access points
5. Central Switch Management support – manage up to 10 VigorSwitch switches
6. New interface with improved design for mobile devices available through: https://<router IP>/mobile
7. Support for DNSSEC added in [Applications] > [DNS Security]
8. [NAT] > [Server Load Balance] added

Improvements

1. The router will notify when another DHCP server is detected
2. DHCP options can now specify DHCP Gateway IP Address
3. Support dynamic prefix for IPv6 LAN
4. WAN Interfaces will default to DHCP when enabled
5. High Availability Hot Standby mode can now be switched manually
6. Firewall now has a Guest group in [Filter Setup] to apply rules to Guest Profile users
7. If Firewall – Default Policy is set to Block, option added to “Block All Incoming Traffic”
8. Bandwidth Limit now supports “Auto Adjust to make best use of available bandwidth” option
9. Bandwidth Limit & Session Limit can now be applied to User Objects, Groups & LDAP
10. Added VPN Disconnect Alert Delay to [Notification Object] > [Advanced Setting]
11. StartTLS Connection Security supported in [Mail Service Object] & Mail Alert
12. Added an option to disable User Login Mail Alert
13. Mail Alerts for WAN Status changes now include the WAN IP
14. HTTPS Management can now be enforced using Enforce HTTPS Management option, forwards HTTP access attempts to the HTTPS interface
15. SSH interface now supports SHA2 authentication
16. Timezone configured in Time and Date settings now defaults to UK
17. Traffic Graph now displays CPU and Coprocessor usage history graphs
18. Added Apply Settings to VigorAP section to TR-069 configuration
19. Support for scheduled reboot on weekdays only
20. Improvements to the Fail to Ban & Access Barrier functions
21. LAN DNS now supports wildcards
22. LAN DNS profiles can now perform conditional DNS forwarding when the Type of the LAN DNS profile is set to FORWARD
23. Dynamic DNS now supports HTTPS
24. Dynamic DNS now supports User Defined mode for custom API configuration

25. Google Domains added to Dynamic DNS
26. OpenDNS added to Dynamic DNS
27. Ping & Trace Route diagnostics can now select which WAN IP Alias to send through
28. Added View button to Certificate Management to view loaded certificate details
29. Search functionality added to:
    a. IP Objects & Groups
    b. Service Type Objects & Groups
    c. Keyword / DNS Objects
    d. User Profiles
    e. VPN Profiles
    f. NAT Port Redirection rules
30. Web Portal can now redirect to specified LAN DNS address instead of IP
31. [User Management] > [Web Portal] – Login History added
32. Clean Deadline button added to Guest Profile to renew usage time of selected account(s)
33. Guest Profile accounts can specify max simultaneous logins
34. Added Search Button in LDAP to allow users to view and select the Base DN/Group DN
35. LDAP now supports SSL connection to LDAP Server
36. Improvements to the RADIUS configuration page
37. [NAT] > [Port Redirection] can specify allowed Source IP Objects to allow only specified IPs to access port forwards without making Firewall Filter Rules
38. Policy Route rules can select Service Type Objects instead of manually specifying ports
39. Policy Route rules can now specify Time Objects to apply rules during specified times only
40. Added a priority graph to Policy Route rules, click "(?)" to view
41. Support for SPF/TXT DNS Records for WAN Inbound Load Balance
42. VPN Profiles can now be renamed
43. VPN Profiles now display Status icon to indicate connection state
44. SSL VPN port can be configured separately from HTTPS management interface
45. SSL VPN can be disabled on individual WAN interfaces in [Access Control] to allow NAT Port Redirections to be configured with that port, to the WAN interface with SSL VPN disabled
46. Allowed WAN interfaces for PPTP VPN server can be selected in [VPN and Remote Access] > [PPP General Setup]
47. IPsec VPN can be set as Default Route/Gateway with Apply NAT Policy enabled for that VPN
48. User Profiles can specify allowed VPN Dial-In times by selecting Time Objects
49. IPsec proposal DH Group now defaults to G5 (1536-bit)
50. Multiple SAs (Security Associations) added to IPsec VPN profiles to specify additional Local & Remote subnets
51. Central VPN Management is now able to configure SSL VPN tunnels

Known Issues

1. High Availability - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process. Reconfigure High Availability after the update
2. Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. F/W 1.2.0 onwards Changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: https://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.2.2 (Formal Release)
Release Date	22nd November 2016
Build Date	13th October 2016
Revision	r6591
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

(None)

Improvement

1. FTP connections in Active mode were not passed correctly through NAT
2. When using [Diagnostics] > [Data Flow Monitor] > Packet Monitor, results could not be filtered by Host
3. Resolved an issue that could cause higher than normal memory usage with some router configurations
4. When configuring a User Management profile for VPN with MOTP enabled, it could not be saved without entering a password
5. TTL values were reported incorrectly in the [Diagnostics] > [Session Table]
6. Improved connectivity for Mac OS X SmartVPN clients

Known Issues

1. High Availability - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. F/W 1.2.0 onwards Changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.2.1 (Formal Release)
Release Date	7th September 2016
Build Date	24th August 2016
Revision	r6454
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

1. The router's Online Status can display "Remote DSL" information from a Vigor 130 or Vigor 120v2 modem connected to the router's WAN ports
2. Support WAN Load Balance by Session, configured in [Routing] > [Default Route], the default is IP-based Load Balancing
3. Packet Monitor facility added to [Diagnostics] > [Data Flow Monitor] to capture WAN/LAN packets and download as a .pcap file
4. Web Content Filter Query Server can now be specified in [Objects Setting] > [Web Category Object] > [Query Server] tab

Improvement

1. NAT efficiency improvements
2. SSL VPN supports Idle Timeout and Reconnect
3. APP-Enforcement Signature updated to improve handling of:
    i. IM-Google Hangouts
    ii. Protocol-DNS
    iii. HTTP
    iv. SSL/TLS
    v. Tunnel-Ultrasurf
    vi. VoIP-RC
    vii. WebHD-HTTP_Upload
4. Web interface response time improved when displaying large numbers of Profiles (User Profile, IP Objects, etc)
5. Improved TCP SYN+FIN filtering mechanism
6. Auto DDoS defense added to reduce CPU load if DDoS occurs

Known Issues

1. High Availability - Updating from a firmware version <=1.1.0.2: Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after the update
2. Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. F/W 1.2.1 Changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for

more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

4. FTP connections do not work in "active" mode, "passive" mode works normally. This will be fixed in the next firmware release.

Firmware Version	1.2.0 (Formal Release)
Release Date	29th December 2015
Build Date	3rd December 2015
Revision	r5723
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

1. CPU, Memory, Traffic Tx/Rx usage added to [Notification Object], configured under Advanced Setting tab
2. [Configuration Backup] > [Analysis] displays details of router configuration on one page
3. Auto Firmware Upgrade and Auto Firmware Patch now available to simplify update process
4. [User Management] > [Web Portal] new features:
   a. Can use SMS as an authentication method (requires internet SMS provider configured)
   b. Option to block mobile devices if required
   c. Customise login & background images in Portal Page Setup
5. MAC/Vendor Object now supported for use with IP Filter
6. SMB Server now available under [USB Application] menu for file sharing of connected USB storage
7. Now supports SHA2_256 for IPsec VPN tunnel authentication
8. SSL VPN port can now be configured as a separate port from HTTPS Management under [System Maintenance] > [Access Control]

Improvement

1. Improvements to the design and functionality of [Applications] > [High Availability]
2. Corrected an issue with Port Redirection which could occur after upgrading to 1.1.x firmware
3. [Firewall] > [Filter Counter] indicates how many sessions have matched each rule
4. General improvements to [Firewall] menus and syslog output
5. Improvements to HTTPS filtering when using Web Content Filtering
6. Specify Remote IP / Host Name to limit Remote Dial-In VPN connections to that WAN IP / Hostname only
7. Bandwidth Limit can now apply to PPTP Remote Dial-In VPN clients
8. [Diagnostics] > [ARP Cache Table] now has an option to quickly create an IP Object for listed IP address
9. Supports Suffix Type in IPv6 Object configuration
10. Time Schedule in Filter Rules can now force sessions to clear when the schedule takes effect
11. Spotify can now be blocked with the Application Filter
12. Can specify which WAN interfaces can be used for remote management
13. Improvements to Traffic Graph and Data Flow Monitor
14. QoS Class was not displayed in the Session Table

15. Support for "esendex" SMS Provider
16. Custom SMS Provider option to define API settings manually for SMS providers not listed
17. Improved the SOA Serial Format for Inbound Load Balance DNS response
18. External Devices can now list up to 200 items

Known Issues

1. Due to significant changes to High Availability functionality, existing HA configuration will be cleared during the update process and it will be necessary to reconfigure High Availability after updating to 1.2.0
2. Disable "Force IPsec with L2TP" option in [VPN and Remote Access] > [PPP General Setup] to allow a standard L2TP tunnel, otherwise the L2TP server will allow L2TP with IPsec only
3. F/W 1.2.0 Changes the behaviour of the IP Filter. After upgrade some IP Filter rules may need to be reconfigured. Please read the "Filter Rule Actions" segment of this guide for more information on the changes: http://www.draytek.co.uk/support/guides/kb-3900-ipfilter-basics

Firmware Version	1.1.0.1 (Formal Release)
Release Date	9th September 2015
Build Date	27th August 2015
Revision	r5461
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

(None)

Improvement

1. Corrected an issue that could cause Port Redirection to not work after upgrading the firmware from 1.0.9 or earlier
2. Syslog to USB was not writing to USB after restarting the router
3. It was not possible to modify the max failed Telnet Login attempts before the router bans the IP
4. Netbios names were not displaying in the ARP cache table correctly
5. Improvements to certificate handling for the router's HTTPS interface
6. DNS Suffix (DHCP Option 15) support added for remote dial-in VPN clients
7. Upgraded OpenSSL to 0.9.8zg for security updates
8. Resolves an WAN connectivity issue that could occur after after an extended duration

Known Issues

1. You need to disable "Force IPsec with L2TP" options for pure L2TP tunnel in [VPN and Remote Access] > [PPP General Setup].
2. The upgrade may affect Port Redirection entries if the router's configuration has been upgraded from 1.0.7.1 or previous firmware. To resolve this issue, please use 1.2.0 firmware. If the router has been factory reset or was installed with 1.0.8 or later firmware, port redirection will work normally.

Firmware Version	1.1.0 (Formal Release)
Release Date	6th August 2015
Build Date	24th July 2015
Revision	r5322
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

1. SSL VPN LAN to LAN tunnel (Supported from DrayTek Vigor 2960 / 3900 1.1.0 firmware and Vigor 2860 / 2925 3.8.x firmware).
2. Internal RADIUS server under [User Management] > [RADIUS].
3. APP Enforcement supported app list added under [Objects Settings] > [APP Support List].
4. Added auto/manual APP Signature Upgrade setting page in [System Maintenance] > [APP Signature Upgrade].
5. [System Maintenance] > [Access Control] Improvements:
    a. Validation Code in Access Control tab to improve web admin security;
    b. Fail to Ban setting page to automatically block IP addresses after failed login attempts;
    c. Access Barrier setting page to protect router services (WUI, FTP etc) from brute force attack.
6. Added Switch Rate Limit setting page in [Firewall] > [Dos Defense].
7. Added [NAT] > [Connection Timeout] to allow altering the session timeout of different traffic types i.e. TCP, UDP etc
8. Wake on LAN can now operate on a schedule by configuring profiles in [Applications] > [Wake on LAN] > [Schedule Wake on LAN]
9. [Diagnostics] > [MAC Address Table] added.
10. [Diagnostics] > [User Status] added, to show PPPoE / Web Portal / VPN / SSL Proxy users in one location.
11. [LAN] > [LAN DNS] now supports wild-card strings and CNAME records for individual LANs using the Specified LAN option.
12. [Routing] > [Policy Route] Improvements:
    d. Priority options (Normal, High, Top) for more flexible routing.
    e. Country Objects as destination addresses.
    f. Failover options for target IP ping failure.
13. Support for Multicast via VPN.
14. Router's web interface can now notify of new firmware upgrades available.

Improvement

1. Improved DDoS protection.
2. SSL VPN settings now available under [VPN and Remote Access] > [PPP General Setup].
3. PPTP Dial-In VPN Profile (LAN to LAN) now supports multiple remote subnets.
4. LDAP/RADIUS support for the router's SSL Proxy facility.
5. [User Management] > [Web Portal] > [Portal Page Setup] now supports uploading an HTML file as the bulletin message.

6. Packet Inspection settings added under [Firewall] > [Filter Setup] > [Default Policy]
7. [User Management] > [User Profile] > [Apply All] improved to allow multiple choice.
8. Port Statistics now shown under [Diagnostics] > [Traffic Statistics].
9. Session Information added to [Diagnostics] > [Traffic Graph].
10. Vendor Information added to [Diagnostics] > [ARP Cache Table].
11. Daily / Period timout settings added to Web Portal under [User Management] > [Web Portal] > [General Setup].
12. Bind IP to MAC can now be applied to specific subnets.
13. Supported added for VPN routing through GRE over IPSec tunnel (VPN Trunk).
14. Keep VPN Setting option added to [Central VPN Management] > [CPE Management].
15. Alert interval of temperature sensor now configurable under [USB Application] > [Temperature Sensor] > [General Setup].
16. The router could not use a DNS server located on the LAN for DNS queries under some circumstances.
17. Traffic was unable to pass between LAN and PPPoE server clients.
18. Web Content Filter category selection page improvements.
19. IP Filter now shows a counter display for matched packets.
20. Policy Route increased to 120 entries, Static Route increased to 200 entries.

Known Issues

1. You need to disable "Force IPsec with L2TP" options for pure L2TP tunnel in [VPN and Remote Access] > [PPP General Setup].

Firmware Version	1.0.9.1 (Formal Release)
Release Date	16th February 2015
Build Date	2nd February 2015
Revision	r4765
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

(None)

Improvement

1. The IGMP Proxy feature's compatibility with some ISPs that use PPPoE has been improved.
2. Support for the Bandluxe C330 USB 3G modem.
3. SSL VPN now changes tunnel MTU in relation to the WAN MTU.
4. PPTP Dial-In User VPN connections could not access the internet under some circumstances.
5. Policy Route was not working with return path traffic.
6. The IPsec option "Auto Dial Out if WAN1 Down" was still taking effect after being disabled in the WUI.
7. The router's memory usage was higher than normal when using the Data Flow Monitor.
8. The Access Control List was not working correctly under some circumstances.
9. Improvements to ensure immunity to Ghost/CVE-2015-0235

Known Issues

1. You need to disable "Force IPsec with L2TP" options for pure L2TP tunnel in VPN and Remote Access >> PPP General Setup.
2. VPN Trunk tunnel should not be used with a profile name over 15 characters.

Firmware Version	1.0.9 (Formal Release)
Release Date	24th December 2014
Build Date	1st December 2014
Revision	r4542
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

1. Supports USB 4G/LTE. Check [USB]-[Modem support list] in the router's web interface for details.
2. Supports USB disk /FTP server.
3. Supports saving Syslog to USB disk.
4. Supports Policy Route (replacing Load Balance Rule and Address Mapping menus).
5. IPSec VPN tunnel can now be configured to pass or block NetBios packets.

Improvement

1. Disabled HTTPS SSL 3.0 for CVE-2014-3566, this can be configured from the [System Maintenance] > [Management] page.
2. Connection request notifications from Vigor ACS were not authenticated
3. Could not establish IPv6 static connection.
4. Allow downloading/uploading private key (for Host to LAN VPN by X.509).
5. Shows the VPN Type/Form fields on VPN History web page.
6. Improved handling for Duplicated Routes (with Static Route Metric). When the static route metric is <=10, the priority of that static route will be greater than a VPN route.
7. Support QoS for VoIP traffic from LAN.
8. Support "Ping to Keep Alive" feature for detecting whether an IPsec tunnel is able to pass traffic
9. Support WAN Port and IP Alias options for PPTP Dial Out connections.
10. Support for RFC 4638 (accommodating an MTU/MRU larger than 1492 for PPPoE protocol WAN connections).
11. Added STUN server option to TR-069 settings.
12. Added Jumbo Frame setting under [LAN]-[Switch]-[Jumbo Frame] to edit Maximum Frame size.
13. Added a "Clear" button for the DDNS settings page.
14. Bind IP to MAC can now export or import a list of IP / MAC addresses.
15. [Sytem Maintenance] > [Access Control] can now be configured to accept pings from the WAN on specified WAN interfaces.
16. Added “OVH” as service provider for DDNS setting.
17. Supports Range-to-many Port Redirection.
18. Improve login page customization for Web Portal setup.
19. Changed mechanism of deleting objects.

Known Issues

1. You need to disable "Force IPsec with L2TP" options for pure L2TP tunnel in VPN and Remote Access >> PPP General Setup.
2. VPN Trunk tunnel should not be used with a profile name over 15 characters.

Firmware Version	1.0.8.2 (Formal Release)
Release Date	15th August 2014
Build Date	13th June 2014
Revision	r3968
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

(None)

Improvement

1. PPTP connection stability improved
2. Web Portal stability improved
3. Improved: Remove management port setting which may occupy port redirection.
4. Improve the stability of High Availability function.
5. Add telnet timeout if login not completed in 60 seconds
6. CPU usage is too high when data flow monitor is enabled.
7. Improved interoperability with SSL VPN client
8. A problem of WCF license occurred when HA is enabled.
9. CVM can't perform configuration backup.
10. NAT Loopback to LAN More Subnet doesn't work.
11. DNS for PPTP Remote dial-in is not assigned according to the LAN Profile.
12. Reboot with Customized Configurations bug.
13. When firewall default policy (block) is used, HTTP is still available for access.
14. Web portal still supports URL redirect when login mode is disabled.
15. Packet count error when PPTP acceleration is enabled.
16. mOTP User profile cannot be saved without Password.
17. WAN Priority Bits doesn't work.
18. Time object error corrected
19. [WAN]>[Switch mode]>[double tag] error corrected
20. Upgrade OpenSSL to 0.9.8za for security updates.
21. Update WCF (Web Content Filter) to account for Commtouch name change to Cyren.
22. High Availability improvements
23. DDNS failover 3G WAN improvements

Known Issues

1. VPN Trunk tunnel doesn't work well when the profile name is more than 15 characters.
2. You need to disable "Force IPsec with L2TP" options for pure L2TP tunnel in VPN and [Remote Access]>[PPP General Setup]

Firmware Version	1.0.8 (Formal Release)
Release Date	11th March 2014
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

1. Same WAN VLAN ID can be used in different WAN interfaces. (WAN >> General Setup Mode: Advance, Switch Mode: Double Tag)
2. QoS for multiple WANs.
3. SNMP v3.
4. Country block for Firewall.
5. WCF white list.
6. LAN DNS server.
7. BGP routing protocol.
8. SSL VPN in tunnel mode
9. Support Web Portal and Hotspot (Guest profile) in User Management.
10. Support PPTP acceleration for PPTP WAN/Remote Dial-in/LAN to LAN
11. QoS retag option added
12. VPN dial-out failover if WAN disconnected.
13. Support VPN LAN to LAN for overlap/duplicate subnets.
14. Display the last UP/DOWN log of VPN profile.
15. Add default policy for Firewall and default block policy can be applied.
16. Add IPv6 firewall settings.
17. Add DNS object.
18. Add a remote capture telnet command (rc), for traffic monitor and wireshark remote capture.
19. Add front panel and VPN status on the dashboard.

Improvements

Web User Interface changes

1. Menu [User Managemen]>[General Setup] renamed [User Management]>[Web Portal]
2. Move [IP Routing] from to [Routing]>[Status Route] and rename as [LAN/WAN Proxy ARP]
3. Move [Inter-LAN Route] to [LAN]>[General Setup] from [LAN]>[Static Route]
4. Move status page to the first tab of each function menu.

Others

5. Support RADIUS, LDAP, Local authentication in User Management.
6. Support NAT option for IPsec LAN to LAN.
7. Support LDAP profile in Firewall.
8. Support ratio configuration for VPN Load Balancing.
9. Port number setting for Access Control in WAN IP alias can be passed to LAN by default.
10. Notification object can be recorded on Syslog through the configuration on [Applications]>[SMS/Mail Alert Service]

11. Support Local/RADIUS/LDAP authentication for PPTP/L2TP/PPPoE
12. Inter-LAN route priority changed so that IP filter can control
13. Support connection failover for TR-069.
14. Display router name in web page title.
15. IPsec VPN dial-in connection with all WANs is supported in default.
16. Support RFC3021.
17. Combine IM/P2P/Protocol object to App Object for blocking more Apps.
18. Management Access Control List increased up to 16 entries
19. Support peer identity for IPsec RSA authentication.
20. Support password encode option for configuration backup.
21. Support more special characters in username for user profile.
22. Number of SSL web proxy/VNC/RDP profiles increased to 30
23. Support customized DDNS.
24. Support acceleration of fragmented UDP packets (maximum 1628 bytes).
25. Support DHCP option 95 (LDAP server), 161(FTP server), and 162 (File path)
26. Support more subnet DHCP servers in Bind IP to MAC.
27. Support DHCP relay over LAN/Non-Direct-Connected LAN.
28. Support DHCP relay settings for PPTP/L2TP/PPPoE.
29. Support open port to the host in remote VPN network.
30. Default route cannot work well when two WAN IPs are in the same IP network.

Firmware Version	1.0.7.1 (Formal Release)
Release Date	13th November 2013
Build Date	12th November 2013
Revision	r3067
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

(None)

Improvement

1. Support USB-WAN for WAN Profile under the Setting tab in Application>> Dynamic DNS.
2. Support WCF (web content filter) in High Availability (HA) application.
3. Modify the mechanism for IP filter, "if no further match" action.
4. Add a subnet mask setting, 255.255.255.254, for WAN IP configuration.
5. Added option disable negotiation for Fiber WAN under the Interface tab in WAN>>Switch.
6. 'space' special character can be used in the username for LDAP
7. QoS IP rule can apply the packets passing through both Local IP and Remote IP.
8. Improved PPTP service mechanism for multiple simultaneous LAN to LAN dial-ins
9. Corrected: Can not block / unblock some IPs on Diagnostics>>Data Flow Monitor.
10. Corrected issue with ICMP packets larger than 8138 bytes over IPSec LAN to LAN tunnel.
11. Corrected: The user can not access Internet when QoS queue weight is set as "0".
12. Corrected: Lower the priority of Inter-LAN routing function.
13. Corrected: LAN DHCP packets do not respond while LAN DHCP Server is OFF.
14. Corrected: Can't accept L2TP VPN from (None) default route WAN.
15. Corrected: RADIUS client (Vigor router) sends wrong NAS IP address (127.0.0.1).
16. Corrected traffic status of DHCP over IPsec in VPN Connection Management.
17. ARP detection may fail when WAN TX traffic is full.
18. Corrected: SMS can't be sent out when L2TP over IPsec is up and down.

Known Issues

1. VPN Trunk tunnel doesn't work well when the profile name is more than 15 characters.
2. You need to disable "Force IPsec with L2TP" options for pure L2TP tunnel in [VPN and Remote Access]>[PPP General Setup]

Firmware Version	1.0.7 (Formal Release)
Revision	2733
Release Date	2nd Sept 2013
Build Date	27th Aug 2013
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

1. Support Central VPN Management (CVM). Up to 16 devices can be managed.
2. Support 3G backup/load balance.
3. Support inbound load balance.
4. Support VPN Trunk failover mode.
5. Support PPPoE quota setting and MAC address filter.
6. Support USB temperature sensor. http://www.draytek.co.uk/products/usb-thermometer.html
7. Support SMS, Email Alert and Notification object profiles for WAN/VPN connection and USB temperature sensor.

Improvement

1. Improved: Support SmartMonitor users up to 500.
2. Improved: VPN Trunk throughput and stability.
3. Improved: By default disable insecure SSL Encryption Key Algorithms
4. Improved: Support DHCP relay on VPN.
5. Improved: Add Active Standby mode for High Availability (HA).
6. Improved: QoS redesigned
7. Improved: Username reported to Syslog
8. Improved: Add option 60(Vendor ID), 61(Client ID) for WAN DHCP mode.
9. Improved: Add default maximum session number for Session limit.
10. Improved: Add flow control settings for Switch.
11. Improved: Add user defined options for DHCP server.
12. Improved: Improve DMZ function.
13. Improved: Add log and force update function for DDNS.
14. Improved: Add Force L2TP with IPsec policy option enabled in default.
15. Improved: Corrected causes for high CPU usage being displayed in Web UI
16. Improved: Stability in TR-069.
17. Improved: Firmware upgrade speed.
18. Fixed: Time object cannot work correctly when daylight saving is enabled.

Known Issues

1. VPN Trunk tunnel doesn't work well when the profile name is more than 15 characters.
2. You need to disable "Force IPsec with L2TP" options for pure L2TP tunnel in [VPN and Remote Access]>[PPP General Setup]

Firmware Version	1.0.6.1 (Formal Release)
Release Date	10th April 2013
Build Date	25th March 2013
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

(None)

Improvement

1. NAT Port Redirection Rule for FTP server didn't work with two WAN connection
2. Customized web content message would disappear after rebooting the router
3. Improvements to VPN Trunk tunnel where profile name are long
4. PPTP connection display error in VPN Graph for syslog utility
5. PPTP WAN could not dial-up if the server was set with a domain name
6. Fixed issue with ping to VPN remote network working after clicking WAN DHCP Renew Button via web user interface
7. Fixed Session limit rule notapplying the correct limit due to subnet mask caculation error
8. Fixed that WAN status displays “up” when the WAN cable is unplugged and WAN detect mode is set with “(None)”
9. Corrected an issue with SNMP set/get Community setting
10. Resolved that VPN traffic wouldn't flow while one of the VPN GRE tunnels is disconnected
11. Corrected issue preventing some vLAN users from accessing Internet via Browser
12. Improved DHCP renewal interoperability
13. Fixed LAN VLAN configuration issues after restoring the web configuration
14. Corrected WAN1 MAC address used
15. Improved SIP ALG feature
16. Fixed that IPSec tunnel uptime would not reset after VPN reconnection
17. Corrected PPTP sessions problem that would prevent new network connections being setup
18. Corrected that a PC from remote subnet could't access Internet via PPTP LAN to LAN tunnel
19. Improvments to IPv6 traffic handling via AICCU
20. Improved load balance where multiple PPPoE connections have the same gateway
21. Corrected issue where multiple WAN disconnections could prevent VPN Trunk from reconnecting
22. Added information for remote network connected with GRE over IPsec to Routing Table
23. Corrected issue where enabling Perfect Forward Secrecy in VPN client could prevent connection
24. Display issue with transmitted/received (TX/ RX) packets in Connection Management fixed for VPN clients behind NAT
25. Improved parameters stability for TR-069
26. Improved throughput between different VLANs
27. Added sending ARP for WAN Alias IP to WAN Gateway when connected
28. Added support for VPN on Alias WAN IP and IP Routing IP
29. Add mail alert when VPN is up

30. High availability improvements

Known Issues

1. VPN Trunk tunnel profile names should be kept to less than 15 characters.

Firmware Version	1.0.6 (Formal Release)
Release Date	2nd Jan 2013
Build Date	6th Nov 2012
Applicable Models	Vigor 3900
Locale	UK ONLY

New Features

1. VPN(IPSEC) Routing Acceleration
2. Supports PPPoE server for LAN PC connection
3. Support VPN Alarm via E-mail & Syslog
4. Support VPN Graph for syslog utility
5. Support PPP mode for IPv6
6. Support domain name for IPSec/PPTP dial-out

Improvements

1. URL filter can block HTTPS connection by host keyword
2. WCF support https block by web category
3. Add QQ account filter for Firewall
4. WAN4 is regarded as physical DMZ port
5. Add time schedule for session limit and bandwidth limit
6. Web content filter (WCF) stability improvements
7. Data flow monitor resource allocation improvements
8. DHCP server cannot work when Multi-LANs is configured
9. Hosts under routing LAN can not access into the router
10. Configuration backup may fail
11. UPnP improved
12. Changing web port could prevent User management from working
13. WebUI server security improvements
14. IPsec RX/TX packets count may have error after entering phase2 rekey
15. L2TP connection status error after disconnection.
1. 16 Cannot create IPsec VPN in aggressive mode when selecting AES as IKE phase 1 encryption.
16. PPTP dial-in may fail while using static IP mode.
17. VPN load balance may not work after connection reconnects
18. SSL Application doesn't work when HTTPS port is not set with 443.
19. Support PPTP dial on demand and idle timeout.
20. Support URL filter rules move up/down.
21. Support VLAN priority in LAN/WAN interface.
22. Support QoS packet by DiffServ (DSCP/TOS) for outgoing packet.
23. Let the user profile password support more special characters in standard ASCII table.
24. Show the IP binding with MAC in DHCP table.
25. Mail Alert Send test e-mail button added
26. Add 36 regions time zone options for NTP.
27. Improve user management login process.

28. Add Common Name Identifier field in LDAP configuration.
29. Add an option for DDNS to select Internet IP or WAN IP.

Known Issues

1. VPN Trunk tunnel profile names must be less than 15 characters.

Firmware Version	1.0.5 (Formal Release)
Release Date	4th Sept 2012
Applicable Models	Vigor 3900
Locale	UK ONLY

First Firmware Release

Known Issues

- Devices on non-NAT subnets are unable to access the routers management interface

[END OF FILE]