WIREGUARD TUNNEL

Requirement for Port Opening and Security Assessment

UDP port 19818 must be opened for the new Stargate solution to operate. This port is used exclusively for establishing and operating the WireGuard tunnel.[1] Without an accessible transport endpoint, the encrypted tunnel cannot be established.

From a security perspective, port opening should not be viewed in isolation as simply an additional open service, but must be evaluated in the context of the target architecture.

Communication connections that were previously routed through publicly accessible application endpoints are transferred into an encrypted, mutually authenticated tunnel. This reduces the public exposure of the affected systems. The ports used previously served to provide direct access to specific application services, such as for SMTP or HTTPS-based communication. In contrast, the additional UDP port 19818 to be opened serves a different function. It does not provide a publicly accessible application service but serves exclusively as a transport endpoint for establishing and operating the WireGuard tunnel. The interface accessible on UDP 19818 accepts only authorized communication; unauthenticated packets are discarded without response. Unlike traditionally exposed application ports, this provides significantly fewer exploitable characteristics for reconnaissance, service identification, and reliable fingerprinting.

Opening the port therefore does not lead to a security-relevant expansion of the attack surface, but rather to its consolidation. While an additional UDP port is required, inter-organizational communication paths are simultaneously shifted from publicly accessible endpoints to a modern, controlled, and cryptographically secured transport layer.

However, the exposure of a UDP port remains fundamentally vulnerable to volumetric attacks at the network level, regardless of the protocol's cryptographic security. Appropriate protective measures must be implemented at the infrastructure and transport levels.

SMTP also remains necessary for the time being for communication with external partners without Stargate; additional Stargate traffic, however, is routed via the mesh and the WireGuard tunnel. The net security effect should ultimately be viewed as a gradual reduction in publicly exposed communication connections.

It should be noted that WireGuard is based on a modern, extensively tested cryptographic foundation. Curve25519 is used for key exchange, ChaCha20-Poly1305 for confidentiality and integrity, and BLAKE2s for cryptographic hashing functions.[2] The absence of cipher negotiation reduces protocol complexity and precludes downgrade attacks on negotiated ciphers. The formal security analyses of the WireGuard protocol are publicly documented.[3]

---

[1] https://www.wireguard.com/papers/wireguard.pdf
[2] https://www.wireguard.com/protocol/
[3] https://www.wireguard.com/formal-verification

The implementation side is also relevant from a security perspective: The Linux implementation of WireGuard is deliberately kept lean compared to traditional VPN stacks and has been part of the mainline kernel since Linux 5.6. As part of the mainline kernel, the implementation is subject to the established review and maintenance processes of the Linux kernel. Given the widespread use of the Linux kernel in security-critical and large-scale environments, it can also be assumed that there is ongoing and very thorough technical review by independent third parties.

Even if the HIN CA is unavailable, the fail-secure principle remains in effect from a security perspective. This means that in the absence of a validation basis, no new trust decisions may be made and no connections may be permitted at a reduced security level. In this context, it is essential for the new solution that the trust relationship no longer depends on an external third-party CA in the same way as in traditional gateway-centric trust models. Authentication is based on cryptographic identity and verifiable, tamper-proof key event logs. This reduces a structural dependency that is inherent in traditional PKI-centric operating models. Consequently, the system's resilience is also improved without compromising security.

The fact that encrypted UDP traffic can only be inspected to a limited extent on the network side does not represent a relevant security disadvantage in this architecture either. Rather, security control simply shifts from a predominantly perimeter-centric inspection approach to a model that is more robust from today's security perspective, based on strong mutual authentication, cryptographic protection, and traceable logging at the participating endpoints.

The opening of UDP port 19818 is therefore necessary from a security perspective because it does not simply serve the additional public provision of an application service, but rather the establishment of a modern, secure transport channel. This enables interorganizational communication relationships to be shifted from publicly addressable endpoints to a more controlled and cryptographically robustly secured overlay. The resulting architecture is advantageous from a security perspective because it gradually reduces public exposure, limits protocol and implementation complexity, reduces dependencies on external trust anchors, and supports consistent fail-secure behavior.