TUNNEL WIREGUARD

Necessità dell'apertura della porta e valutazione della sicurezza

Per il funzionamento della nuova soluzione Stargate è necessaria l'apertura della porta UDP 19818. Questa porta viene utilizzata esclusivamente per la creazione e il funzionamento del tunnel WireGuard.[1] Senza un endpoint di trasporto raggiungibile, non è possibile stabilire il tunnel crittografato.

Dal punto di vista della sicurezza, l'apertura della porta non deve essere valutata isolatamente come un semplice servizio aggiuntivo aperto, ma deve essere considerata nel contesto dell'architettura di destinazione.

Le relazioni di comunicazione che finora sono state gestite tramite endpoint applicativi accessibili pubblicamente vengono trasferite in un tunnel crittografato e autenticato reciprocamente. Ciò riduce l'esposizione pubblica dei sistemi interessati. Le porte utilizzate finora servivano per l'accessibilità diretta a servizi applicativi specifici, ad esempio per la comunicazione basata su SMTP o HTTPS. La porta UDP 19818, che deve essere resa disponibile in aggiunta, svolge invece una funzione diversa. Non fornisce un servizio applicativo utilizzabile pubblicamente, ma serve esclusivamente come endpoint di trasporto per la creazione e il funzionamento del tunnel WireGuard. L'interfaccia raggiungibile su UDP 19818 accetta solo comunicazioni autorizzate; i pacchetti non autenticati vengono scartati senza risposta. A differenza delle classiche porte applicative esposte, ciò fornisce caratteristiche significativamente meno utilizzabili per la ricognizione, l'identificazione del servizio e il fingerprinting affidabile.

L'apertura della porta non comporta quindi un ampliamento rilevante dal punto di vista della sicurezza della superficie di attacco, ma piuttosto il suo consolidamento. Sebbene sia necessaria una porta UDP aggiuntiva, allo stesso tempo i percorsi di comunicazione interorganizzativi vengono spostati da endpoint accessibili pubblicamente a un livello di trasporto moderno, controllato e protetto crittograficamente.

L'esposizione di una porta UDP rimane tuttavia fondamentalmente vulnerabile agli attacchi volumetrici a livello di rete, indipendentemente dalla protezione crittografica del protocollo. È necessario prevedere misure di protezione adeguate a livello di infrastruttura e di trasporto.

Anche SMTP rimane necessario fino a nuovo avviso per lo scambio con partner di comunicazione esterni senza Stargate; il traffico Stargate aggiuntivo viene invece instradato attraverso la mesh e il tunnel WireGuard. L'effetto netto in termini di sicurezza è da valutarsi, in definitiva, come una riduzione graduale delle relazioni di comunicazione esposte pubblicamente.

Va notato che WireGuard si basa su una base crittografica moderna e ampiamente testata. Vengono utilizzati Curve25519 per lo scambio di chiavi, ChaCha20-Poly1305 per la riservatezza e l'integrità e BLAKE2s per le funzioni di hashing crittografico.[2] La rinuncia alla Cipher Negotiation

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

riduce la complessità del protocollo ed esclude attacchi di downgrade ai metodi negoziati. Le analisi formali di sicurezza del protocollo WireGuard sono documentate pubblicamente.[3]

Anche il lato dell'implementazione è rilevante dal punto di vista della sicurezza: l'implementazione Linux di WireGuard è volutamente snella rispetto ai classici stack VPN e fa parte del kernel mainline a partire da Linux 5.6. In quanto parte del kernel mainline, l'implementazione è soggetta ai processi di revisione e manutenzione consolidati del kernel Linux. Considerando l'ampio utilizzo del kernel Linux in ambienti critici per la sicurezza e su larga scala, si può inoltre presumere che vi sia una verifica tecnica continua e molto accurata da parte di terzi indipendenti.

Anche in caso di non raggiungibilità della CA HIN, dal punto di vista della sicurezza tecnica si applica invariato il principio «fail-secure». Ciò significa che, in assenza di una base di convalida, non devono essere prese nuove decisioni di fiducia e non devono essere consentite connessioni con un livello di sicurezza ridotto. Per la nuova soluzione è essenziale, in questo contesto, che il rapporto di fiducia non dipenda più in modo analogo da una CA di terze parti esterna come nei classici modelli di fiducia incentrati sul gateway. L'autenticazione si basa sull'identità crittografica e su registri degli eventi delle chiavi verificabili e a prova di manomissione. Ciò riduce una dipendenza strutturale che è intrinseca nei modelli operativi classici incentrati sulla PKI. Di conseguenza, viene migliorata in particolare anche la resilienza del sistema, senza compromettere la sicurezza.

Il fatto che il traffico UDP crittografato sia ispezionabile solo in modo limitato a livello di rete non rappresenta un svantaggio rilevante in termini di sicurezza in questa architettura. Il controllo di sicurezza si sposta piuttosto semplicemente da un approccio di ispezione prevalentemente incentrato sul perimetro verso un modello più robusto dal punto di vista della sicurezza odierna, basato su una forte autenticazione reciproca, protezione crittografica e registrazione tracciabile sugli endpoint coinvolti.

L'abilitazione di UDP 19818 è quindi necessaria dal punto di vista della sicurezza, poiché non serve semplicemente alla fornitura pubblica aggiuntiva di un servizio applicativo, ma alla creazione di un canale di trasporto protetto in modo moderno. Ciò consente di spostare le relazioni di comunicazione interorganizzative da endpoint indirizzabili pubblicamente a un overlay più controllato e protetto in modo crittograficamente più robusto. L'architettura risultante è vantaggiosa dal punto di vista della sicurezza, poiché riduce gradualmente l'esposizione pubblica, limita la complessità del protocollo e dell'implementazione, riduce le dipendenze da ancore di fiducia esterne e supporta un comportamento «fail-secure» coerente.

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