NO:AP1101-2 V.1

Release Note for Vigor2962

Firmware Version:	4.4.3.1
Release Type:	Normal - Upgrade recommended when convenient
Applied Models:	Vigor2962, Vigor2962P

Read First

- Due to the WebGUI security issue (fixed in 3.9.6.3), we recommend **changing the passwords** for admin login and password/PSKs for VPN profiles after upgrading the latest firmware from 3.9.6.2 or earlier.
- Before upgrading to 4.4.3, please upgrade to 4.3.2.7 or after to avoid configuration compatibility first.

New Features

- Support four WANs.

Improvement

- Improved: Improve the Web GUI Security.
- Improved: Issues related to WCF Improvements.
- Improved: Increase the RADIUS Timeout up to 120 seconds.
- Improved: Support Auto-check WAN MTU for PPPoE connection.
- Improved: Support for multiple untagged PPPoE on the same port.
- Improved: Add the country code in alert mail for VPN connections.
- Improved: Display the unit for Block Time on Firewall>>Defense Setup.
- Improved: Support unlimited quota for Customized SMS Service Object.
- Improved: Support WAN alias IP for Server Load Balance and Port Knocking.
- Improved: Increase Webhook Server URL character limit (beyond 64 characters).
- Improved: Support complete certificate chain for IKEv2 EAP VPN authentication.
- Improved: Modify Brute Force Protection due to usage by Smart Action (Suricata).
- Improved: Improve Management/SNMP WUI so it no longer requires a router reboot.
- Improved: Add a new log alert: "VPN service is disabled for WANx" when VPN service is not enabled.
- Improved: Support for customizing the port in "Vigor Router SMS Gateway" (SMS Service Object).
- Improved: Support Vigor management from TR-069 servers using either uppercase or lowercase HTTP headers.
- Improved: Add a new option of Port Knocking as Source IP for NAT>>Open Ports and NAT>>Port Redirection.
- Improved: Improve the User Management redirect speed by eliminating unnecessary HTTPS page redirection.
- Improved: Add an IP search box for Blocked IP List (Brute Force IP) on System

Maintenance>>Management.

- Improved: Unify Port Knocking for Local Service and Brute Force Protection on System Maintenance >> Management.
- Improved: Add early notification for expiring certificates to Syslog to prevent connection issues due to expired certificates.
- Improved: Add a note about VPN support for LDAP/AD Authentication on VPN and Remote Access >> PPP General Setup.
- Improved: Add the Port Knocking Tools download link on the pages of NAT>>Port Knocking and System Maintenance>>Management.
- Improved: A local certificate with an expiration date less than or equal to 397 will not get a warning message after modification.
- Corrected: An issue with the buffer overflow in SSL VPN.
- Corrected: An issue with reversed Internet IP for DrayDDNS.
- Corrected: An issue with failure to connect to third-party ACS.
- Corrected: An issue with PPTP VPN failure from Android Phone.
- Corrected: An issue with failure to set a hotspot with the created API.
- Corrected: An issue with failure to restore backup NAT configuration.
- Corrected: Issues related to Remote Dial-in User's IPsec Peer Identity.
- Corrected: An issue that some NAT WUIs showed unused WAN interfaces.
- Corrected: An issue with rebooting every few hours after enabling the WCF.
- Corrected: An issue with the host display on Diagnostics>>Data Flow Monitor.
- Corrected: An issue with import/export configuration related to long integer values.
- Corrected: An issue with missing the Management option on WAN>>Multi-VLAN.
- Corrected: An issue that Firewall Filter Set 1 was empty after the firmware upgrade.
- Corrected: An issue with the router reboot while editing the remote dial-in user profile.
- Corrected: An issue with failure to open Bandwidth Management >> Quality of Service.
- Corrected: An issue that LAN DNS behavior changed between versions 4.3.2.7 and 4.4.3.
- Corrected: An issue with a router reboot problem caused by the conntrack table being full.
- Corrected: An issue that SFP P1 link was up (1Gbps) but no ARP entry after upgrading to 4.4.3.
- Corrected: An issue with not centering the Login Page Greeting in WUI when using HTTP.
- Corrected: An issue with unnecessary character appeared on Diagnostics>>NAT Sessions Table.
- Corrected: An issue with network stability (dropped regularly every 2-3 days) of OpenVPN.
- Corrected: An issue that failure to renew DrayDDNS after changing the IP address of WAN interface.
- Corrected: An issue with missing Delete and Rename options on the USB Application >> File Explorer.
- Corrected: An issue with the password and key on VPN LAN-to-LAN not hidden well on the backup file.
- Corrected: An issue that Open Port failed to direct the traffic to a virtual server which had two IP addresses.
- Corrected: An issue with failure to use SSL VPN LAN-LAN in NAT mode to reach the remote network.
- Corrected: An issue with an error message appeared on User Management after enabled the Validation Code.
- Corrected: An issue with the CPE device lost Internet access via high availability while

using two switches.

- Corrected: An issue that WANx first for the DrayDDNS service not working when the Internet IP was used.
- Corrected: An issue with the wrong direction display of VPN Log Details on Diagnostics>>VPN Graph.
- Corrected: An issue that DDNS failed to update correctly because HA status was not yet complete during the boot process.
- Corrected: An issue that WUI login logs was being displayed under User Access, but it should be under Others on Syslog.
- Corrected: An issue with displaying incorrect values when editing a filter rule with the direction of WAN-> LAN/RT/VPN selected.
- Corrected: An issue that URL Filter failure to block HTTPS websites when TLS 1.3 hybridized Kyber was enabled in the browser.
- Corrected: An issue with Hotspot HTTPS redirection not working when Vigor HTTPS management port was set to a non-default value.
- Corrected: An issue that NAT Port Redirection Rule (e.g., index 2) was disabled automatically when modifying rules on other pages.

Known Issue

- TR-069 parameters for Application >> Smart Action is not completed.
- The web portal may cause the router to be too busy to respond quickly.
- The encryption method for OpenVPN will be returned to the factory default settings if upgrading the firmware version from V3.9.7.x to V4.3.1.
- To prevent potential errors when upgrading firmware, it is recommended to upgrade firmware sequentially one version at a time. (e.g., if the current firmware is 3.9.1, upgrade to 3.9.2 then 3.9.7.2, and then the latest version).
- When the firmware is downgrading via “System Maintenance > Firmware Upgrade”, one might have a chance to experience a config compatibility error, which causes the config of a certain function to return to the default setting. To avoid this error, “System Maintenance >> Configuration Export >> Restore Firmware with config” is the preferred way for firmware “downgrading”. We suggest backup the config file before upgrading any firmware as well.
- Inter-LAN routing setting exported/backed up from firmware 4.3.2 release might be incorrect, please check inter-LAN routing settings.