양자 시대를 대비한 VPN 솔루션

Future Systems

WeGuardia™ ITU Q-VPN

ITU는 양자 내성 암호(Post-Quantum Cryptography, PQC)를 기반으로 설계된 **차세대 VPN 솔루션**으로
미래의 양자 컴퓨터 위협에도 안전한 네트워크 접속을 보장합니다.
기존의 ECDH(DH) 기반 키 교환과 더불어, PQC 하이브리드 모드를 지원하여,
현재 인프라와의 호환성을 유지하면서도 장기적 안전성을 동시에 제공합니다.

양자 VPN 보안의 패러다임

기존 VPN은 ECDH(DH) 기반 키 교환으로 통해 안전성을 제공해왔으나,
양자컴퓨터 시대에는 이러한 알고리즘이 더 이상 안전하지 않습니다.
양자 VPN(ITU)은 NIST PQC 3종과 KPQC 4종을 지원하며,
ECDH(DH)+PQC 하이브리드 키 교환을 통해 현재와 미래 모두를 보호합니다.



제품 이미지

WeGuardia™ ITU Q-VPN

기존 VPN (Legacy VPN)

'기존 VPN'은 RSA/ECC와 같은 고전 암호를 기반으로 키 교환과 인증을 수행하여 안전한 통신을 보장해왔습니다.

하지만 양자컴퓨터가 실용화되면 RSA, ECC 등은 빠르게 해독될 수 있어 장기적인 보안성을 보장하기 어렵습니다.

따라서 과거 VPN의 보안은 현재 환경에서는 충분하지만, 미래의 양자 위협에는 취약한 구조를 가지고 있습니다.

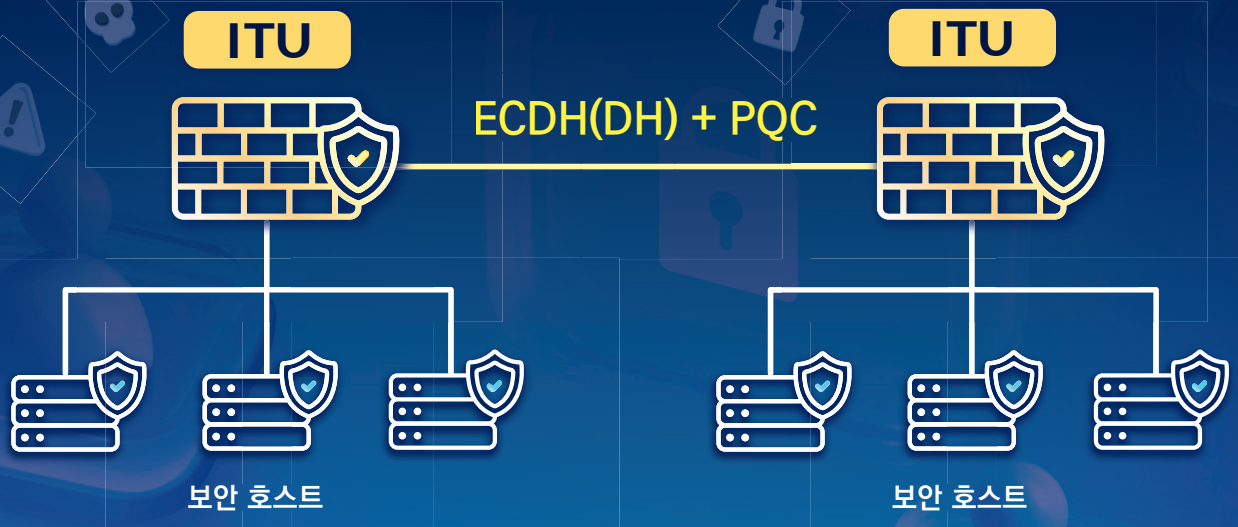


양자 VPN (Quantum VPN)

'양자 VPN'은 **양자 내성 암호(PQC)**를 적용하여, **NIST PQC 표준 3종과 KPQC 4종**을 지원합니다.

또한 기존 ECDH(DH) 키 교환과 PQC 키 교환을 결합한 하이브리드 모드를 통해 현재의 네트워크 인프라와 호환성을 유지하면서도, 양자컴퓨터 공격에도 안전한 통신을 보장합니다.

[Q-VPN 구성도]



Q-VPN 주요기능

[키 교환]

- ML-KEM

[서명]

- ML-DSA
- SLH-DSA

NIST 표준 알고리즘 지원

[키 교환]

- SMAUG-T
- NTRU+

[서명]

- AIMer
- HAETAE

KPQC 알고리즘 지원

ECDH (DH) + PQC

안전한 하이브리드 구성

전통 암호와 양자내성암호를 함께 사용하는 것이 NIST 권고사항입니다.

양자내성암호 표준화 동향

2024년 NIST 8월 표준 3개 발표 ▶ 2025년 KPQC 국내 표준화 작업 중이며, 4개 발표 (SMAUG-T, NTRU+, AIMer, HAETAE) ▶ 2027년 이내에 ISO에서 국제 표준 제정할 것으로 예상

Future Systems

서울특별시 구로구 디지털로 26길 61 (에이스하이엔드타워 2차), 1902호
070-8853-6327 02-837-2986 www.future.co.kr
영업문의 business@future.co.kr(사업본부)