

Tailscale in der Praxis

Sichere Netzwerke ohne komplizierte VPN-Konfiguration

Kapitel 1

Klassische VPN-Architekturen und ihre Trugschlüsse

1.1 Klassische VPN-Architekturen und ihre Trugschlüsse

Kurz-Glossar fuer klassische VPN-Begriffe (ausfuehrliche Erklaerung jeweils in den folgenden Abschnitten):

- **DMZ** (demilitarisierte Zone): Ein vom internen Netz isolierter Bereich, in dem Dienste laufen, die aus dem Internet erreichbar sein muessen. Klassischer Standort fuer VPN-Gateways.
- **DynDNS** (Dynamic DNS): Ein Dienst, der eine wechselnde oeffentliche IP-Adresse des Routers unter einem festen Domain-Namen erreichbar macht. Erlaubt den Zugriff auf das Heimnetz ohne statische IP.
- **GRE** (Generic Routing Encapsulation): Ein Tunnel-Protokoll auf IP-Ebene, das von PPTP fuer die eigentliche Datenkapselung genutzt wird. PPTP nutzt zusaetzlich TCP-Port 1723 fuer die Steuerung.
- **IPSec** (Internet Protocol Security): Eine Familie von Protokol-

möchte vielleicht auf einen Drucker im Heimnetz zugreifen oder eine Sicherheitskamera einsehen, die nur intern erreichbar ist. In einer klassischen VPN-Architektur gibt es dafür im Wesentlichen zwei Wege: Entweder das Kind bekommt einen vollständigen VPN-Client-Zugang mit dem gleichen Profil wie ein Administrator, oder es gibt einen Sonderweg mit Doppel-NAT und Portfreigaben. Beides ist un schön.

Die Summe dieser Alltagsprobleme macht klar, dass das VPN-Problem nicht in einer fehlenden Funktion besteht. IPSec, SSL-VPN, WireGuard und andere Protokolle können verschlüsseln, authentifizieren und routen. Das Problem besteht in der Kombination aus Bereitstellungsaufwand, Endgeräte-Vielfalt, wechselnden Netzbedingungen und der Erwartung, dass alles “einfach funktioniert”, ohne dass pro Standort, pro Gerät und pro Anwendungsfall ein eigenes Konfigurationspaket geschnürt werden muss.

1.3 Sicherheitsrisiken offener Ports und zentraler VPN-Gateways

Die meisten Sicherheitsvorfälle, die in den vergangenen Jahren über Schlagzeilen bekannt wurden, hatten eine Gemeinsamkeit: Ein exponiertes System mit einem offenen Port, der nicht hätte offen sein sollen, oder ein zentraler Authentifizierungsdienst, der kompromittiert wurde und allen Angreifern Tür und Tor öffnete. Klassische VPN-Gateways sitzen genau in diesem Brennpunkt. Sie müssen von außen erreichbar sein, sonst kann sich niemand verbinden. Sie akzeptieren Verbindungen von beliebigen Quell-IPs, weil der Anwender sich morgen in einem Hotel in Tokio oder in einem Café in Lissabon befinden kann. Sie prüfen Anmeldeinformationen und öffnen danach den Datenverkehr in das interne Netz. Damit sind sie ein lohnendes Ziel.

Die Angriffsfläche lässt sich grob in vier Bereiche gliedern. Der erste Bereich betrifft die Implementierung des VPN-Protokolls selbst. Über die Jahre hinweg gab es wiederholt schwerwiegende Schwachstellen in IPSec-Implementierungen, in SSL-VPN-Bibliotheken und in der Handhabung von Zertifikaten. Solange der Quellcode fehlerfrei ist und Patches zeitnah eingespielt werden, ist das Risiko begrenzt. In

einfache Weise adressierbar sind.

Die Lösung sollte Skalierbarkeit nicht durch zentrale Engpässe erkaufen. Wenn einhundert Anwender gleichzeitig verbunden sind, sollte die Architektur nicht in die Knie gehen. Das bedeutet in der Praxis, dass die Datenebene (die tatsächliche Verschlüsselung und Weiterleitung der Pakete) nicht durch einen zentralen Tunnel-Server laufen sollte, sondern direkt zwischen den Endpunkten.

Schließlich sollte die Lösung Zero-Trust-Prinzipien unterstützen. Zero Trust bedeutet, dass kein Gerät, kein Anwender und kein Dienst aufgrund seiner Position im Netz als “vertrauenswürdig” gilt. Stattdessen wird jede Verbindung einzeln authentifiziert, autorisiert und protokolliert. Ein modernes Mesh-VPN ist ein natürlicher Ausgangspunkt für eine Zero-Trust-Architektur, weil jeder Knoten von Anfang an als potenziell kompromittiert behandelt wird und jede Verbindung explizit erlaubt werden muss.

Anforderung	Klassisches VPN	Mesh-VPN (Tailscale)
Eingehende Portfreigabe nötig	Ja (z. B. UDP 500, ESP)	Nein
Funktioniert hinter CGNAT	Nur mit Tricks	Ja
Konfigurationszeit pro Knoten	Stunden	Minuten
Granulare Zugriffsrechte	Über Firewall-Regeln	Über ACL-Datei
DNS im VPN	Manuell	MagicDNS
Zero-Trust-fähig	Nur mit Zusatzaufwand	Integriert
Skalierbarkeit	Begrenzt durch Gateway	Skaliert mit Endpunkten

Diese Tabelle ist keine Wertung, sondern eine Verdichtung der strukturellen Unterschiede. In der Praxis wird mancher Administrator weiterhin klassische IPSec-Gateways betreiben, etwa weil regulatorische Vorgaben es verlangen oder weil ein bestehender Vertrag mit einem Hardware-Hersteller dies vorschreibt. Für die Mehrzahl der Alltagsfälle jedoch, und insbesondere für die im nächsten Abschnitt beschriebenen Szenarien, ist ein Mesh-VPN die schlankere Lösung.