netskope

White Paper

Preparing for a Future with Post Quantum Cryptography

Guidance on the Use of Encryption within Netskope One

Table of Contents

CONTENTS

INTRODUCTION

Classical public-key cryptography relies upon mathematical concepts that are difficult for classical computers to solve. This type of encryption is standard in most of today's digital systems, but may be easily solved by a large-scale quantum computer.

The advancing progress of quantum computing is creating a new urgency for the development of techniques and algorithms that could withstand an attack by a large-scale quantum incursion.

Post quantum cryptography (PQC) refers to cryptographic techniques and algorithms specifically designed to withstand reverse engineering attacks by powerful quantum computers.

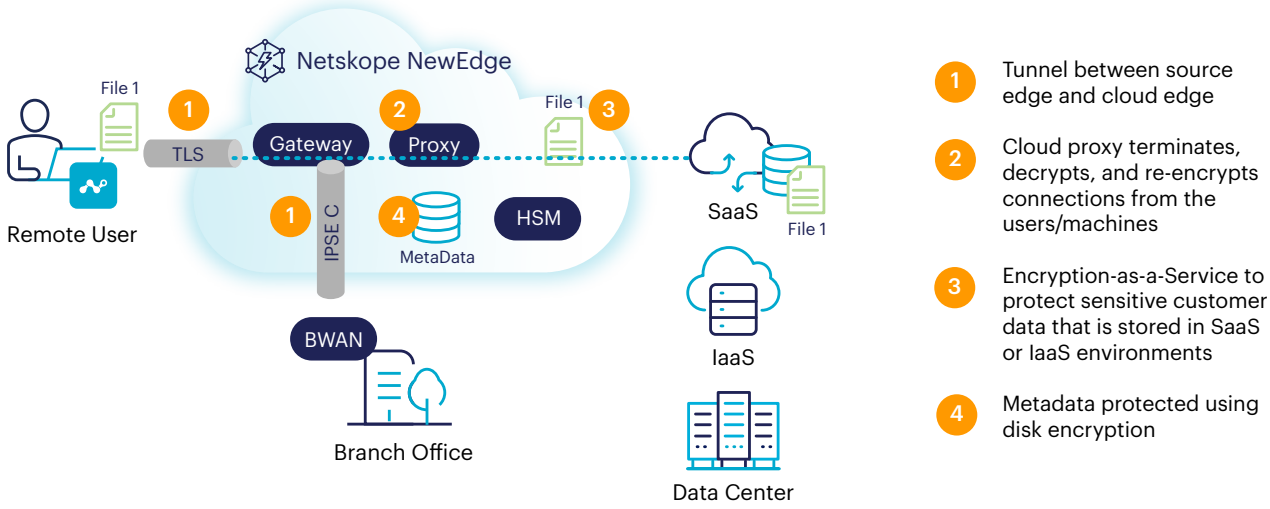
Two areas of current focus for PQC development are:

- Key Exchange Protocols: Updating secure key exchange protocols, such as Diffie-Hellman and RSA, which could be vulnerable to attacks from a large-scale quantum computer.
- Digital Signatures: Replacing cryptographic hash functions and digital signatures that are used for data authentication but may not provide sufficient security against quantum attacks.

This document has been designed to provide an overview of the way in which encryption is currently used within the Netskope One platform, and provide Netskope's current view of dealing with the emerging threat of quantum computing.

CRYPTOGRAPHY IN ACTION IN NETSKOPE ONE

The Netskope One platform leverages encryption technology in a number of different areas as part of the provision of its various security and networking services. The figure below is a representation of the environment with the different use cases for encryption.



The main areas where encryption is used are: (numbers in parentheses refer to the figure above)

- **Traffic Steering:** Users/machines generate network traffic destined for SaaS, Iaas/PaaS, web, or internal applications. This traffic has to be steered to the Netskope NewEdge Network for the delivery of security service edge (SSE) services. Steering can be controlled by either the Netskope One Client, a single endpoint agent, or Netskope One Gateway, an SD-WAN/edge router. Both the endpoint agents and the gateway/routers establish tunnels (1) between the source edge and the cloud edge. The tunnels are TLS or IPsec, which use encryption for securing the traffic.
- **Cloud Proxy:** In the delivery of security services, the cloud proxy needs to terminate, decrypt, and re-encrypt the TLS connections (2) from the users/machines. In order to do this, the proxy has to negotiate the encryption algorithms used in the TLS connections.
- **Data Encryption:** The Netskope One SASE platform offers encryption as a service to protect sensitive customer data (3) that is stored in SaaS/IaaS environments. Additionally, metadata that is persistent in the SASE platform itself is protected (4) using disk encryption.
- **Internal Comms:** Internal systems within the Netskope One SASE platform use TLS to communicate between themselves. Additionally the systems are administered using secure access protocols like SSH that use encryption for data in transit across the network.

CURRENT ENCRYPTION KEY ARCHITECTURES

There are two types of encryption key architectures in use in the Netskope One Platform, and the threat of quantum computing differs based on the type of encryption.

Encryption in use within Netskope One:

- Symmetric key encryption used inside the established TLS/SSH connection as well as for data encryption
- Asymmetric key encryption used in IPsec and TLS/SSH connection setup and for digital signatures

Symmetric encryption algorithms like the Advanced Encryption Standard (AES-256) are considered to be less susceptible to post quantum computing and hence not of major concern because they use well established mathematical operations. In the immediate future the security of symmetric encryption algorithms can be further strengthened by using larger key sizes that would require much more computing power to crack and hence not of concern even with quantum computers.

Netskope currently uses AES-256 GCM algorithm for symmetric encryption that is considered to be immune to known factoring based threats.

Asymmetric encryption algorithms are more vulnerable to quantum computing. A large-scale quantum computer with the capability to run Shor's algorithm could significantly reduce the time needed to factor large numbers. In the last few years, advances in quantum computing have been made public, raising concerns of a new threat called “harvest now decrypt later” (HNDL) becoming a reality.

Optimistic estimates suggest that these algorithms will be “quantum safe” for the next several years, but Netskope is already taking action to address this threat.

Netskope Best Practices

- The Netskope One Platform implements industry-accepted best practices in the implementation of encryption algorithms to strengthen its stance. Notably:
- Netskope NewEdge Network and infrastructure contains FIPS 140-2 Level 3 certified Hardware Security Modules (HSM) for securing sensitive cryptographic keys.
- All private keys only reside in HSM or process memory (with a locally generated key pair) and never traverse network connections.
- Private keys not residing in HSM are short lived (as little as seven days) to limit the usefulness of the key in case of any compromise.
- The Netskope One Platform supports the BYOK option for using the HSM in a customer premise in place of the HSM in Netskope’s Cloud.
- For symmetric encryption, the Netskope One Platform defaults to the AES-256 GCM algorithm, considered safe from quantum computing-powered cracking attempts.
- For asymmetric encryption, the Netskope One Platform uses RSA and Elliptic Curve cipher suites with plans for supporting PQC algorithms (discussed below).

QUANTUM SAFE/POST QUANTUM CRYPTOGRAPHY OPTIONS

There are multiple tracks of research in progress across academia and private industry, working to come up with secure and efficient algorithms that are quantum safe.

- Quantum Safe/PQC Encryption Algorithms
  - NIST, ITU, and ETSI are all working on the standardization of quantum safe encryption algorithms. NIST has selected four algorithms (one for key exchange and three for signatures) that can withstand attacks from quantum computers and has released draft standards for three of them, which are now ready for use.
  - NIST is also sponsoring the Open Quantum Safe (OQS) project that supports the prototyping and development of open-source implementations of these algorithms. Liboqs is part of the OQS project, aiming to develop and integrate quantum safe cryptography into applications
  - Liboqs is a fork off the main branch of openssl library and not officially blessed by the OpenSSL foundation. The OpenSSL team is working on their native implementation of the PQC algorithms and expect them to be available around Q2 2025.
- Quantum Key Distribution (QKD): QKD leverages quantum mechanical systems to generate and distribute cryptographic keys. This requires specialized systems that communicate over dedicated links. QKD only provides confidentiality of the data and does not support the mechanisms for authentication and integrity that are needed for the various use cases listed in this document.

Netskope has a technical advisory board that includes cryptography experts, and is keeping up with NIST activities on standardization of post quantum cryptography algorithms. At this time, the shortcomings of QKD do not make it a viable option for the Netskope use cases, so Netskope is focusing on the addition of support for the PQC algorithms.

POST QUANTUM CRYPTOGRAPHY—THE ROAD AHEAD

Netskope leverages the OpenSSL library for cryptography functions, and OpenSSL v3.5 will be the initial public release of the library to support PQC algorithms. The timeline for this is the second half of 2025. In the meantime, the existing release of OpenSSL can be integrated with alternative crypto providers like liboqs that support PQC algorithms.

Netskope's PQC roadmap will address the most vulnerable part of the TLS/IPsec protocol, which is the key agreement phase. ML-KEM (one of the NIST approved algorithms) is used for the key agreement phase of the TLS/IPsec connection and is gaining momentum with most popular browsers already supporting this algorithm.

There are three parameter sets of the ML-KEM algorithm—512, 768, and 1024. Netskope will be supporting ML-KEM 768 for the TLS/IPsec key establishment in a multi-phase approach. This follows the NIST recommendation that the ML-KEM 768 parameter set provides a large security margin at a reasonable performance cost.

This support will be rolled out in a phased approach:

Phase 1

Netskope traffic steering components – Netskope One Gateway and Netskope One Client tunnel the user traffic through TLS/IPSec tunnels to avoid the unsecured internet. The Client and Gateways will support ML-KEM 768 PQC algorithms for the client and server side of the TLS/IPSec tunnels. In subsequent releases support for additional parameter sets of the ML-KEM algorithm will be added.

The Netskope proxy will support ML-KEM 768 PQC algorithms for client-to-proxy and proxy-to-server TLS connections.

Phase 2:

Netskope will roll out PQC support broadly in other parts of its internal infrastructure where IPsec/TLS is used for communications.

Phase 3:

Netskope will support PQC-enabled X.509 certificates that incorporate PQC algorithms alongside traditional cryptography algorithms.

Initial support for PQC will be made available in a sandbox environment for customers to test. After sufficient sandbox testing and once PQC support is officially released in OpenSSL, Netskope will make the PQC functionality generally available in the production environment.

STAYING AT THE FOREFRONT OF INNOVATION AND EXCELLENCE

Netskope is committed to staying ahead of new technology and trends in the market as they evolve.

We welcome collaborative engagement with customers and prospects to ensure we continue to exceed the security and performance needs of the market as post quantum cryptography matures.

REFERENCES

https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

NIST FIPS 203 ML-KEM Standard
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

Open Quantum Safe
https://openquantumsafe.org/

Short-Lived TLS Certificates
https://www.ieee-security.org/TC/W2SP/2012/papers/w2sp12-final9.pdf

Cloud Security Alliance Quantum-Safe Security Working Group
https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

Interested in learning more?

Request a demo

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs. Learn more at netskope.com.