KATIM® GATEWAY 9011-X

Easy to deploy, post quantum secure network solution for easy roll-out of any IT service/application with a full network security.

TECHNICAL SPECIFICATION AND KEY FEATURES

Next-gen security – stop security trade-offs forced by legacy encryptors

- Custom designed encryption control plane for key exchange, encryption and authentication
- Post Quantum cryptography with Crypto Agility day 1
- Custom cryptography via 3-rd part black box algorithm integration
- Latest in device security with always-on tamper protection including transport
- Viper OS S/W: stops security trade-offs for functionality like bypass, networking features, plain/cipher firewalls

Cloud overlay concepts applied to network encryption

- Overlay QoS-aware security planes isolate encryption from underlying network
- KATIM® Gateway application mapping to pre-established KATIM® Gateway security planes allow easy IT roll-out of services and new applications
- Cipher and plain firewalls atop of secure planes restore network perimeter for Intranet, allow IS to increase focus on external network traffic risks

S/W programmable platform that adapts to your needs

- No more dedicated devices to meet you various capacity, functionality needs
- Any of L2/L3, P2P, P2MP, MP2MP, built-in diode support – via S/W license and/or S/W upgrade
- Flexible capacity options with s/w upgradability for grow-as-you-need

CRYPTOGRAPHY AND KEY MANAGEMENT

Algorithms

- Full custom cryptography integration for cryptography support.
- Fully programmable H/W module for crypto evolution and custom cryptography support including post-quantum cryptography
- UAE National crypto post quantum suite integration for an UAE developed product

Peer-authentication, Key Exchange and VPN Tunneling of Encrypted Traffic

- Noise-based custom built next generation protocol
- Flexible crypto protocol handshake
- Independent, asymmetric classic and post-quantum key exchange using UAE National crypto suite
- Authenticated key exchange with peer identity protection by pre-shared discovery keys
- Data confidentiality and integrity protection in protocol handshakes and encrypted data packets
- Aggressive, customisable up to an individual packet level key ratcheting with per every encryption tunnel keys
- Frequent re-handshake for post compromise security
- Stealth protocol operation