

NITRO Wireless

Post Quantum Cryptography (PQC) Test

A TeraVM Security Solution, preparing for a quantum safe future

The Challenge Facing Managed Security Service Providers (MSSP)

Quantum computers have the potential to break public-key cryptography once they begin operating at a large scale – Governments, military, enterprises and mobile operators are already preparing for a quantum-safe future to protect their vast stores of sensitive data. The U.S. federal government has mandated the migration of all existing public-key cryptographic systems including network security devices such as firewalls and VPN gateways to PQC. Post quantum cryptography protocols in wireless networks will introduce additional network performance overhead that can impact the end-user experience.

The VIAVI Solution

Testing is essential for developing and deploying all cryptographic systems, including newly established PQC-based systems. TeraVM Security Test enables benchmarking of the performance of enterprise devices, content delivery networks and endpoints that initiate or terminate IPSec Traffic using PQC. VIAVI has years of experience in security device testing which translates into tangible solution benefits that enable our customers to bring products to market faster and with less risk of bugs slipping through. The TeraVM Security Solution provides high capacity performance testing at scale on devices embedded with PQC technology.

Business Impact

Organizations need to upgrade their processes, systems, hardware, software and services to avoid Store Now, Decrypt Later (SNDL) threats where encrypted sensitive information can be hacked and stored to be decrypted and acted upon when quantum computers are available. When cryptographic protocols are deployed in data transmission infrastructure, they can place a significant load on communications and cause latency problems, resulting in poor quality and lower throughput. Not testing new PQC algorithms on security devices could be risky, there may be serious impact on network performance.



Sample Use Cases

Use Case 1: Benchmarking the performance of VPN tunnels hardened with PQC. Measure latency and throughput KPIs as tunnels scale up.

Use Case 2: Test hybrid mode with mix of PQC and classic algorithms across VPN tunnels.

VIAVI Benefits

- ✓ **First PQC Test Solution**
TeraVM is the first cloud-enabled test platform to support PQC algorithms mandated by the U.S. National Institute of Standards and Technology (NIST).
- ✓ **Virtualized and Containerized Solution**
TeraVM Security Test is a fully virtualized, containerized solution which is also supported on all major cloud platforms.
- ✓ **Proven Security Test Experience**
Over 15 years experience testing next-generation Firewalls.
- ✓ **Performance Metrics on Tap**
Easy access to user performance metrics – MoS scores, Latency, Throughput, Tunnel establishment time.



Get started with PQC Test solutions

Visit: viavisolutions.com/pqc



Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

© 2024 VIAVI Solutions Inc.
Product specifications and descriptions in this document are subject to change without notice.
Patented as described at
viavisolutions.com/patents
ppqc-nitwir-br-wir-nse-ae
30194259 900 1024