TUNNEL WIREGUARD

Nécessité de l'ouverture du port et évaluation de la sécurité

L'ouverture du port UDP 19818 est nécessaire au fonctionnement de la nouvelle solution Stargate. Ce port est utilisé exclusivement pour l'établissement et le fonctionnement du tunnel WireGuard.[1] Sans point de terminaison de transport accessible, le tunnel crypté ne peut pas être établi.

D'un point de vue technique et sécuritaire, l'ouverture de ce port ne doit pas être considérée isolément comme un simple service ouvert supplémentaire, mais doit être évaluée dans le contexte de l'architecture cible.

Les relations de communication qui passaient jusqu'à présent par des points de terminaison d'application accessibles au public sont transférées dans un tunnel crypté et mutuellement authentifié. Cela réduit l'exposition publique des systèmes concernés. Les ports utilisés jusqu'à présent servaient à l'accessibilité directe de services d'application concrets, par exemple pour la communication basée sur SMTP ou HTTPS. Le port UDP 19818, qui doit être ouvert en plus, remplit en revanche une autre fonction. Il ne fournit pas de service d'application accessible au public, mais sert exclusivement de point de terminaison de transport pour l'établissement et l'exploitation du tunnel WireGuard. L'interface accessible sur UDP 19818 n'accepte que les communications autorisées ; les paquets non authentifiés sont rejetés sans réponse. Contrairement aux ports d'application classiques exposés, cela fournit nettement moins de caractéristiques exploitables pour la reconnaissance, l'identification des services et l'empreinte digitale fiable.

L'ouverture du port n'entraîne donc pas une extension de la surface d'attaque en termes de sécurité, mais sa consolidation. Certes, un port UDP supplémentaire est nécessaire, mais dans le même temps, les voies de communication interorganisationnelles sont transférées depuis des points d'extrémité accessibles au public vers une couche de transport moderne, contrôlée et sécurisée par cryptographie.

L'exposition d'un port UDP reste toutefois fondamentalement vulnérable aux attaques volumétriques au niveau du réseau, indépendamment de la sécurisation cryptographique du protocole. Des mesures de protection appropriées doivent être prévues au niveau de l'infrastructure et du transport.

De même, le protocole SMTP reste pour l'instant indispensable pour les échanges avec des partenaires de communication externes ne disposant pas de Stargate ; le trafic Stargate supplémentaire est en revanche acheminé via le maillage et le tunnel WireGuard. L'effet net en termes de sécurité doit finalement être considéré comme une réduction progressive des relations de communication exposées au public.

Il convient de noter que WireGuard repose sur une base cryptographique moderne et largement testée. Sont utilisés Curve25519 pour l'échange de clés, ChaCha20-Poly1305 pour la confidentialité

[1] https://www.wireguard.com/papers/wireguard.pdf

et l'intégrité, ainsi que BLAKE2s pour les fonctions de hachage cryptographiques.[2] L'absence de négociation de chiffrement réduit la complexité du protocole et exclut les attaques par downgrade sur les méthodes négociées. Les analyses formelles de sécurité du protocole WireGuard sont documentées publiquement.[3]

Le côté implémentation est également pertinent en termes de sécurité : l'implémentation Linux de WireGuard est délibérément allégée par rapport aux piles VPN classiques et fait partie du noyau principal depuis Linux 5.6. En tant que composante du noyau principal, l'implémentation est soumise aux processus de révision et de maintenance établis du noyau Linux. Compte tenu de la large utilisation du noyau Linux dans des environnements critiques en matière de sécurité et à grande échelle, on peut en outre supposer qu'il fait l'objet d'un examen technique continu et très précis par des tiers indépendants.

Même en cas d'indisponibilité de la CA HIN, le principe «fail-secure» s'applique toujours du point de vue de la sécurité. Cela signifie qu'en l'absence de base de validation, aucune nouvelle décision de confiance ne doit être prise et aucune connexion ne doit être autorisée avec un niveau de sécurité réduit. Dans ce contexte, il est essentiel pour la nouvelle solution que la relation de confiance ne dépende plus de la même manière d'une autorité de certification tierce externe que dans les modèles de confiance classiques centrés sur une passerelle. L'authentification repose sur l'identité cryptographique et sur des journaux d'événements de clés vérifiables et inviolables. Cela permet de réduire une dépendance structurelle inhérente aux modèles d'exploitation classiques centrés sur l'infrastructure PKI. Par conséquent, la résilience du système est notamment améliorée, sans pour autant compromettre la sécurité.

Le fait que le trafic UDP chiffré ne puisse être inspecté que de manière limitée au niveau du réseau ne constitue pas non plus un inconvénient de sécurité significatif dans cette architecture. Le contrôle de sécurité passe simplement d'une approche d'inspection principalement centrée sur le périmètre à un modèle plus robuste du point de vue des techniques de sécurité actuelles, qui repose sur une authentification mutuelle forte, une sécurisation cryptographique et une journalisation traçable au niveau des terminaux concernés.

L'activation du port UDP 19818 s'impose donc d'un point de vue technique, car elle ne sert pas simplement à la mise à disposition publique supplémentaire d'un service d'application, mais à l'établissement d'un canal de transport sécurisé de manière moderne. Cela permet de transférer les relations de communication interorganisationnelles depuis des points d'extrémité accessibles publiquement vers une superposition (overlay) plus contrôlée et sécurisée de manière cryptographique plus robuste. L'architecture qui en résulte est avantageuse du point de vue de la sécurité, car elle réduit progressivement l'exposition publique, limite la complexité des protocoles et de la mise en œuvre, diminue les dépendances vis-à-vis d'ancres de confiance externes et prend en charge un comportement «fail-secure» cohérent.

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