NO:AP1101-2 V.1

Release Note for Vigor2962

Firmware Version:	4.4.3
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 to avoid configuration compatibility first.

New Features

- Support NAT >> Server Load Balance.
- Support port knocking (for local service).
- Support VPN Traffic Graph on Diagnostics>>VPN Graph.
- Support TLS v1.3 on System Maintenance>>Management.
- Support TOTP for Remote Web Management on System Maintenance>>Administrator Password.
- Support VPN Isolation, VPN packets capture, Active Directory and 2FA for VPN users, IPsec AES-GCM and SHA-512 authentication.

Improvement

- Improved: The primary router can sync Time & Date settings for High Availability.
- Improved: Upgrade jQuery to version 3.5.1 for web security.
- Improved: Add VPN Peer IP country info in VPN Connection Status.
- Improved: Enhancement for Brute Force Protection, DoS and Firewall.
- Improved: Add Fail login and Brute Force Protection Alerts in Notification Objects.
- Improved: Enlarge Radius client numbers from 30 to 200 to make the Web Portal function work in a School Dormitory.
- Improved: Support the new Fast NAT option to skip the DNS packet inspection to reduce the CPU load in a specific environment.
- Corrected: An issue that VPN Log Details WUI showed wrong direction.
- Corrected: An issue that DoS defense failed to stop TCP SYN flood attack.
- Corrected: An issue that User data quota in User Management did not work.

- Corrected: An issue with any LAN port traffic information not shown by PRTG.
- Corrected: An issue that the firewall did not block incoming ICMP packets from VPN LAN to LAN.
- Corrected: An issue that no traffic on UDP port until reboot when Wireguard VPN dropped and came back.
- Corrected: An issue with failure to work in the SMS customized object and the Send a Test message function notes.
- Corrected: An issue where 200 IPsec Dial-Out VPNs (neither NordVPN nor IPVanish) couldn't go online after a system reboot.
- Corrected: An issue that VoIP - Incoming/outgoing calls failed based on the "Allow pass inbound fragmented large packets" status.
- Corrected: An issue with failure to block specific websites by using URL Reputation, "Get Request Resource Failure" showed in the syslog.
- Corrected: An issue with failure to dial-up IPsec VPN to the server with Domain Name when the server changed to a new IP (due to DNS cache time being too long).

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.