Solution Brief

Post-Quantum Security for Mobile Classified Data Access

Equus, Arqit, and Intel achieve a CSfC-compliant MACP architecture designed to protect classified data against emerging threats from cryptographically relevant quantum computing

The Mobile Access Capability Package (MACP)[1] was developed by the U.S. National Security Agency as part of its Commercial Solutions for Classified (CSfC) program with the aim of protecting classified data in transit (DIT) across untrusted networks to and from mobile end user devices.

The ability for remote work to be accomplished securely is a critical operational requirement which spans across commercial enterprises and government agencies. Therefore, it is crucial to address mobile requirements for organizations that handle classified or other sensitive data while maintaining highly secure DIT without losing the flexibility that mobile operations fundamentally provide.

The MACP can achieve this most effectively by leveraging the NSA CSfC Enterprise Gray architecture (see Figure 1), which requires that sensitive data that needs to be transported across unsecured internet space (black) from one secure network enclave (red) to another must do so through two layers of encrypted tunnels, built using commercial off-the-shelf encryption components such as VPN clients and gateways operating in an intermediate service network layer (gray).

The establishment of MACP solutions via Enterprise Gray is fundamentally intended to eliminate the need for Type 1 encryption products, saving substantially on cost in addition to size, weight and power (SWaP) while also eliminating the extensive technical support requirements and limitations of dedicated hardware encryptors.

However, organizations still face several challenges when implementing a MACP solution. New technologies threaten existing encryption. In particular the key exchange method used in establishing IPsec connections can be broken by cryptographically relevant quantum computers (CRQC) via Shor's algorithm.

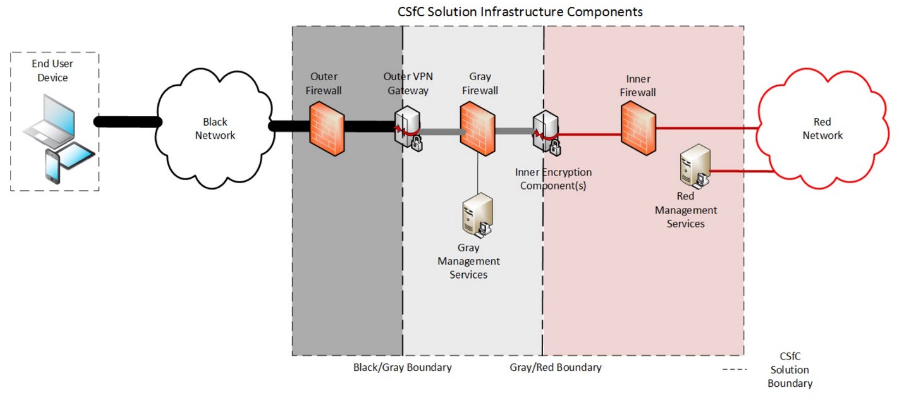

Figure 1. Image depicts the Enterprise Gray architecture enabling end user device access to a secure network. Source: CSfC Mobile Access Capability Package.

This risk is considered both serious and inevitable enough to warrant the U.S. Government to release the 2022 National Security Memorandum (NSM) 10 expounding upon it, and mandating adoption of quantum-secure encryption schemes.[2]

Security management and upkeep are particularly challenging in environments with diverse components and solutions in geographically separate locations. The traditional methods of furnishing sensitive assets with encryption resources – such as manual key generation, couriering, and fill – have proven to be logistically impractical at scale and inherently preclude benefiting from modern paradigms. The addition of the "mobile" aspect of the MACP only serves to exacerbate this dilemma.

Updating MACP to be Quantum Safe

Intel® Industry Solution Builders members Equus Compute Solutions (ECS) and Arqit Quantum have teamed up with Intel to develop a practical solution that provides next-generation security and performance for relevant topologies and use-cases while bringing the entire solution into the modern era. The solution was deployed between the ECS and Intel technical labs, located in California and Oregon respectively, providing a testbed that directly addresses both the threat posed by quantum computers as well as the cryptographic logistics problem at the heart of symmetric key management.

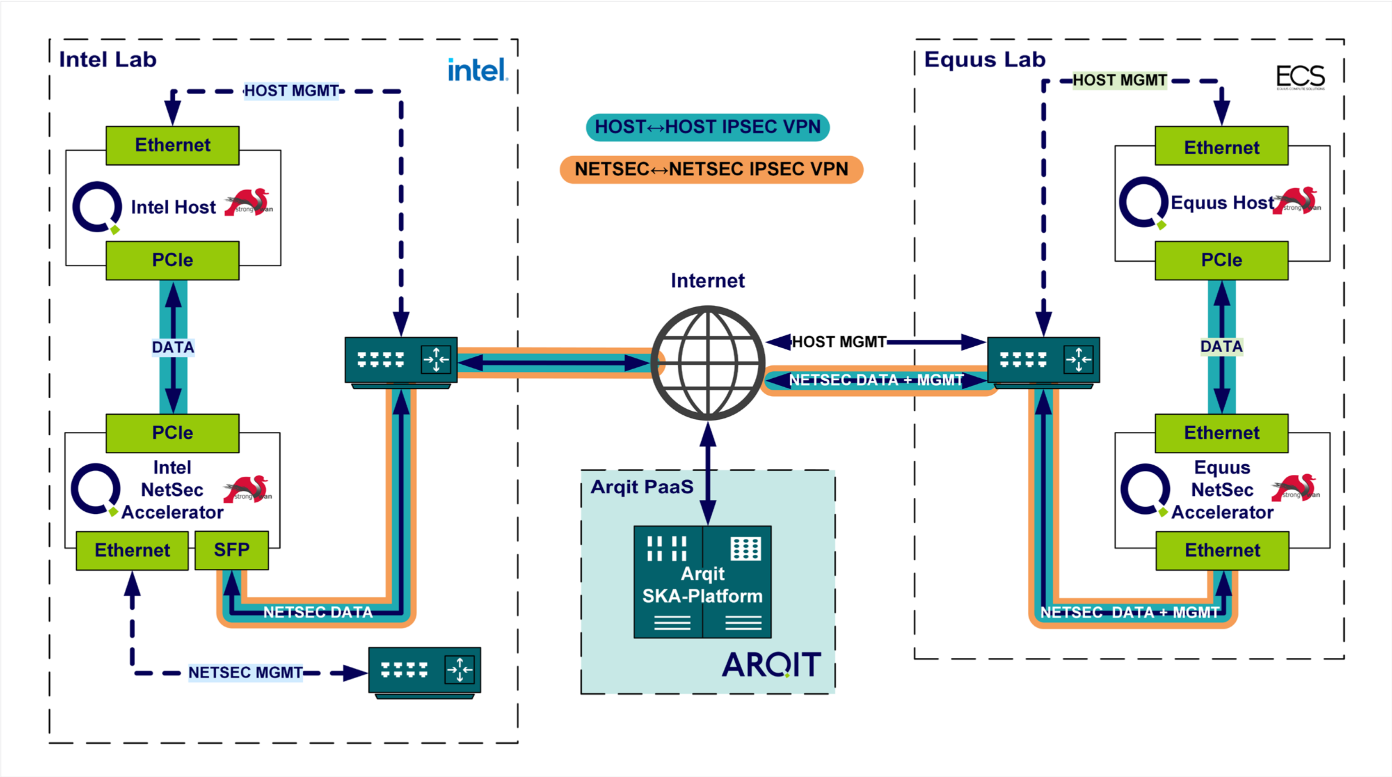

Figure 2. Highly secure and performant MACP architecture achieved by ECS, Arqit and Intel. Note that standard firewall components were deployed at the edge of each lab and on the Intel hosts to ensure MACP compliance.

Figure 2 displays the architecture that was deployed between the two lab environments. For the red and gray (inner and outer) VPN components, the open-source IPSec-based strongSwan application was chosen due to its implementation of RFC 8784[3] (a post-quantum security standard that complies with the CSfC Symmetric Key Management Requirements Annex[4]) as well as its ability to be natively integrated with other solution components such as post-quantum key management. Other components of the solution include:

- **Quantum Safe Security:** Arqit's SKA-Platform* allows IPSec tunnel endpoints to generate symmetric keys that meet current government recommendations and standards, protecting networks against attacks even by a CRQC. The keys which the SKA-Platform enables negotiation of can be refreshed – and thereby used to dynamically rekey IPSec tunnels – at rapid rates, in some cases multiple times per second. This dramatically reduces the lifetime of the encryption key and mitigates the opportunity for a device to be "spoofed" or impersonated on the network. Most importantly, Arqit's SKA process eliminates the need for manual key generation, couriering, loading, auditing, accounting, and other manpower-intensive and fundamentally unscalable key management operations.
- **Security Hardware Accelerators :** The solution utilizes Intel® Xeon® Scalable processor-based hosts with Intel® NetSec Accelerator Reference Design network security accelerator cards. These cards combine an Intel® Ethernet Controller with an Intel® Xeon® D processor, packaged in a PCIe add-in card form factor. They are designed to deliver the data plane and cryptography performance needed for the MACP application as well as other network security workloads. Its unique form factor allows deployment of additional network security optimized computers in space- and power-constrained data centers and edge locations.

- **RFC-8784-Compliant VPN:** strongSwan is a widely used open-source VPN library that can create an out-of-the-box quantum-safe VPN. Leveraging Arqit SKA-Platform, this setup generates post-quantum, symmetric pre-shared keys (PSK), which are then passed into the strongSwan configuration. This configuration makes the solution compliant with RFC-8784 standards. These keys make the strongSwan IPsec tunnel quantum-safe and can be refreshed as often as required. In the MACP application, the strongSwan VPN nodes are automatically monitored to ensure they are always verified, and the symmetric session keys are rotated every 30 seconds to ensure perfect forward secrecy.

Testing and Results

Evaluation of the combined MACP laydown was accomplished in two phases: functional validation between geographically segregated lab environments, and performance benchmarking within a single lab enclave. This division of efforts was chosen to demonstrate both the end-to-end feasibility of architecture in a real-world environment, as well as to quantify the impacts of introducing nested encryption schemes into high-throughput network testing.

To ensure a consistent and representative test environment, two identically provisioned Dell R750 systems were used as host platforms for the performance evaluations. These systems were configured with ample compute and memory headroom to prevent host-level bottlenecks from influencing throughput measurements. While each ran a different kernel version to validate compatibility across software revisions, both platforms utilized the same Intel network interface hardware and firmware, and each system was equipped with a dual-socket Intel® Xeon® 6338N processor configuration. The full hardware and software specifications of each test system are provided below:

Specification	Initiator Host	Receiver Host
Platform	Dell R750	Dell R750
Operating System	Ubuntu 22.04	Ubuntu 22.04
Kernel Version	6.8.0-57-generic	5.15.0-136-generic
Network Driver	ice	ice
Driver Version	6.8.0-57-generic	5.15.0-136-generic
Firmware Version	4.40 0x8001c98b 1.3534.0	4.40 0x8001c98b 1.3534.0
RAM	512 GB DDR4	512 GB DDR4
CPU	Dual socket Intel Xeon 6338N	Dual socket Intel Xeon 6338N

Table 1. Host system specifications.

The test environment was intentionally left unoptimized to reflect default, out-of-the-box behavior across all layers of the network stack. All systems operated with a standard Ethernet MTU of 1500 bytes, and no modifications were made to MSS values, socket buffer sizes, or TCP tuning parameters. Traffic was generated using iperf3 with default settings, resulting in standard TCP flows without application-level packet size constraints or protocol enhancements. IPSec tunnels were implemented using strongSwan, configured with the AES256-GCM12 cipher suite for authenticated encryption and x25519 as the key exchange mechanism, with no additional parameters set beyond what was necessary to establish the Security Associations. Fragmentation control, MSS clamping, and PMTU discovery behavior were all left at system defaults. This configuration represents a realistic yet unoptimized deployment scenario, allowing for evaluation of IPSec tunnel performance—including nesting—under conditions that closely mirror those found in typical production environments where advanced tuning has not been applied.

The functional validation was successful in achieving its primary goal of establishing a nested, quantum-secure strongSwan-based IPSec VPN connection between the two host systems across the open internet. The initial "outer" tunnels were first established between the netsec accelerator card installed on the bare metal hosts' respective PCIe interfaces. These tunnels were dynamically keyed via the Arqit SKA-Platform API integrated directly into the strongSwan daemon, leveraging a remotely hosted SKA-Platform instance to act as the broker for key agreement between the cards. The hosts and netsec accelerator cards were configured such that the accelerator card acted as the default data ingress/egress route for non-management network traffic. By default, strongSwan does not support nesting of IPSec security associations and tunnels, requiring the bypassing of port-based XFRM traps and default traffic policies on the initiator NIC.

Once these outer tunnels were established and the appropriate plugin and policy modifications were made to support nesting, a second "inner" tunnel was established between the bare metal hosts through the original tunnel. This inner tunnel was also keyed using the Arqit SKA-Platform. Successful nesting of the IPSec tunnels was validated through analysis of the native strongSwan security association metrics, XFRM policy states, and TCP/IP stack traces showing encrypted Encapsulated Security Payload (ESP) packets over the PCIe network interfaces to/from the host systems.

While this evaluation was sufficient to demonstrate the viability of the larger MACP concept, it was inappropriate for performance testing due to the non-deterministic uncertainties imposed by the open internet backhaul. Therefore, performance testing was conducted by migrating both systems to the same physical and logical network enclave (Figure 3).

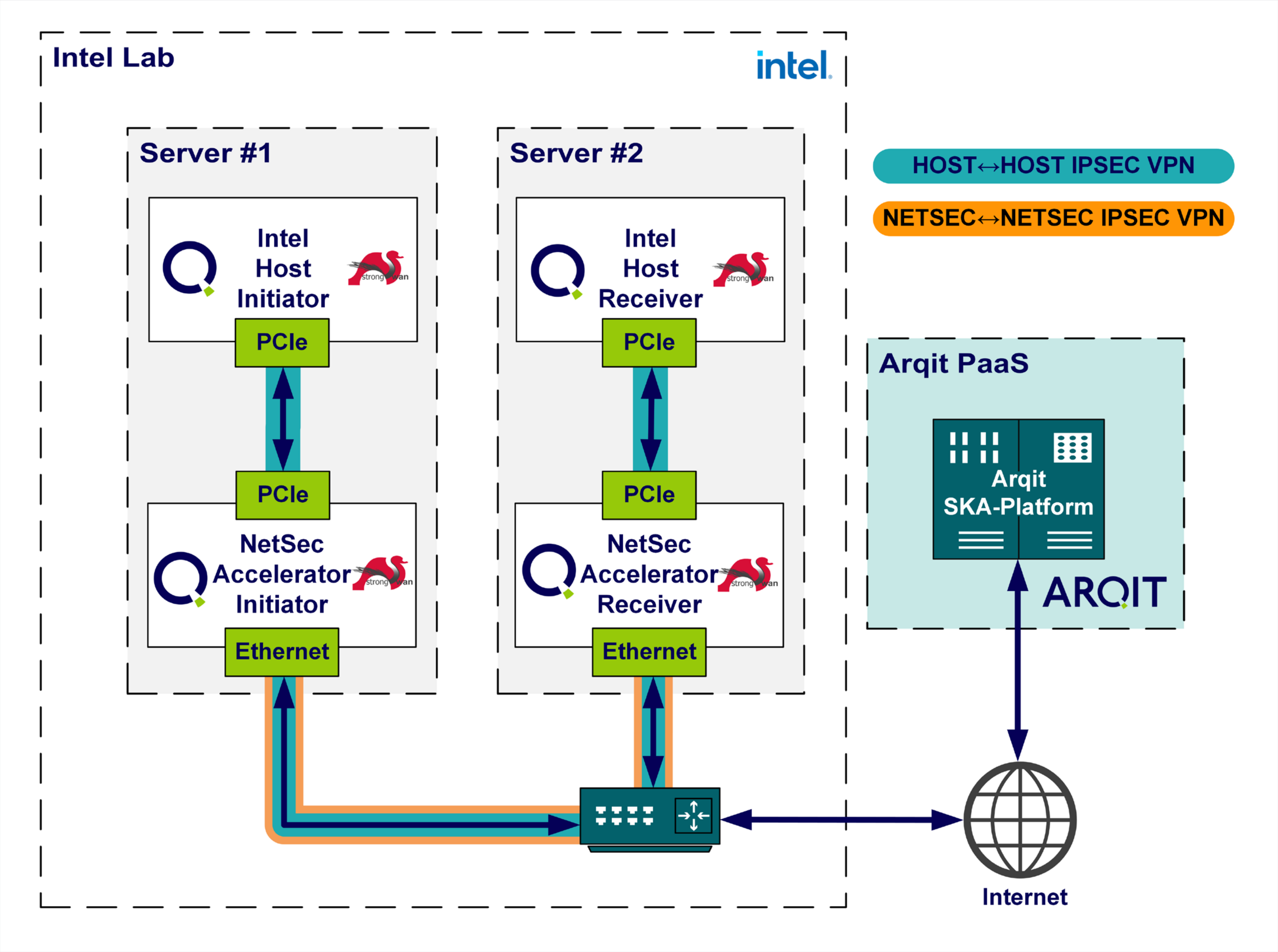

Figure 3. Modified lab laydown for performance evaluation.

While the Arqit SKA-Platform still required open internet connectivity to execute the symmetric key agreement process for the tunnels, the strongSwan tunnels were configured to be re-keyed every 30 seconds "make before break." This meant that re-keying of the tunnels wouldn't result in degradation of network performance, and the key agreement process itself did not act as a limiting factor to throughput.

The evaluation consisted of three sequential iperf3 test scenarios, each designed to incrementally increase the complexity of the traffic path while maintaining consistency in hardware, software, and environmental conditions.

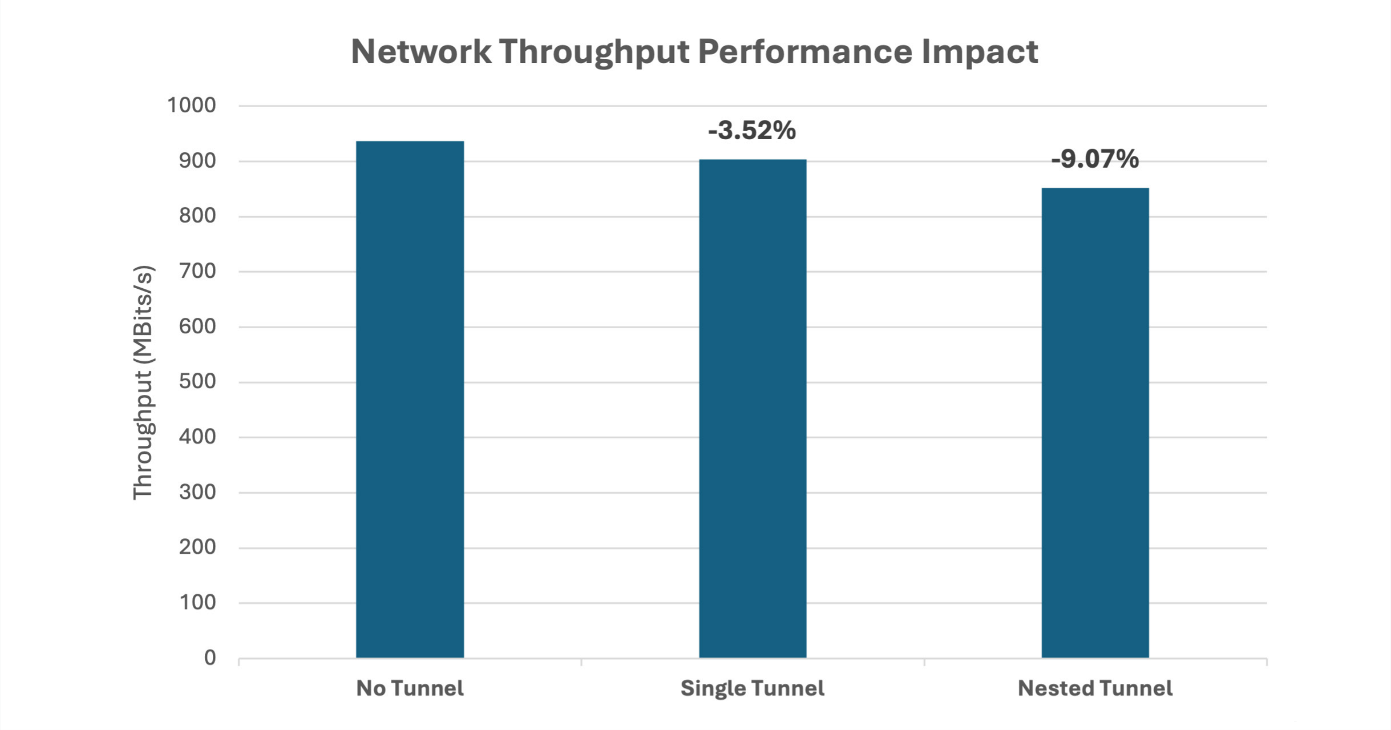

Figure 4. MACP topology throughput performance evaluation results.

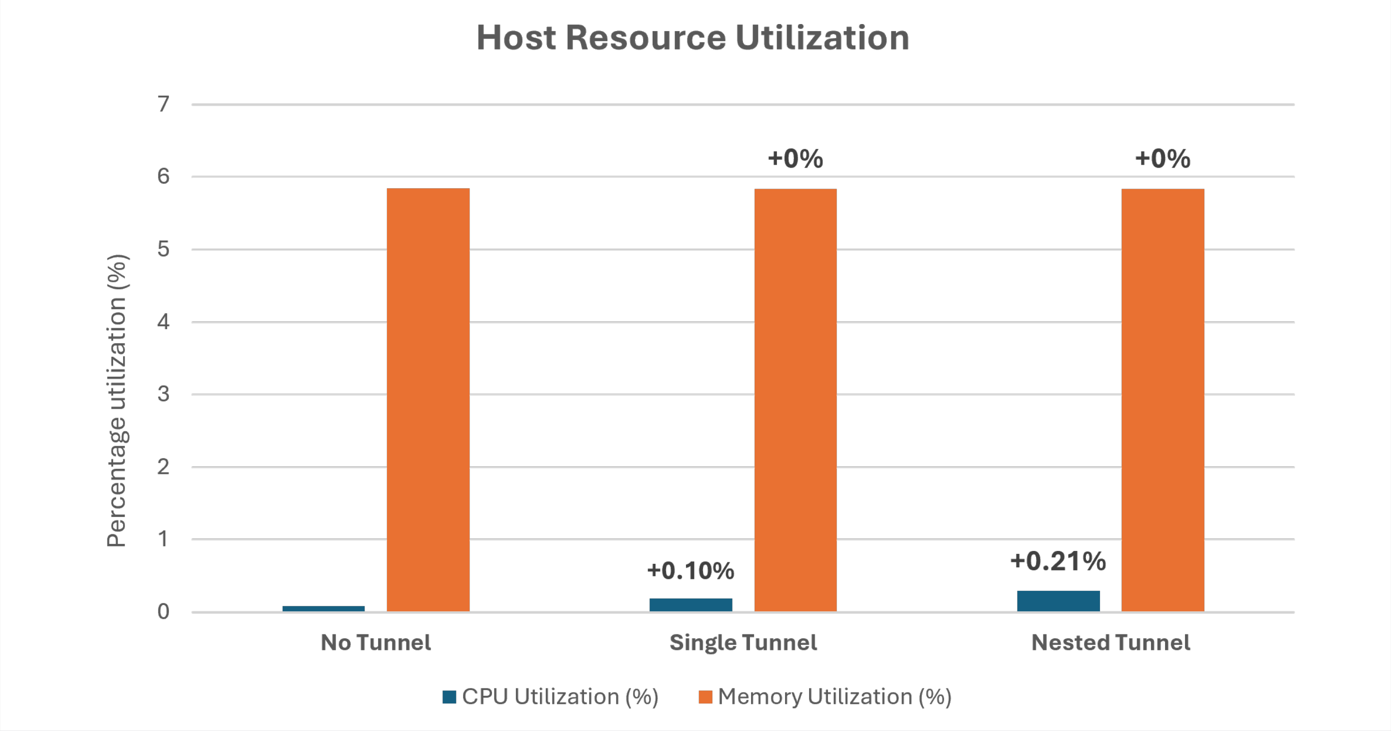

Figure 5. Host resource utilization results.

Unencrypted Baseline (No Tunnel)

In the baseline test, traffic was exchanged directly between the two hosts via their respective netsec accelerator cards, which acted as default gateways. No IPSec tunnels were in place. The measured throughput in this configuration averaged 937 Mbps, effectively establishing the raw performance ceiling of the setup in its unencrypted form.

This baseline figure represents the highest achievable throughput because it has no encapsulation overhead or cryptographic processing. It provides a reference point from which the impact of IPSec tunnel layering can be objectively assessed. Importantly, the testbed—featuring a standard Ethernet MTU of 1500 bytes and unmodified iperf3 defaults—demonstrated clean, stable results with negligible variance, underscoring the reliability of the local setup and the absence of extraneous bottlenecks.

Single Tunnel Configuration (NIC-to-NIC IPSec Tunnel)

Two netsec accelerators acting as NICs established the single tunnel. The average measured throughput for a single tunnel was 904 Mbps, representing a 3.5% decrease from the unencrypted baseline. Despite the additional overhead of encapsulation and cryptographic processing, the impact on performance was minor. Throughput remained stable and consistent, with no significant jitter or retransmission events observed.

The performance penalty incurred by a single layer of IPSec—under default conditions and without tuning—is modest. This result demonstrates that IPSec can be applied at the NIC level without materially degrading throughput, particularly when the encryption algorithm is implemented efficiently, and no fragmentation is induced.

Nested Tunnel Configuration (Host-to-Host Tunnel Encapsulated in NIC-to-NIC Tunnel)

Under the nested configuration, the average throughput measured was 852 Mbps, a further reduction of 5.8% from the single tunnel scenario, and a total decrease of 9.1% relative to the unencrypted baseline.

Despite the compounded encryption and additional protocol encapsulation, the system continued to deliver stable and reliable throughput. No adverse behaviors—such as significant retransmission, fragmentation, or erratic TCP behavior—were observed.

The results in aggregate demonstrate that quantum-secure, nested IPSec tunnels can be deployed without significant performance loss, even when no tuning has been applied. The performance impact is additive but not multiplicative—each layer introduces a predictable, bounded penalty.

> ***"We've designed this solution to address real-world security challenges by testing in deliberate phases. Phase I validated our ability to securely communicate between labs. In Phase II, we successfully sent pre-encrypted data through the same tunnel, with automated asymmetric key rotation. Phase III will integrate this solution into a private 5G environment, enabling secure communications and connectivity for classified operations. Our phased approach ensures each layer of security and performance is validated before moving to the next milestone."***
>
> **- Yazz Krdzalic, VP of Market Development at ECS**

Conclusion

This joint effort by ECS, Arqit, and Intel demonstrates a highly effective, CSfC-compliant MACP solution that is both quantum-safe and operationally scalable. By leveraging Arqit's SKA-Platform for symmetric key agreement and Intel NetSec Accelerator Reference Design for efficient cryptographic processing, the architecture overcomes the limitations of traditional key distribution and cryptographic agility. Performance testing confirmed that even a nested, dual-layer IPSec configuration—keyed dynamically via a post-quantum mechanism—introduces only modest and predictable performance penalties, validating its feasibility for real-world deployment without specialized tuning. The results confirm that high-assurance mobile access to classified networks can be achieved using commercial, software-defined components that scale to dynamic mission environments.

Complementary capabilities, including the Zscaler Branch Connector and Client Connector, extend these protections to encompass cloud environments, hybrid networks, and end-user devices. By enabling zero trust enforcement at both the edge and device level, this approach implements tightly controlled, identity-driven access policies that safeguard users and data. Together, this architecture provides a secure, future-ready solution for classified mobile access, ensuring resilience against emerging threats such as cryptographically relevant quantum computers.

Learn More

Equus Compute Systems Home Page

Arqit SKA Platform*

Mobile Access Capability Package (MACP) (PDF download)

Zscaler Home Page

strongSwan IPsec VPN

Intel® NetSec Accelerator Reference Design

Intel® Xeon® Processors

Intel® Industry Solution Builders

Notices & Disclaimers

[1] CSfC, "Mobile Access Capability Package V2.1" (Washington, DC: NSA, 2018)

[2] White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems" (official memorandum, Washington, DC: White House, 2022)

[3] Fluhrer, S, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", RFC 8784, 10.17487/RFC8784, June 2020, https://www.rfc-editor.org/info/rfc8784.

[4] CSfC, "Symmetric Key Management Requirements Annex V2.1" (Washington, DC: NSA, 2022)

Performance varies by use, configuration and other factors.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure for details. No product or component can be absolutely secure.

Intel optimizations, for Intel compilers or other products, may not optimize to the same degree for non-Intel products.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

See our complete legal Notices and Disclaimers.

Intel is committed to respecting human rights and avoiding causing or contributing to adverse impacts on human rights. See Intel's Global Human Rights Principles. Intel's products and software are intended only to be used in applications that do not cause or contribute to adverse impacts on human rights.

0425/DP/DJA/PDF ♻ Please Recycle 365210-001US